Algebra

Contents

Part I
Group Theory

In this part of the document, we will study group theory.

1 Basic Definitions

Throughout this section, let X be a nonempty set.

1.1 Definition of a Group

Definition 1.1. A **binary operation** $\star$ on X is a function $\star\colon X \times X \to X$, which we denote by

$$(x, y) \mapsto x \star y.$$

A set X equipped with a binary operation $\star$ is called a **magma**, and is denoted $(X, \star)$. The pair $(X, \star)$ is called a **semigroup** if the binary operation is **associative**; that is

$$(x \star y) \star z = x \star (y \star z)$$

for all $x, y, z \in X$. The pair $(X, \star)$ is called a **monoid** if $(X, \star)$ is a semigroup and there exists a **left** and **right inverse element**; that is, there exists $e, e' \in X$ such that

$$e \star x = x = x \star e'$$

for all $x \in X$. In fact, we automatically have $e = e'$. Indeed, we have

$$\begin{aligned} e' &= e \star e' \\ &= e. \end{aligned}$$

For this reason, we say e is the **identity element**. The pair $(X, \star)$ is called a **group** if $(X, \star)$ and every element has a **left** and **right inverse**; that is, for all $x \in X$ there exists $y, z \in X$ such that

$$x \star z = e = y \star x.$$

In fact, associativity automatically implies $y = z$. Indeed, we have

$$\begin{aligned} y &= y \star e \\ &= y \star (x \star z) \\ &= (y \star x) \star z \\ &= e \star z \\ &= z. \end{aligned}$$

For this reason, we say x has an **inverse element**, rather than a left and right inverse since they are the same element anyways, and we denote the inverse of x by x^{-1}. The pair $(X, \star)$ is called an **abelian group** if $(X, \star)$ is a group and the binary operation is **commutative**; that is

$$x \star y = y \star x$$

for all $x, y \in X$.

Remark 1. We often denote a group by G where we view G as a set equipped with a binary operation. Arbitrary groups are usually denoted by G, H, and K, and abelian groups are usually denoted by A,B, and C. The binary operation for a group G is usually denoted by $\cdot$ rather than $\star$. To ease notation, if $g, h \in G$, then we often write gh rather than $g \cdot h$.

1.1.1 Abelian Groups $\mathbb{Z}$ and $\mathbb{Q}^\times$

Example 1.1. Addition is a binary operation on $\mathbb{N}$, however negation is not a binary operation on $\mathbb{N}$. For example, $1 - 5 \notin \mathbb{N}$. The pair $(\mathbb{N}, +)$ forms a semigroup with identity 0. It is not quite a group yet, but we can make it into a group by *adjoining* inverse elements. When we do this, we obtain the group of integers under addition, denoted by $\mathbb{Z}$. Similarly, multiplication is a binary operation on $\mathbb{Z}$, but division is not a binary operation on $\mathbb{Z}$. The pair $(\mathbb{Z}, \cdot)$ forms a semigroup with identity 1. This semigroup is also not a group because we are again missing inverses as in the case of $(\mathbb{N}, +)$. This time however, if we try to adjoin inverses to *all* elements in $(\mathbb{Z}, \cdot)$, then we will run into a problem; namely adjoining an inverse to 0 will collapse the whole structure to the trivial group $(\{1\}, \cdot)$:

$$\begin{aligned} a &= 1 \cdot a \\ &= (0^{-1}0) \cdot a \\ &= 0^{-1}(0 \cdot a) \\ &= 0^{-1}0 \\ &= 1. \end{aligned}$$

In order to avoid this, we adjoint inverses to all elements in $\mathbb{Z}$ *except* 0. The pair $(\mathbb{Q}, \cdot)$ is still not a group yet, but if we restrict multiplication to $\mathbb{Q}\backslash\{0\} \times \mathbb{Q}\backslash\{0\}$, then we do get a group, denoted by $\mathbb{Q}^\times$. To see this, we just need to verify that restricting multiplication to $\mathbb{Q}\backslash\{0\} \times \mathbb{Q}\backslash\{0\}$ lands in $\mathbb{Q}\backslash\{0\}$. Indeed, assume for a contradiction that there exists $a, b \in \mathbb{Q}\backslash\{0\}$ such that $ab = 0$. As $a \neq 0$, we can multiply both sides by a^{-1} to obtain $b = 0$, which is a contradiction.

Example 1.2. Define a binary operation $\star$ on $\mathbb{Q}$ by

$$a \star b = ab + 3a + 3b + 6$$

for all $a, b \in \mathbb{Q}$. The binary operation is clearly abelian. It is also associative. Indeed, we have

$$\begin{aligned} (a \star b) \star c &= (ab + 3a + 3b + 6)c + 3(ab + 3a + 3b + 6) + 3c + 6 \\ &= abc + 3ab + 3ac + 3bc + 9a + 9b + 9c + 24 \\ &= a(bc + 3b + 3c + 6) + 3a + 3(bc + 3b + 3c + 6) + 6 \\ &= a \star (b \star c). \end{aligned}$$

There also exists an identity element; namely -2 $\in \mathbb{Q}$. To see this, we only need to check that -2 is a right inverse since the binary operation is abelian. For all $a \in \mathbb{Q}$, we have

$$\begin{aligned} a \star -2 &= a(-2) + 3a + 3(-2) + 6 \\ &= -2a + 3a - 6 + 6 \\ &= a. \end{aligned}$$

On the other hand, not every element in $\mathbb{Q}$ has an inverse. Indeed, let $a \in \mathbb{Q}$. To find the inverse of a, we solve for b in

$$ab + 3a + 3b + 6 = -2.$$

We obtain

$$a^{-1} = \frac{-3a - 8}{a + 3}.$$

Thus every element in $\mathbb{Q}\backslash\{-3\}$ has an inverse element, but -3 does not have an inverse element. Thus $(\mathbb{Q}, \star)$ is a monoid, but not quite a group. However, if we restrict the binary operation $\star$ to the set $\mathbb{Q}\backslash\{-3\} \times \mathbb{Q}\backslash\{-3\}$, then we do get a group $(\mathbb{Q}\backslash\{-3\}, \star)$. To see this, we just need to verify that $\star$ restricted to $\mathbb{Q}\backslash\{-3\} \times \mathbb{Q}\backslash\{-3\}$ lands in $\mathbb{Q}\backslash\{-3\}$. Indeed, assume for a contradiction that $a \star b = -3$ for some $a, b \in \mathbb{Q}\backslash\{-3\}$. Then

$$\begin{aligned} 0 &= a \star b + 3 \\ &= ab + 3a + 3b + 9 \\ &= (a + 3)(b + 3) \end{aligned}$$

implies either $a + 3 = 0$ or $b + 3 = 0$. In either case, we obtain a contradiction.

Later on we will show that the group $(\mathbb{Q}\backslash\{-3\}, \star)$ is in fact isomorphic (a term which we shall define later) to the group $\mathbb{Q}^\times$, with the isomorphism $\varphi \colon \mathbb{Q}^\times \to (\mathbb{Q}\backslash\{-3\}, \star)$ defined by

$$\varphi(a) = a - 3$$

for all $a \in \mathbb{Q}^\times$.

1.1.2 Abelian Group $(\mathcal{P}(X), \Delta)$

Definition 1.2. The **power set** of X, denoted by $\mathcal{P}(X)$, is the set of all subsets of X. The **symmetric difference** of two subsets A and B of X is defined by

$$A\Delta B = (A \cup B) \backslash (A \cap B).$$

This gives rise to a binary operation $\Delta \colon X \times X \to X$.

Proposition 1.1. *The pair $(\mathcal{P}(X), \Delta)$ forms an abelian group.*

Proof. The identity element for $(\mathcal{P}(X), \Delta)$ is clearly the empty set. Clearly Δ is abelian. Let us show that it is also associative. Let $A, B, C \in \mathcal{P}(X)$. Then we have

$$\begin{aligned}
(A\Delta B)\Delta C &= ((A\Delta B) \cup C) \cap ((A\Delta B) \cap C)^c \\
&= ((A\Delta B) \cup C) \cap ((A\Delta B)^c \cup C^c) \\
&= (((A \cup B) \cap (A \cap B)^c) \cup C)) \cap ((A \cap B^c) \cup (A^c \cap B))^c \cup C^c) \\
&= (A \cup B \cup C) \cap (A^c \cup B^c \cup C) \cap (((A \cap B^c)^c \cap (A^c \cap B)^c) \cup C^c) \\
&= (A \cup B \cup C) \cap (A^c \cup B^c \cup C) \cap ((A^c \cup B) \cap (A \cup B^c)) \cup C^c) \\
&= (A \cup B \cup C) \cap (A^c \cup B^c \cup C) \cap (A^c \cup B \cup C^c) \cap (A \cup B^c \cup C^c) \\
&= (B \cup C \cup A) \cap (B^c \cup C^c \cup A) \cap (B^c \cup C \cup A^c) \cap (B \cup C^c \cup A^c) \\
&= ((B \cup C \cup A) \cap (B^c \cup C^c \cup A)) \cap ((B^c \cup C) \cap (B \cup C^c)) \cup A^c) \\
&= ((B \cup C \cup A) \cap (B^c \cup C^c \cup A)) \cap (((B \cap C^c)^c \cap (B^c \cap C)^c) \cup A^c) \\
&= (((B \cup C) \cap (B \cap C)^c) \cup A)) \cap ((B \cap C^c) \cup (B^c \cap C))^c \cup A^c) \\
&= ((B\Delta C) \cup A) \cap ((B\Delta C)^c \cup A^c) \\
&= ((B\Delta C) \cup A) \cap ((B\Delta C) \cap A)^c \\
&= (B\Delta C)\Delta A \\
&= A\Delta(B\Delta C).
\end{aligned}$$

Inverse elements also exist; every subset of X is its own inverse. □

1.1.3 Matrix Groups

In linear algebra, matrices get into row echelon form by elementary row operations:

- Add a multilple of one row to another.
- Multiply a row by a nonzero scalar.
- Exchange two rows.

Elementary row operations on an $m \times n$ matrix can be expressed using left multiplication by an $m \times m$ matrix called an **elementary matrix**. These elementary matrices come in three flavors.

First we have $e_{ij}(a) = \exp(aE_{ij}) = I_n + aE_{ij}$. The effect of multiplying an $m \times n$ matrix A by $e_{ij}(\lambda)$ on the left is an elementary row operation:

$$e_{ij}(a)A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{i1} + aa_{j1} & \cdots & a_{in} + aa_{jn} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix},$$

and the effect of multiplying A by $e_{ij}(\lambda)$ on the right is an elementary column operation:

$$Ae_{ij}(a) = \begin{pmatrix} a_{11} & \cdots & a_{1j} + aa_{1i} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mj} + aa_{mi} & \cdots & a_{mn} \end{pmatrix}.$$

These elementary matrices satisfy the following relations, called the **Steinberg relations**:

$$\begin{aligned}
&e_{ij}(a)e_{ij}(b) = e_{ij}(a+b); \\
&e_{ij}(a)e_{jk}(b) = e_{ik}(ab)e_{jk}(b)e_{ij}(a), \quad \text{for } i \neq k; \\
&e_{ij}(a)e_{kl}(b) = e_{kl}(b)e_{ij}(a), \quad \text{for } i \neq l \text{ and } j \neq k.
\end{aligned}$$

It is useful to think of the second relation as, "you can move $e_{ij}(a)$ from the left to the right of $e_{jk}(b)$ at the cost of multiplying by an element $e_{ik}(ab)$". A similar interpretation can be given for the other relations.

Next we have $d_i(a)$, which has entries 1 on the main diagonal except for a nonzero $a \neq 1$ in the ith spot along the diagonal. The effect of multiplying an $m \times n$ matrix A by $d_i(a)$ on the left is an elementary row operation: multiply the ith row by a. The effect of multiplying an $m \times n$ matrix A by $d_i(a)$ on the right is an elementary column operation: multiply the ith column by a. These matrices together with the $e_{ij}(a)$'s satisfy the following relations:

$$\begin{aligned}
d_i(a)d_i(b) &= d_i(ab);\\
d_i(a)d_j(b) &= d_j(b)d_i(a);\\
d_i(a)e_{ij}(b) &= e_{ij}(ab)d_i(a);\\
e_{ij}(b)d_j(a) &= d_j(a)e_{ij}(ab).
\end{aligned}$$

It is useful to think of the third relation as "you can move $d_i(a)$ from the left to the right of $e_{ij}(b)$ at the cost of replacing $e_{ij}(b)$ with $e_{ij}(ab)$". A similar interpretation can be given for the other relations.

The last type of elementary matrix to discuss is s_{ij} with $i \neq j$, which is the matrix that has entry 1 in positions (i,j) and (j,i) and also in every diagonal position except the ith and jth, and 0's everywhere else. The effect of multiplying an $m \times n$ matrix A by s_{ij} on the left is an elementary row operation: swap the ith row and jth row. The effect of multiplying an $m \times n$ matrix A by s_{ij} on the right is an elementary column operation: swap the ith column and jth column. These matrices together with the $d_i(a)'s$ and $e_{ij}(b)'s$ satisfy the following relations

$$\begin{aligned}
s_{ij}^2 &= I;\\
s_{ij} &= s_{ji};\\
s_{ij}s_{jk}s_{ij} &= s_{jk}s_{ij}s_{jk};\\
s_{ij}s_{kl} &= s_{kl}s_{ij}, \quad \text{for } i \neq k \neq j \text{ and } i \neq l \neq j;\\
s_{ij}e_{kl}(a) &= e_{\sigma(k)\sigma(l)}(a)s_{ij}, \quad \sigma = (1,2);\\
s_{ij}d_j(a) &= d_{\sigma(j)}(a)s_{ij}, \quad \sigma = (1,2);
\end{aligned}$$

Example 1.3. Addition and multilpication are commutative on $\mathbb{R}$, but negation and division are not commutative on $\mathbb{R}$.

Example 1.4. Matrix multiplication is an associative binary operation which is not commutative: $e_{12}(a)e_{23}(b) = e_{23}(a)e_{12}(b)e_{13}(ab)$.

Example 1.5. Let $G = \{f : \mathbb{R} \to \mathbb{R}\}$. Composition $\circ$ of functions is an associative binary operation on G which is not commutative.

Example 1.6. Define $\star$ on $\mathbb{R}$ by $a \star b = \frac{a+b}{2}$. This is clearly commutative, however it is not associative since:

$$(a \star b) \star c = \frac{\frac{a+b}{2} + c}{2} = \frac{a+b+2c}{4}$$

$$a \star (b \star c) = \frac{a + \frac{b+c}{2}}{2} = \frac{2a+b+c}{4}$$

Definition 1.3. Let G be a nonempty set and let $\star$ be a binary operation on G. An **identity element** is an element $e \in G$ such that $a \star e = e \star a = a$ for all $a \in G$.

Example 1.7. Multiplication on $\mathbb{R} \setminus \{0\}$ has identity element $e = 1$. Every $a \in \mathbb{R}$ has an inverse, $\frac{1}{a}$.

Example 1.8. Let $\star$ be the binary operation $\mathbb{R} \setminus \{3\}$ be given by $a \star b = ab + 3a + 3b + 6 = (a+3)(b+3) - 3$. Let's verify that $\star$ really is a binary operation on $\mathbb{R} \setminus \{3\}$. For all $a, b \in \mathbb{R} \setminus \{-3\}$, we certainly have $a \star b \in \mathbb{R}$. If $a \star b = -3$, then

$$(a+3)(b+3) - 3 = -3 \quad \Longrightarrow \quad (a+3)(b+3) = 0 \quad \Longrightarrow \quad a = b = -3.$$

Thus, it is a binary operation on $\mathbb{R} \setminus \{-3\}$. Does $\star$ have an identity element? Does there exist $e \in \mathbb{R}$ such that $a \star e = e = e \star a$ for all $a \in \mathbb{R}$? In fact $e = -2$ works since $a \star e = (a-3)(-2+3) - 3 = a$. And since $\star$ is commutative, $a \star e = e \star a$. What about inverses? Given $a \in \mathbb{R}$, can we find a $b \in \mathbb{R}$ such that $a \star b = -2$? Suppose $a \star b = -2$.

$$(a+3)(b+3) - 3 = -2 \quad \Longrightarrow \quad (a+3)(b+3) = 1 \quad \Longrightarrow \quad (a+3)b = -3a - 8 \quad \Longrightarrow \quad b = \frac{-3a-8}{a+3}$$

So each element except -3, has an inverse. We have just proved that $(\mathbb{R} \setminus \{3\}, \star)$ is a group. Now we want to show that this group is actually isomorphic to $(\mathbb{R} \setminus \{0\}, \cdot\}$. The isomorphism $\varphi : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{3\}$ will be given by $a \mapsto a - 3$, where $a \in \mathbb{R} \setminus \{0\}$. We need to show $\varphi(ab) = \varphi(a) \star \varphi(b)$. The left side equals

$$\varphi(ab) = ab - 3.$$

The right side equals

$$\varphi(a) \star \varphi(b) = (a-3) \star (b-3) = ab - 3.$$

So this is a homomorphism. In fact, it is an isomorphism since φ is a bijection, with inverse $\phi : \mathbb{R} \setminus \{3\} \to \mathbb{R} \setminus \{0\}$ given by $a \mapsto a + 3$, where $a \in \mathbb{R} \setminus \{3\}$.

1.2 Group Homomorphisms

Definition 1.4. Let G and H be groups and let $\varphi \colon G \to H$ be a function. We say φ is a **group homomorphism** if it preserves the group operation, that is, if

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G$. We say φ is an **isomorphism** if there exists a group homomorphism $\psi \colon H \to G$ such that $\varphi\psi = 1_H$ and $\psi\varphi = 1_G$ where $1_G \colon G \to G$ and $1_H \colon H \to H$ are the identity maps. Equivalently, φ is an isomorphism if it is a group homomorphism and a bijection of the underlying sets. Indeed, if φ is a bijection, then φ^{-1} must be a group homomorphism too since for all $h_1, h_2 \in H$ we have

$$\begin{aligned}\varphi^{-1}(h_1 h_2) &= \varphi^{-1}(\varphi(\varphi^{-1}(h_1)))\varphi^{-1}(\varphi(\varphi^{-1}(h_2))) \\ &= \varphi^{-1}(h_1)\varphi^{-1}(h_2).\end{aligned}$$

If $\varphi \colon G \to H$ is an isomorphism, then we G and H are **isomorphic** to each other, and we denote this by $G \cong H$.

If we write "let $\varphi \colon G \to H$ be a group homomorphism" without first specifying what G and H are, then it is understood that G and H are groups. Also if we specify first that G and H are groups and we write "let $\varphi \colon G \to H$ be a homomorphism", then it is understood that φ is a *group* homomorphism. In all cases, everything should be clear from context.

1.2.1 Group Homomorphisms Sends Identities to Identities and Inverses to Inverses

Proposition 1.2. *Let $\varphi \colon G \to G'$ be a group homomorphism. Then we have the following:*

1. *The homomorphism preserves the identity element. In other words, $\varphi(1) = 1$.*
2. *The homomorphism preserves inverses. In other words, we have $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.*

Proof. 1. Observe that

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1). \tag{1}$$

Now we multiply both sides of (1) by $\varphi(1)^{-1}$ to get the desired result.

2. Let $g \in G$. Then we have

$$\begin{aligned}1 &= \varphi(1) \\ &= \varphi(gg^{-1}) \\ &= \varphi(g)\varphi(g^{-1}).\end{aligned}$$

It follows that $\varphi(g)^{-1} = \varphi(g^{-1})$. □

1.3 Examples of Group Homomorphisms

1.3.1 Determinant Homomorphism

Example 1.9. Let K be a field and let $n \in \mathbb{N}$. The determinant map $\det \colon \mathrm{GL}_n(K) \to K^\times$ is a homomorphism. Indeed, if $A, B \in \mathrm{GL}_n(K)$, then one learns from linear algebra that

$$\det(AB) = \det(A)\det(B).$$

1.3.2 Isomorphism from $\mathbb{R}$ to $\mathbb{R}^\times$

Example 1.10. The exponential map $\mathbb{R} \to \mathbb{R}^\times$, given by $x \mapsto e^x$, is an isomorphism. Indeed, for all $x, y \in \mathbb{R}$, we have

$$e^{x+y} = e^x e^y.$$

Furthemore, the exponential map is a bijection, with the logarithm map $\log\colon \mathbb{R}^\times \to \mathbb{R}$ being its inverse.

1.4 Subgroups

Definition 1.5. Let G be a group and let H be a nonempty subset of G. We say H is a **subgroup** of G, denoted $H \leq G$, if H forms a group under the group operation.

Thus if H is a subgroup of G, then $x, y \in H$ implies $xy \in H$. Similarly, $x \in H$ implies $x^{-1} \in H$. Note that these two conditions (together with the fact that H is nonempty) implies $1 \in H$. So H and G necessarily share the same identity. In fact, suppose that all we know is that H is just a subset of G. Then to see that H is a subgroup of G, we just need to check that $x, y \in H$ implies $xy^{-1} \in H$. Indeed, in this case, $x \in H$ implies $1 = xx^{-1} \in H$. Also $1, x \in H$ implies $x^{-1} = 1 \cdot x^{-1} \in H$. Finally, $x, y \in H$ implies $x, y^{-1} \in H$ which implies $xy = x(y^{-1})^{-1} \in H$. Let's use this test in the following example

Example 1.11. Let $G = \mathrm{GL}_2(\mathbb{R})$ and let $H = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \mid a \in \mathbb{R}^\times \right\}$. Clearly H is nonempty, so to see that H is a subgroup of G, we just need to check that $A, B \in H$ implies $AB^{-1} \in H$. So given $A = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} b & 0 \\ 0 & b \end{smallmatrix}\right)$ in H, we compute

$$\begin{aligned} AB^{-1} &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}^{-1} \\ &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b^{-1} & 0 \\ 0 & b^{-1} \end{pmatrix} \\ &= \begin{pmatrix} ab^{-1} & 0 \\ 0 & ab^{-1} \end{pmatrix} \\ &\in H. \end{aligned}$$

Thus H is a subgroup of G.

1.5 Quotient Groups and Homomorphisms

1.5.1 Normal Subgroups

Let G be a group and let $H \leq G$. Consider the relation $\sim$ on G:

$$a \sim b \quad \text{if} \quad a^{-1}b \in H$$

$\sim$ is an equivalence relation:

1. $\sim$ is reflexive: $a^{-1}a = e \in H \implies a \sim a, \forall a \in G$.
2. $\sim$ is symmetric: If $a^{-1}b \in H$, then $b^{-1}a = \left(a^{-1}b\right)^{-1} \in H$ since H is closed under inverses. Therefore $a \sim b$ if and only if $b \sim a$.
3. $\sim$ is transitive: Suppose $a \sim b$ and $b \sim c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$ implies $a^{-1}c = \left(a^{-1}b\right)\left(b^{-1}c\right) \in H$ since H is closed under products. Therefore $a \sim c$.

The equivalence class of $a \in G$ is

$$\{b \in G \mid a^{-1}b \in H\} = \{ah \mid h \in H\} = aH$$

aH is called the **left coset of H in G containing a**. We have

$$aH = bH \quad \text{if and only if} \quad a \sim b$$

The **right coset of H in G containing a** is given by

$$Ha = \{ha \mid h \in H\}$$

A subgroup H of G is **normal in G** if $aH = Ha$ for all $a \in G$. If H is normal in G, we write $H \trianglelefteq G$.

Example 1.12. $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$.

Example 1.13. If G is abelian then any subgroup H is normal in G.

Theorem 1.1. *Let $H \leq G$. Any left H-coset in G has a bijection with H. In particular, when H is finite, the cosets of H all have the same size as H.*

Proof. Pick a left coset, say gH. We can pass from gH to H by left multiplication by $g^{-1} : g^{-1}(gh) = h \in H$. Conversely, we can pass from H to gH by left multiplication by g. These functions from gH to H and vice versa are inverses to each other, showing gH and H are in bijection with each other. □

Definition 1.6. Let $H \leq G$. The **index** of H in G is the number of left cosets of H in G. This number, which is a positive integer or ∞, is denoted $[G : H]$.

Remark 2. The number of left cosets of H in G is equal to the number of right cosets of H in G. A bijection from is given by the inverse map:

$$aH \mapsto Ha^{-1}$$

Theorem 1.2. *Let $H \leq G$. The following statements are equivalent*

1. $H \trianglelefteq G$
2. $gHg^{-1} = H$ *for all* $g \in G$, *where* $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$
3. $N_G(H) = G$
4. $gHg^{-1} \subseteq H$ *for all* $g \in G$

Proof. $(1 \implies 2) : H \trianglelefteq G$ means $gH = Hg$ for all $g \in G$. Multiply both sides by g^{-1} (a bijection) to get $gHg^{-1} = Hgg^{-1} = H$. $(2 \implies 3) :$ Recall $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. By assumption, $gHg^{-1} = H$ for all $g \in G$, therefore $N_G(H) = G$. $(3 \implies 4) :$ By assumption $gHg^{-1} = H$ for all $g \in G$, therefore $gHg^{-1} \subseteq H$. $(4 \implies 1) :$ We need to show $gHg^{-1} \supseteq H$ for all $g \in G$. Suppose $h \in H$. Then $g^{-1}hg \in H$ by assumption. Then $h = gg^{-1}hgg^{-1} \in gHg^{-1}$.

□

Example 1.14. We show $SL_2(\mathbb{R}) \trianglelefteq GL_2(\mathbb{R})$. It suffices to check $MAM^{-1} \subseteq SL_2(\mathbb{R})$ for all $M \in GL_2(\mathbb{R})$ and $A \in SL_2(\mathbb{R})$. Given any such M and A,

$$\det(MAM^{-1}) = \det(M)\det(A)\det(M^{-1}) = \det(M)\det(M^{-1}) = \det(I) = 1$$

Therefore $MAM^{-1} \in SL_2(\mathbb{R})$.

1.5.2 Quotient Group

Let $H \leq G$. Define multiplication on the left cosets by

$$(aH)(bH) = abH$$

Check that this is well-defined iff $H \trianglelefteq G$.

Definition 1.7. Let G be a group and let $H \leq G$. Let

$$G/H = \{gH \mid g \in G\}$$

Define multiplication on G/H by

$$(aH)(bH) = abH$$

Proposition 1.3. *Multiplication of left cosets is well defined if and only if $H \trianglelefteq G$.*

Proof. Choose different coset representatives a' and b'. So $b' = bh_1$ and $a' = ah_2$. Then

$$(a'H)(b'H) = (ah_2H)(bh_1H) = aHbH = abH'H$$

If $H' = H$ for all $b \in G$, then H is normal.

□

$$HK = \{hk \mid h \in H, k \in K\}$$

Proposition 1.4. *If $H \trianglelefteq G$, then $G/H = \{gH \mid g \in G\}$ is a group with multiplication $\cdot$ being $(aH)(bH) = abH$ for all $a, b \in G$. We say G/H is the quotient group $G \mod H$.*

Proof. 1. Binary Operation: For all $a, b \in G$, abH is a left coset of H. So $\cdot$ is a binary operation defined on the set of left cosets of H.

2. Associativity: For all, $a, b, c \in G$, we have$((aH)(bH))(cH) = (abH)(cH) = ((ab)cH) = (a(bc)H) = (aH)(bcH) = (aH)((bH)(cH))$

3. Identity: For all $a \in G$, we have $(aH)(eH) = aeH = aH = eaH = (eH)(aH)$

4. Inverse: For all $a \in G$, we have $(aH)(a^{-1}H) = aa^{-1}H = eH = H = eH = a^{-1}aH = (a^{-1}H)(aH)$.

□

Example 1.15. Let $K = \langle(1,2,3)\rangle \trianglelefteq S_3$. Then $(1,2)K = \{(1,2),(2,3),(1,3)\}$, $(2,3)K = \{(2,3),(1,3),(1,2)\}$, and $(1,3)K = \{(1,3),(1,2),(2,3)\}$. So $(1,2)K = (2,3)K = (1,3)K$ and $()K = (1,2,3)K = (3,2,1)K$. So there are two elements in S_3/K, and they are represented by $\{()K, (1,2)K\}$. Let $\varphi : S_3/K \to \mathbb{Z}_2$ be given by $\varphi(()K) = \bar{0}$ and $\varphi((1,2)K) = \bar{1}$. Then φ is an isomorphism.

Remark 3. If G is abelian then G/H is abelian: $(aH)(bH) = abH = baH = (bH)(aH)$. If G is cyclic then G/H is cyclic: Suppose $G = \langle a\rangle$. Then $bH = a^nH = (aH)^n$. Therefore $G/H = \langle aH\rangle$.

What does it mean to say G/H is abelian. It means for all $a, b \in G$, $ab = \varphi(a,b)ba$ where $\varphi(a,b) \in H$. So we have a function $\varphi : G \times G \to H$. What can we say about this function φ? First of all, $ab = ba$ if and only if $\varphi(a,b) = e$ for all $a, b \in G$. Next

$$ab = \varphi(a,b)ba = \varphi(a,b)\varphi(b,a)ab$$

tells us $\varphi(a,b) = \varphi(b,a)^{-1}$. Next, associativity tells us

$$\varphi(a,b)\varphi(b,ac)acb = \varphi(a,b)bac = abc = a\varphi(b,c)cb = \varphi(a,\varphi(b,c))\varphi(b,c)acb \qquad \forall a,b,c \in G$$

So

$$a\varphi(b,c)a^{-1} = \varphi(a,\varphi(b,c))\varphi(b,c) = \varphi(a,b)\varphi(b,ac) \qquad \forall a,b,c \in G \tag{2}$$

.
And finally, the identity element e tells us

$$a\varphi(e,a) = ae\varphi(e,a) = ea = a = ae = ea\varphi(a,e) = a\varphi(a,e)$$

So

$$\varphi(a,e) = \varphi(e,a) = e \qquad \forall a \in G \tag{3}$$

Given $b, c \in G$, suppose $bc = cb$ or in other words $\varphi(b,c) = e$. Then using (2) and (3) we get

$$e = \varphi(a,b)\varphi(b,ac)$$

What we've been calling φ actually goes by a better name.

Definition 1.8. Given $a, b \in G$, the **commutator** $[a,b]$ of a and b is

$$[a,b] = aba^{-1}b^{-1}$$

Check that $ab = [a,b]ba$ so what we've been calling $\varphi(a,b)$ can also be thought of as $[a,b]$. Next, what does it mean to say G/H is cyclic? It means for every $b \in G$, $b = a^{\psi(b)}\varphi(b)$ where $\varphi(b) \in H$ and $\psi(b) \in \mathbb{Z}$. Now suppose H is abelian. Then

$$a^{\psi(b)+\psi(c)}\varphi(b)\varphi(c) = a^{\psi(b)}\varphi(b)a^{\psi(c)}\varphi(c) = bc = a^{\psi(bc)}\varphi(bc)$$

Example 1.16. If $G/Z(G)$ is cyclic, then G is abelian.

Theorem 1.3. *A subgroup H of G is normal in G if and only if H is the kernel of a group homomorphism.*

Proof. If $H \trianglelefteq G$ then $G/H = \{aH \mid a \in G\}$ is a group. Let $\pi : G \to G/H$ be given by $\pi(a) = aH$. π is a homomorphism: $\pi(ab) = abH = (aH)(bH) = \pi(a)\pi(b)$ for all $a, b \in G$. And $\mathrm{Ker}\pi = \{a \in G \mid \pi(a) = H\} = \{a \in G \mid aH = H\} = H$. Conversely, let $\varphi : G \to G'$ be a homomorphism. Then $a\mathrm{Ker}\varphi a^{-1} \subset \mathrm{Ker}\varphi$ since

$$\varphi(axa^{-1}) = \varphi(a)\varphi(x)\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = 1 \qquad \forall x \in \mathrm{Ker}\varphi$$

We also have $\mathrm{Ker}\varphi \subset a\mathrm{Ker}\varphi a^{-1}$ since $x = a(a^{-1}xa)a^{-1}$ for all $x \in \mathrm{Ker}\varphi$.

□

Example 1.17. $\det : (GL_n(\mathbb{R}), \cdot) \to (\mathbb{R} \setminus \{0\}, \cdot)$ is a homomorphism with $\mathrm{Ker}\det = SL_n(\mathbb{R})$, so $SL_n(\mathbb{R})$ is a normal subgroup in $GL_n(\mathbb{R})$

1.6 Cyclic Groups and Subgroups

Proposition 1.5. *Let G be a group with identity e and let $a \in G$. Then*

$$H = \{a^m \mid m \in \mathbb{Z}\}$$

*is a subgroup of G. H is the **cyclic subgroup** generated by a. Notation: $H = \langle a \rangle$.*

Proof. H is nonempty since $a \in H$. Suppose $b, c \in H$, then $b = a^i$ and $c = a^j$ for some $i, j \in \mathbb{Z}$. So $bc^{-1} = \left(a^i\right)\left(a^j\right)^{-1} = a^{i-j} \in H$. $\square$

Example 1.18. In $\mathbb{Z}$, $\langle 3 \rangle = \{3 \cdot m \mid m \in \mathbb{Z}\} = 3\mathbb{Z}$.

Example 1.19. In $\mathbb{Z}/10\mathbb{Z}$, $\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{0}\}$

Example 1.20. In S_3, $\langle (1,2,3) \rangle = \{(1,2,3), (1,3,2), 1\}$

Definition 1.9. A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$.

Example 1.21. $\mathbb{Z}$ is cyclic since $\mathbb{Z} = \langle 1 \rangle$.

Example 1.22. $\mathbb{Z}/m\mathbb{Z}$ is cyclic since $\mathbb{Z}/m\mathbb{Z} = \langle \bar{1} \rangle$.

Example 1.23. S_3 is not cyclic.

Example 1.24. $\mathbb{Q}$ is not cyclic: To obtain a contradiction, suppose $\langle \frac{a}{b} \rangle = \mathbb{Q}$. Then for any prime p, $\frac{1}{p} \in \langle \frac{a}{b} \rangle \implies \frac{1}{p} = n\frac{a}{b}$ for some $n \in \mathbb{Z}$. Thus $b = pma \implies p \mid b$ for any prime p which is a contradiction.

Proposition 1.6. *Let $H = \langle a \rangle$. Then $|H| = \text{ord}a$. More precisely:*

1. *If $\text{ord}a = m < \infty$ then $H = \{e, a, a^2, \ldots, a^{n-1}\}$*
2. *If $\text{ord}a = \infty$ then $a^k \neq a^\ell$ for $k, \ell \in \mathbb{Z}$ where $k \neq \ell$.*

Proposition 1.7. *Let $H = \langle a \rangle$ with $\text{ord}a = m < \infty$. Then $\text{ord}(a^k) = \frac{m}{\gcd(m,k)}$.*

Proof. Let $m = \text{ord}(a)$ and $d = \gcd(m, k)$. Then $m = dm'$, $k = dk'$, and $\gcd(m', k') = 1$. We need to prove that $\text{ord}(a^k) = \frac{m}{d} = m'$. We have $(a^k)^{m'} = a^{km'} = a^{\frac{km}{d}} = a^{k'm} = (a^m)^{k'} = e^{k'} = e$. So $\text{ord}(a^k) \mid m'$. Let $\text{ord}(a^k) = t$. Then $(a^k)^t = e \implies a^{kt} = e \implies m \mid kt \implies dm' \mid dk't \implies m' \mid k't \implies m' \mid t$. So $m' \mid \text{ord}(a^k)$. $\square$

Example 1.25. In $\mathbb{Z}/m\mathbb{Z}$, $\text{ord}(\bar{k}) = \frac{m}{\gcd(m,k)}$.

Corollary 1. *Let $H = \langle a \rangle$ with $\text{ord}a = m < \infty$. Then $\langle a^k \rangle = H$ if and only if $\gcd(m, k) = 1$.*

Exercise 1. Find the number of generators of $\mathbb{Z}/625\mathbb{Z}$.

Answer: $\varphi(625) = \varphi(5^4) = 5^4 - 5^3 = 500$.

Proposition 1.8. *Any two cyclic groups having the same order are isomorphic. More specifically:*

1. *If $\langle x \rangle$ and $\langle y \rangle$ both have order $m < \infty$, then $\varphi : \langle x \rangle \to \langle y \rangle$ given by $\varphi(x^k) = y^k$ is an isomorphism.*
2. *If $\langle x \rangle$ is an infinite cycle group, then $\psi : \mathbb{Z} \to \langle x \rangle$ given by $\psi(k) = x^k$ is an isomorphism.*

Theorem 1.4. *Every subgroup of a cyclic group $H = \langle x \rangle$ is still cyclic.*

Proof. Let $K \leq H$. If $K = \{e\}$, then $K = \langle e \rangle$. If $K \neq \{e\}$, then there exists $x^a \in K \setminus \{e\}$. Since K is a group, we can assume $a \in \mathbb{N}$. So $P = \{b \in \mathbb{N} \mid x^b \in K\} \neq \emptyset$. Let $d = \min P$. We will show $K = \langle x^d \rangle$. We have $\langle x^d \rangle \subseteq K$ since $x^{nd} \in K$. For the reverse inclusion, let $y \in K$. Since $K \leq \langle x \rangle$, we have $y = x^\ell$, for some integer ℓ. Now

$$\ell = gd + r \qquad \text{with } 0 \leq r \leq d - 1$$

So $y = x^{dg+r} = x^{dg}x^r$. If $r \neq 0$, then $x^r = x^{-dg}y \in K$, which is a contradiction since $d = \min P$.

$\square$

Corollary 2. *Let H be a cyclic group of order $m < \infty$. If $d \mid m$, then there exists a unique subgroup of H of order d.*

Proof. Let $H = \langle x \rangle$. We first prove existence. Recall

$$\operatorname{ord}(x^a) = \frac{\operatorname{ord}(x)}{\gcd(\operatorname{ord}(x), a)} = \frac{m}{\gcd(m, a)}$$

$d \mid m \implies m = dk$ and so

$$|\langle x^k \rangle| = \operatorname{ord}(x^k) = \frac{m}{\gcd(m, k)} = \frac{m}{k} = d$$

Now we prove uniqueness. Let $L \leq H$ such that $|L| = d$. Since $L \leq H$, $L = \langle x^t \rangle$ for some $t \in \mathbb{Z}$.

$$|L| = |\langle x^t \rangle| = \operatorname{ord}(x^t) = \frac{m}{\gcd(m, t)} = d = \frac{m}{k}$$

So $\gcd(m, t) = k$ implies $k \mid t$ which implies $t = ku$. Then $x^t = x^{ku} \in \langle x^k \rangle$. Thus $\langle x^t \rangle = L \subseteq \langle x^k \rangle$. Since $|L| = \langle x^k \rangle$ and $L \subseteq \langle x^k \rangle$, we must have $L = \langle x^k \rangle$. $\square$

Remark 4. The number of subgroups of a cyclic group of order m is equal to the number of divisors of m.

Exercise 2. Find all the subgroups of $\mathbb{Z}/12\mathbb{Z}$, giving a generator for each.

The number of subgroups of $\mathbb{Z}/12\mathbb{Z}$ is equal to the number of divisors of $12 = 2^2 \cdot 3$. If $m = p_1^{e_1} \cdots p_k^{e_k}$, then the number of divisors of m is $(e_1 + 1) \cdots (e_k + 1)$.

1.7 Subgroups generated by Subsets

Definition 1.10. Let G be a group. Let A be a nonempty subset of G. The subgroup of G **generated by** A is

$$\langle A \rangle = \bigcap_{A \subseteq K \leq G} K$$

Theorem 1.5. *Let G be a group. Let A be a nonempty subset of G. Let*

$$\bar{A} = \{a_1^{e_1} \cdots a_m^{e_m} \mid m \in \mathbb{N},\, a_i \in A,\, e_i = \pm 1,\, 1 \leq i \leq m\}$$

Then $\bar{A} = \langle A \rangle$.

Proof. First we note that $A \subseteq \bar{A}$ since for any $a \in A$, $a = a^1 \in \bar{A}$. Next we check that $\bar{A}$ is a subgroup of G. $\bar{A}$ is nonempty since $A \subseteq \bar{A}$. Let $a = a_1^{e_1} \cdots a_m^{e_m}$ and $b = b_1^{f_1} \cdots b_m^{f_m}$ be two elements in $\bar{A}$. Then $b^{-1} = b_m^{-f_m} \cdots b_1^{-f_1} \in \bar{A}$ and $ab = a_1^{e_1} \cdots a_m^{e_m} \cdot b_m^{-f_m} \cdots b_1^{-f_1} \in \bar{A}$. Since $\langle A \rangle$ is the smallest subgroup of G which contains A, we have $\langle A \rangle \subseteq \bar{A}$. For the reverse inclusion, suppose $a = a_1^{e_1} \cdots a_m^{e_m}$ and $A \subseteq K \leq G$. Then $a \in K$ since K is a subgroup of G which contains A. Therefore $\bar{A} \subseteq \langle A \rangle$. $\square$

Remark 5. If G is abelian, then $\langle A \rangle = \{a_1^{e_1} \cdots a_m^{e_m} \mid m \in \mathbb{N},\, a_i \in A,\, e_i \in \mathbb{Z},\, 1 \leq i \leq m\}$. Notice in this case the exponents can be any integer.

Example 1.26. In $\mathbb{Z}$,$\langle a, b \rangle = \{ma + kb \mid m, k \in \mathbb{Z}\}$. Since $\mathbb{Z}$ is cyclic, $\langle a, b \rangle = \langle d \rangle$ for some $d \in \mathbb{Z}$. In fact $d = \gcd(a, b)$. Proof: Since $d \mid a$ and $d \mid b$, we must have $da' = a$ and $db' = b$ for some $a', b' \in \mathbb{Z}$. Then for all $m, k \in \mathbb{Z}$, we have$ma + kb = ma'd + kb'd = (ma' + kb')d \in \langle d \rangle$. So $\langle a, b \rangle \subseteq \langle d \rangle$. For the reverse inclusion, note that $d = ax + by$ for some $x, y \in \mathbb{Z}$, therefore $\langle d \rangle = \langle ax + by \rangle \subseteq \langle a, b \rangle$.

Example 1.27. In S_m

1. $\langle A \rangle = S_m$ where $A = \{(1,2), (1,3), \ldots, (1,m)\}$.
2. $\langle B \rangle = S_m$ where $B = \{(1,2), (2,3), \ldots, (m-1,m)\}$.
3. $\langle C \rangle = S_m$ where $C = \{(1,2), (1,2,\ldots,m)\}$.

To prove (1), we first note that any $\sigma \in S_m$ is a product of transpositions. So it suffices to show that any transposition $(i,j) \in \langle A \rangle$. Since $(i,j) = (1,i)(1,j)(1,i)$, we have $(i,j) \in \langle A \rangle$. To prove (2), it suffices to show any transposition $(i,j) \in \langle B \rangle$. Without loss of generality, assume $i < j$. Since $(i,j) = (j-1,j) \cdots (i+1,i+2)(i,i+1)(i+1,i+2) \cdots (j-1,j)$, we have $(i,j) \in \langle B \rangle$. To prove (3), note that $(1,2,\ldots,m)^k(1,2)(m,m-1,\ldots,1)^k = (k,k+1)$. Thus $B \in \langle C \rangle$ which implies $\langle C \rangle = S_m$.

1.8 Order

Definition 1.11. Let G be a group and let $g \in G$. The **order** of g is the least natural number $n \in \mathbb{Z}_{\geq 1}$ such that $g^n = e$. If no such integer exists, we say g has infinite order. We sometimes denote the order of g by $\mathrm{ord}(g)$.

Remark 6. The order of an element can also be thought of as the size of the cyclic group generated by g.

Example 1.28. In the group $\mathbb{Z}$, every nonzero element has infinite order.

Example 1.29. In the group $\mathbb{C}^\times$, there are infinitely many elements which have finite order. The elements in $\mathbb{C}$ which have finite order are called the **roots of unity**. The set of all roots of unity is given by

$$T = \{e^{2\pi i r} \mid r \in \mathbb{Q}\}.$$

Lemma 1.6. *Suppose G is a finite group. Then every $g \in G$ has finite order.*

Proof. Consider the set $\{g^n \mid n \in \mathbb{Z}_{\geq 1}\}$. Since G is finite, we must have $g^m = g$ for some $m \in \mathbb{Z}_{\geq 1}$. This implies $g^{m-1} = 1$. □

Lemma 1.7. *Let $g \in G$ and let m be the order of g. If $g^n = e$, then $m \mid n$.*

Proof. First note that $m \leq n$ since m is the least natural number which kills g. Since $\mathbb{Z}$ is a Euclidean domain and $m \leq n$, there exists $k \in \mathbb{Z}_{\geq 1}$ and $0 \leq r < m$ such that $n = mk + r$. Assume for a contradiction that $r \neq 0$. Then we have

$$\begin{aligned} e &= g^n \\ &= g^{mk+r} \\ &= (g^m)^k g^r \\ &= g^r. \end{aligned}$$

This contradicts the fact that m is least natural number which kills g. So we must have $r = 0$ which implies $m \mid n$. □

1.8.1 Order of a Product of Two Elements

Proposition 1.9. *Let G be a group and let $g_1, g_2 \in G$ with orders m and n respectively. If g_1 and g_2 commute with one another and m is relatively prime to n, then the order of $g_1 g_2$ is mn.*

Proof. Let k be the order of $g_1 g_2$. First note that since g_1 and g_2 commute with each other, we have

$$\begin{aligned} (g_1 g_2)^{mn} &= g_1^{mn} g_2^{mn} \\ &= (g_1^m)^n (g_2^n)^m \\ &= e^n e^m \\ &= e. \end{aligned}$$

Therefore $k \mid mn$. On the other hand, since k is the order of $g_1 g_2$ and g_1 commutes with g_2, we have

$$e = g_1^k g_2^k. \tag{4}$$

Raising both sides of (4) to the nth power gives us $e = g_1^{kn}$. Therefore $m \mid kn$, and since m is relatively prime to n, this implies $m \mid k$. A similar calculation shows $n \mid k$. Since both m and n divide k, we must have $mn \mid k$. So since $k \mid mn$ and $mn \mid k$, we must have $mn = k$. □

Note that we need *both* g_1 to commute with g_2 *and* m to be relatively prime to n in order to conclude (1.9). In one of these conditions do not hold, then the conclusion of (1.9) may not hold.

Example 1.30. If g_1 and g_2 do not commute, then the result can fail. For example, in S_3, let $g_1 = (13)$ and $g_2 = (12)$. Then $g_1 g_2 = (13)(12) = (123)$ has order 3, but g_1 and g_2 both have order 2. Even if g_1 and g_2 commute, if their order is not relatively prime, the result can still fail. For example, in $\mathbb{Z}/12\mathbb{Z}$, the order of $\overline{2}$ is 6 and the order of $\overline{6}$ is 2. But the order of $\overline{2} + \overline{6} = \overline{8}$ is 3.

Proposition 1.10. *Let g_1 and g_2 be elements in a group G with orders n_1 and n_2 respectively. Suppose g_1 commutes with g_2 and $\mathrm{ord}(g_1 g_2) = n_1 n_2$. Then $(n_1, n_2) = 1$.*

Proof. Assume for a contradiction that $(n_1, n_2) \neq 1$. Denote $k = (n_1, n_2)$, so n_1/k Then n_1 and n_2 have a nontrivial factor

□

Suppose $\operatorname{ord}(g_1g_2) = mn$ and that is mn

Lemma 1.8. *Let m and n be positive integers. Denote $a = \gcd(m,n)$ and $b = \operatorname{lcm}(m,n)$. Then*

$$ab = mn.$$

Proof. We will show $a = mn/b$. Observe that $m \mid m(n/b)$ and $n \mid (m/b)n$. Therefore $a \mid mn/b$. Conversely, observe that $mn/a \mid m$ since $(mn/a)(a/n) = m$. Similarly, $mn/a \mid n$ since $(mn/a)(a/n) = n$. It follows that $b \mid mn/a$. In other words, $mn/b \mid a$. Since we have $a \mid mn/b$ and $mn/b \mid a$, it follows that $a = mn/b$. □

1.9 Normalizers and Centralizers

Definition 1.12. Let G be a group and let S be a subset of G.

1. The **centralizer** of S in G, denoted $\mathrm{C}_G(S)$, is the subgroup of G defined by

$$\mathrm{C}_G(S) = \{g \in G \mid gs = sg \text{ for all } s \in S\}.$$

2. The **normalizer** of S in G, denoted $\mathrm{N}_G(S)$, is the subgroup of G defined by

$$\mathrm{N}_G(S) = \{g \in G \mid gS = Sg\}.$$

Recall that $gS = Sg$ means that for each $g \in G$ and $s \in S$ there exists $s_g \in S$ such that $gs = s_g g$. In particular, we must have $s_g = gsg^{-1}$. Writing things this way makes it clear that $\mathrm{N}_G(S)$ is a group. For instance, given $g_1, g_2 \in G$ and $s \in S$, we have

$$\begin{aligned} g_1g_2s &= g_1s_{g_2}g_2 \\ &= (s_{g_2})_{g_1}g_1g_2 \\ &= s_{g_1g_2}g_1g_2 \end{aligned}$$

where $s_{g_1g_2} \in S$. This shows that $g_1g_2 \in \mathrm{N}_G(S)$. Note that the last equality follows from

$$\begin{aligned} (s_{g_2})_{g_1} &= g_1(g_2sg_2^{-1})g_1^{-1} \\ &= g_1g_2sg_2^{-1}g_1^{-1} \\ &= (g_1g_2)s(g_1g_2)^{-1} \\ &= s_{g_1g_2}. \end{aligned}$$

The reason why we had to switch g_1 and g_2 to get our notation to work is because conjugation doesn't behave well as a right action. On the other hand, conjugation does work as a left action. Indeed, if we had used the notation ${}_gs$ instead of s_g, then one can check that ${}_{g_1g_2}s =_{g_1} ({}_{g_2}s)$.

2 Basic Theorems

2.1 Lagrange's Theorem

Lemma 2.1. *Let G be a group and let $H \leq G$. Then $|H| = |gH|$ for all $g \in G$.*

Proof. The idea is that multiplying H by g on the left is an isomorphism since g^{-1} exists. □

Theorem 2.2. *(Lagrange's Theorem) Let G be a finite group. If $H \leq G$ then $|H|$ divides $|G|$.*

Proof. The set of left cosets of H form a partition of G into equal sized parts. □

Remark 7. 1. $|G| = |H|[G : H]$.

2. If $H \trianglelefteq G$ then $|G/H| = \frac{|G|}{|H|} = [G : H]$

Corollary 3. *If G is a finite group then $\operatorname{ord} a$ divides $|G|$ for any $a \in G$.*

Proof. Let $H = \langle a \rangle$. Then $|H| = \operatorname{ord} a$ and by Lagrange's Theorem $|H|$ divides $|G|$. □

Corollary 4. *If G is a finite group with $|G| = p$, then G is cyclic.*

Proof. Choose $a \in G \setminus \{e\}$. Then since $\operatorname{ord} a$ divides $|G| = p$ implies $\operatorname{ord} a = p$, we have $G = \langle a \rangle$. □

Example 2.1. Recall if $G/Z(G)$ is cyclic then G is abelian (Proof: $G/Z(G)$ is cyclic means $\exists g \in G$ such that for all $h, h' \in G$, $h = zg^n$ and $h' = z'g^{n'}$ for some $z, z' \in Z(G)$ and $n, n' \in \mathbb{Z}$. So $hh' = zg^n z' g^{n'} = zz'g^{n+n'} = zz'g^{n'+n} = z'g^{n'}zg^n = h'h$). If G is a finite group of order pq where both p and q are prime, then either $Z(G) = \{e\}$ or G is abelian. The possibilities for $|G/Z(G)|$ are $1, p, q$, or pq. If $|G/Z(G)| = 1, p$, or q, then $G/Z(G)$ is cyclic which implies G is abelian. If $|G/Z(G)| = pq$, then $Z(G) = \{e\}$.

Theorem 2.3. *(Cauchy's Theorem) Let G be a finite abelian group and let p be a prime. If $p \mid |G|$ then G has an element of order p.*

Proof. We prove by induction on $|G|$. The base case is $|G| = p$. In this case, $G = \langle a \rangle$ for some $a \in G$ and thus a has order p. Now let $x \in G \setminus \{e\}$. If $p | \text{ord}x$, then $\text{ord}x = pm$ and $\text{ord}(x^m) = p$. So assume p does not divide $\text{ord}x$. Let $N = \langle x \rangle$. Then $N \trianglelefteq G$ because G is abelian and $|G| = |N||G/N|$. Since p divides G but does not divide $|N|$, p divides $|G/N|$. Since $p||G/N|$ and $|G/N| < |G|$, then by the induction hypothesis there exists $yN \in G/N$ such that $\text{ord}(yN) = p$. Then $(yN)^p = y^pN = N$ and this implies $y^p = n$ for some $n \in N$. Since $\langle y^p \rangle \subset \langle y \rangle$ and the inclusion is strict, it follows that $\text{ord}(y^p) = \dfrac{\text{ord}y}{\text{gcd}(\text{ord}y,p)} < \text{ord}(y)$, which implies $1 < \text{gcd}(\text{ord}y, p)$. It follows that $\text{gcd}(\text{ord}y, p) = p$. So $p | \text{ord}y$. □

Alternate Proof: This part doesn't require the induction part. Let $G = \{g_1, \dots, g_n\}$ and $m = \text{lcm}(\text{ord}g_1, \dots, \text{ord}g_n)$. Assume no element in g has order p. Then p does not divide m. Construct homomorphism

$$\varphi : \mathbb{Z}^n_{(m)} \mapsto G, \qquad (\overline{a_1}, \dots, \overline{a_n}) \mapsto g_1^{a_1} \cdots g_n^{a_n}$$

This implies $|\text{Ker}\varphi||G| = m^n$. Since $p \mid |G|$, it must divide m^n, which implies it divides m, which is a contradiction.

2.2 The Isomorphism Theorems

2.2.1 First Isomorphism Theorem

Definition 2.1. Let $\varphi \colon G \to H$ be a group homomorphism.

1. The **kernel** of φ, denoted $\ker \varphi$, is defined to be the set
$$\ker \varphi := \{g \in G \mid \varphi(g) = 1\}.$$

2. The **image** of φ, denoted $\text{im}\, \varphi$, is defined to be the set
$$\text{im}\, \varphi := \{\varphi(g) \in H \mid g \in G\}.$$

Theorem 2.4. *Let G and H be groups and let $\varphi \colon G \to H$ be a group homomorphism. Then*

1. *The kernel of φ is a normal subgroup of G.*

2. *The image of φ is a subgroup of H and moreover we have the isomorphism $G/\ker \varphi \cong \text{im}\, \varphi$.*

Proof. 1. First let us check $\ker \varphi$ is a subgroup of G. It is nonempty since $\varphi(e) = e$ implies $e \in \ker \varphi$. Let $g_1, g_2 \in \ker \varphi$. Then observe that

$$\begin{aligned} \varphi(g_1 g_2^{-1}) &= \varphi(g_1)\varphi(g_2)^{-1} \\ &= ee \\ &= e \end{aligned}$$

implies $g_1 g_2^{-1} \in \ker \varphi$. It follows that $\ker \varphi$ is a subgroup of G.

Next, we check that $\ker \varphi$ is a normal subgroup of G. Let $g \in G$ and let $x \in \ker \varphi$. Then observe that

$$\begin{aligned} \varphi(gxg^{-1}) &= \varphi(g)\varphi(x)\varphi(g)^{-1} \\ &= \varphi(g)e\varphi(g)^{-1} \\ &= \varphi(g)\varphi(g)^{-1} \\ &= e \end{aligned}$$

implies $gxg^{-1} \in \ker \varphi$. It follows that $\ker \varphi$ is a normal subgroup of G.

2. First let us check $\operatorname{im}\varphi$ is a subgroup of H. It is nonempty since $\varphi(e) = e$ implies $e \in \operatorname{im}\varphi$. Let $\varphi(g_1), \varphi(g_2) \in \operatorname{im}\varphi$. Then observe that

$$\varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1 g_2^{-1})$$

implies $\varphi(g_1)\varphi(g_2)^{-1} \in \operatorname{im}\varphi$. It follows that $\operatorname{im}\varphi$ is a subgroup of H.

Next, we define $\overline{\varphi}\colon G/\ker\varphi \to \operatorname{im}\varphi$ by

$$\overline{\varphi}(\overline{g}) = \varphi(g) \tag{5}$$

for all $\overline{g} \in G/\ker\varphi$. We need to check that (5) is well-defined. Let gx be another coset representative of $\overline{g}$ (so $\varphi(x) = e$). Then

$$\begin{aligned}
\overline{\varphi}(\overline{gx}) &= \varphi(gx) \\
&= \varphi(g)\varphi(x) \\
&= \varphi(g)e \\
&= \varphi(g) \\
&= \overline{\varphi}(\overline{g}).
\end{aligned}$$

Thus (5) is well-defined. Now we show $\overline{\varphi}$ gives us an isomorphism from $G/\ker\varphi$ to $\operatorname{im}\varphi$. It is a group homomorphism since if $g_1, g_2 \in G$, then

$$\begin{aligned}
\overline{\varphi}(\overline{g}_1\overline{g}_2) &= \varphi(g_1 g_2) \\
&= \varphi(g_1)\varphi(g_2) \\
&= \overline{\varphi}(\overline{g}_1)\overline{\varphi}(\overline{g}_2).
\end{aligned}$$

It is also surjective since if $\varphi(g) \in \operatorname{im}\varphi$, then $\overline{\varphi}(\overline{g}) = \varphi(g)$. Finally, it is injective since

$$\begin{aligned}
\overline{\varphi}(\overline{g}) = e &\implies \varphi(g) = e \\
&\implies g \in \ker\varphi \\
&\implies \overline{g} = e.
\end{aligned}$$

Thus $\overline{\varphi}$ is in fact a group isomorphism. □

.

2.2.2 Second Isomorphism Theorem

Theorem 2.5. *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. Then the following hold:*

1. *The product HN is a subgroup of G.*
2. *The intersection $H \cap N$ is a normal subgroup of H.*
3. *The quotient groups $(HN)/N$ and $H/(H \cap N)$ are isomorphic.*

Proof. 1. First note that HN is nonempty since $e = ee \in HN$. Let $h_1n_1, h_2n_2 \in HN$. Then

$$\begin{aligned}
(h_1n_1)(h_2n_2)^{-1} &= h_1n_1n_2^{-1}h_2^{-1} \\
&= h_1(h_2^{-1}h_2)n_1n_2^{-1}h_2^{-1} \\
&= h_1h_2^{-1}(h_2n_1n_2^{-1}h_2^{-1}) \\
&\in HN.
\end{aligned}$$

It follows that HN is a subgroup of G.

2. Let us check that it is a subgroup of H first. It is nonempty since $e \in H \cap N$. Let $x, y \in H \cap N$. Then $xy^{-1} \in H \cap N$ also since both H and N are groups. Thus $H \cap N$ is a subgroup of H.

Now let us check that $H \cap N$ is a normal subgroup of H. Let $x \in H \cap N$ and let $h \in H$. Then $hxh^{-1} \in N$ since N is normal. Also $hxh^{-1} \in H$ since H is a group. Thus $hxh^{-1} \in H \cap N$. It follows that $H \cap N$ is a normal subgroup of H.

3. We shall define an isomorphism from $H/(H \cap N)$ to $(HN)/N$. To simplify notation in what follows, we denote by $\overline{h}$ to be the coset in $(HN)/N$ represented by $h \in H$ and we denote by $\underline{h}$ to be the coset in $H/(H \cap N)$ represented by $h \in H$. Define a map $\varphi\colon H/(H \cap N) \to (HN)/N$ by

$$\varphi(\underline{h}) = \overline{h} \tag{6}$$

for all cosets $\underline{h} \in H/(H \cap N)$. We need to check that (6) is well-defined (that is, does not depend on the coset representative). Suppose hx is another coset representative of $\underline{h}$ where $x \in H \cap N$. Then clearly hx is another coset representative of $\overline{h}$ since $x \in N$. Thus (6) is well-defined.

It is easy to see that φ is a group homomorphism. It is also surjective since every coset in $(HN)/N$ can be represented by an element in H (since $\overline{hn} = \overline{h}$ for all $h \in H$ and $n \in N$). Finally, let us check that φ is injective. Suppose $\underline{h} \in \ker \varphi$ (so $\overline{h} = \overline{e}$). This implies $h \in N$. Since $h \in H$ already, we see that $h \in H \cap N$. Thus $\underline{h} = \underline{e}$, which implies φ is injective. Thus φ is a group isomorphism, and we are done. □

Remark 8. Here's something to watch out for: It is tempting to define $\psi\colon (HN)/N \to H/(H \cap N)$ by

$$\psi(\overline{h}) = \underline{h} \tag{7}$$

for all cosets $\overline{h} \in HN/N$. While it is true that every coset in $(HN)/N$ can be represented by an $h \in H$, the definition of ψ in (7) does not make it clear what ψ is doing to a general coset representative of $(HN)/N$. One should instead define ψ by

$$\psi(\overline{hn}) = \underline{h} \tag{8}$$

for all cosets $\overline{hn} \in HN/N$. The definition of ψ in (6) makes it clear that we are chopping off the term which lies in N, unlike the definition of ψ in (7). When defining a map out of a quotient group, one should always describe how the map acts on a general coset representative, and then show that this map is well-defined by showing the map acts the same on another general coset representative which represents the same coset. Do not define a map out of a quotient group by describing how the map acts on a special coset representative!

2.2.3 Third Isomorphism Theorem

Theorem 2.6. *(The Third Isomorphism Theorem) Let $(G, \cdot)$ be a group. Let $H, K \trianglelefteq G$ such that $H \leq K$. Then*

$$(G/H)/(K/H) \cong G/K$$

Proof. Let $\varphi : G/H \to G/K$ be given by mapping $\varphi(aH) = aK$. To be sure this is well defined, suppose $aH = bH$. We want to show $\varphi(aH) = \varphi(bH)$ or $aK = bK$. Since $aH = bH$, then $b = ah$ where $h \in H \subset K$. This implies $b \in aK$, and therefore $bK = aK$. Next we check this is a homomorphism.

$$\begin{aligned}
\varphi(aHbH) &= \varphi(abH) \\
&= abK \\
&= aKbK \\
&= \varphi(aH)\varphi(bH)
\end{aligned}$$

By the first isomorhpism theorem, $(G/H)/\mathrm{Ker}\varphi \cong \varphi(G/H)$. So

$$\mathrm{Ker}\varphi = \{aH \in G/H \mid aK = K\} = \{aH \in G/H \mid a \in K\} = K/H$$

Also $\varphi(G/H) = G/K$ because for any $aK \in G/K$ we have $aK = \varphi(aH)$. □

Example 2.2. Let $H = 8\mathbb{Z}$, $K = 4\mathbb{Z}$. Then $H \trianglelefteq \mathbb{Z}$, $K \trianglelefteq \mathbb{Z}$ and $8\mathbb{Z} \leq 4\mathbb{Z}$. By the third isomorphism theorem, $(\mathbb{Z}/8\mathbb{Z})/(4\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$.

Proposition 2.1. *Let $(G, \cdot)$ be a group and let $H \trianglelefteq G$.*

1. *If $T \leq G/H$, then $T = A/H$ with $A \leq G$ such that $H \leq A$.*
2. *$A/H \trianglelefteq G/H$ if and only if $A \trianglelefteq G$.*

Proof. (1) : Let $A = \{a \in G \mid aH \in T\}$. We need to check that $A \leq G$ and $H \leq A$ and $A/H = T$. We have $e \in A$ because $eH \in T$. We have closure under multiplication because $a, b \in A$ implies $aH, bH \in T$, and since T is a group, we have $abH = (aH)(bH) \in T$ which implies $ab \in A$. Finally we check for inverses. $a \in A$ implies $aH \in T$. Since T is a group, aH has an inverse, namely $a^{-1}H$. This implies $a^{-1} \in A$. So $A \leq G$. Now if $x \in H$ then $xH = H \in T$, so $x \in A$. Thus $H \subset A$. Finally, we have $A/H = \{aH \mid a \in A\} = T$.

(2) : First assume $A/H \trianglelefteq G/H$. We need to show for all $g \in G$, we have $gAg^{-1} \subset A$. Let $g \in G$ and let $a \in A$. We know $gHaHg^{-1}H = gaHg^{-1}H = gag^{-1}H = a'H$. some $a' \in A$. Therefore $gAg^{-1} \subset A$. Thus $A \trianglelefteq G$. To prove the converse, assume $A \trianglelefteq G$. Then we want to show $gH(A/H)(gH)^{-1} \subset A/H$ for all $g \in G$. So let $g \in G$ and $a \in A$. We know that $gag^{-1} = a'$ for some $a' \in A$. Then $gHaH(gH)^{-1} = gag^{-1}H = a'H$. □

Example 2.3. All the subgroups of $\mathbb{Z}/10\mathbb{Z}$ are of the form $A/10\mathbb{Z}$ with $10\mathbb{Z} \leq A \leq \mathbb{Z}$. So any subgroup of $\mathbb{Z}/10\mathbb{Z}$ is of the form $d\mathbb{Z}/10\mathbb{Z}$ with $d|10$.

2.3 Cauchy's Theorem

Theorem 2.7. *Let G be a finite group and p be a prime factor of $|G|$. Then G contains an element of order p. Equivalently, G contains a subgroup of size p.*

We will use induction on $|G|$. Let $n = |G|$. The base case is $n = p$. In this case, any nonidentity element has order p. Now suppose $n > p$, $p|n$, and the theorem is true for all groups of order less than n and divisible by p.

Case 1: G is abelian. Assume no element of G has order p. If g has order kp for some $k \in \mathbb{N}$, then g^k has order p. Thus, no element has order divisible by p. Let $G = \{g_1, g_2, \ldots, g_n\}$ and let g_i have order m_i, so m_i is not divisible by p. Set m to be the least common multiple of the $m_i's$. Since $g_i^m = e$ for all $1 \leq i \leq n$, there exists a homomorphism of abelian groups $f : (\mathbb{Z}/(m))^n \to G$ given by $f(\overline{a_1}, \ldots, \overline{a_n}) = g_1^{a_1} \cdots g_r^{a_r}$. It is obviously surjective (for example, $f(\overline{1}, \overline{0}, \overline{0} \ldots, \overline{0}) = g_1$, $f(\overline{0}, \overline{1}, \overline{0} \ldots, \overline{0}) = g_2$, etc...), and so there is a short exact sequence given by:

$$1 \longrightarrow \ker f \longrightarrow (\mathbb{Z}/(m))^n \xrightarrow{f} G \longrightarrow 1$$

We deduce from this short exact sequence the equation

$$|\ker f| \cdot |G| = m^n$$

Since p divides $|G|$, it divides m^n too. But m^n is not divisible by p since m is not divisible by p, so we have reached a contradiction.

Case 2: G is nonabelian. If a proper subgroup H of G has order divisible by p, then by induction there is an element of order p in H, which gives us an element of order p in G. Thus we may assume no proper subgroup of G has order divisible by p. We will show $|Z(G)|$ is divisible by p, and hence $Z(G)$ can't be a proper subgroup of G, and the proof reduces to the abelian case. For any proper subgroup H, $|G| = |H| \cdot [G : H]$ and $|H|$ is not divisible by p, so $p|[G : H]$ for every proper subgroup H. Let the conjugacy classes in G with size greater than 1 be represented by $g_1, g_2, \ldots, g_k$. The conjugacy classes of size 1 are the elements in $Z(G)$. Since the conjugacy classes are a partition of G, counting $|G|$ by counting conjugacy classes implies

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : Z(g_i)]$$

where $Z(g_i)$ is the centralizer of g_i. Since the conjugacy class of each g_i has size greater than 1, $[G : Z(g_i)] > 1$, so $Z(g_i) \neq G$. Therefore $p|[G : Z(g_i)]$. The left side is divisible by p and each index in the sum on the right side is divisible by p, so $|Z(G)|$ is divisible by p. Since proper subgroups of G don't have order divisible by p, $Z(G)$ has to be all of G. That means G is abelian, which is a contradiction.

2.4 Sylow Theorems

Let G be a group such that $|G| = p^k m$ where p is a prime and $k, m \geq 1$. Cauchy's Theorem tells us that there exists a subgroup of G whose order is p. In fact, we can do much better than this. It turns out that there exists a subgroup of G whose order is p^i for all $1 \leq i \leq k$. This is part of the content of what the Sylow Theorems tells us.

2.4.1 p-Sylow Subgroups

Definition 2.2. Let G be a group such that $|G| = p^k m$ where p is a prime and $k, m \geq 1$. Any subgroup of G whose order is p^k is called a p-**Sylow subgroup** of G. A p-Sylow subgroup for some p is called a **Sylow subgroup**.

Example 2.4. In $\mathbb{Z}/(12)$, where $|\mathbb{Z}/(12)| = 12 = 2^2 \cdot 3$, the only 2-Sylow subgroup is $\{0, 3, 6, 9\} = \langle 3 \rangle$. The only 3-Sylow subgroup is $\{0, 4, 8\} = \langle 4 \rangle$.

Example 2.5. In A_4, where $|A_4| = 12 = 2^2 \cdot 3$. The only 2-Sylow subgroup is $V = \langle (12)(34), (14)(23) \rangle$. There are four 3-Sylow subgroups:

$$\langle (123) \rangle \quad \langle (124) \rangle \quad \langle (134) \rangle \quad \langle (234) \rangle$$

A_4 arises as the Galois group of $f(T) = T^4 + 8T + 12 = (T - r_1)(T - r_2)(T - r_3)(T - r_4)$ over $\mathbb{Q}$. Here's how we know this: The discriminant of $f(T)$ is $-3^3 \cdot 8^4 + 4^4 12^3 = 331776$, which is a square, so the Galois group is contained in A_4. Here's how $f(T)$ factors modulo different primes:

$$f(T) \equiv (T+1)(T^3 + 4T^2 + T + 2) \bmod 5$$
$$f(T) \equiv (T^2 + 4T + 7)(T^2 + 13T + 9) \bmod 17$$

From these factorizations, we know there is an element in the Galois group with cycle type $(1,3)$ (i.e. a 3-cycle) and an element in the Galois group with cycle type $(2,2)$. We can also see from these factorizations that $f(T)$ is irreducible over $\mathbb{Q}$ (There's no degree 2 factor mod 5, and there's no degree 1 factor mod 17). Since there exists a 3-cycle, we know the Galois group is divisible by 3. Since we know $f(T)$ has degree 4 and is irreducible over $\mathbb{Q}$, there is a sequence of field extensions

$$\begin{tikzcd}[arrows=dash] L \\ \mathbb{Q}(r_1) \arrow[u, "n"] \\ \mathbb{Q} \arrow[u, "4"] \end{tikzcd}$$

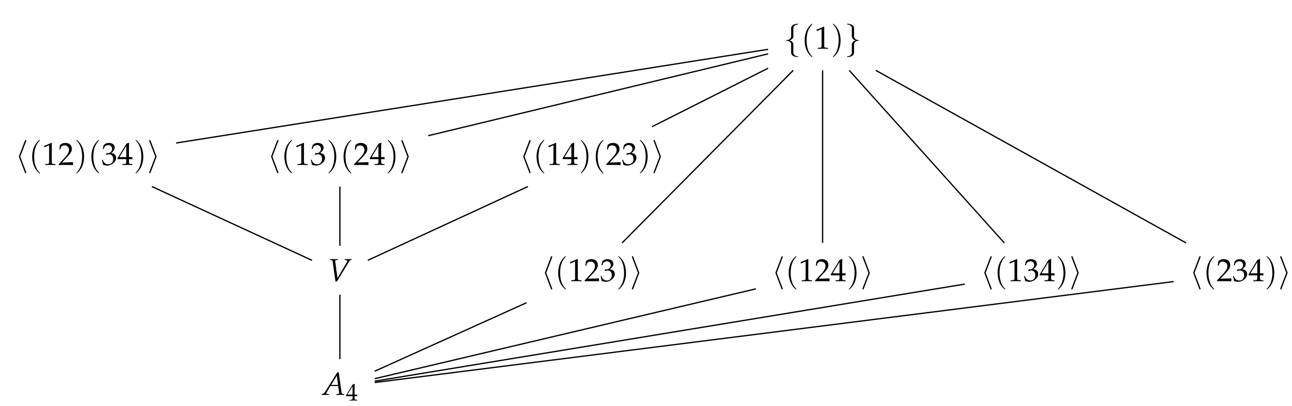
Where L is the splitting field of $f(T)$ and $\mathbb{Q}(r_1)$ has degree 4 Then as a field extension over $\mathbb{Q}$. This information tells us that $|Gal(L/\mathbb{Q})| = [L : \mathbb{Q}] = 4n$. Since the Galois group is divisible by 3 and 4, and is contained in A_4, it must be isomorphic to A_4. Since $|A_4| = 12$, $[L : \mathbb{Q}(r_1)] = 12/4 = 3$. So the set of all automorphisms of L that fix $\mathbb{Q}(r_1)$ must be a subgroup of A_4 which has order 3. This subgroup corresponds to one of the four 3-sylow subgroups, in particular, it is $\langle(234)\rangle$. Of course, I arbitrarily decided to focus on the field $\mathbb{Q}(r_1)$, but I could have easily focused on $\mathbb{Q}(r_2)$ instead. But this is just a relabeling of indices, and relabeling indices is the same as conjugating in S_4, so the corresponding Galois group for $\mathbb{Q}(r_2)$ is given by conjugating $\langle(234)\rangle$ with an element in A_4 that sends 1 to 2, like$(12)(34)$. The cubic resolvent of $f(T)$ is $T^3 - 48T - 64 = (T - (r_1r_2 + r_3r_4))(T - (r_1r_3 + r_2r_4))(T - (r_1r_4 + r_2r_3))$. The cubic resolvent of $f(T)$ is irreducible since it is irreducible mod 5. This means there is a sequence of field extensions

$$\begin{tikzcd}[arrows=dash] L \\ \mathbb{Q}(r_1r_2 + r_3r_4) \arrow[u, "n"] \\ \mathbb{Q} \arrow[u, "4"] \end{tikzcd}$$

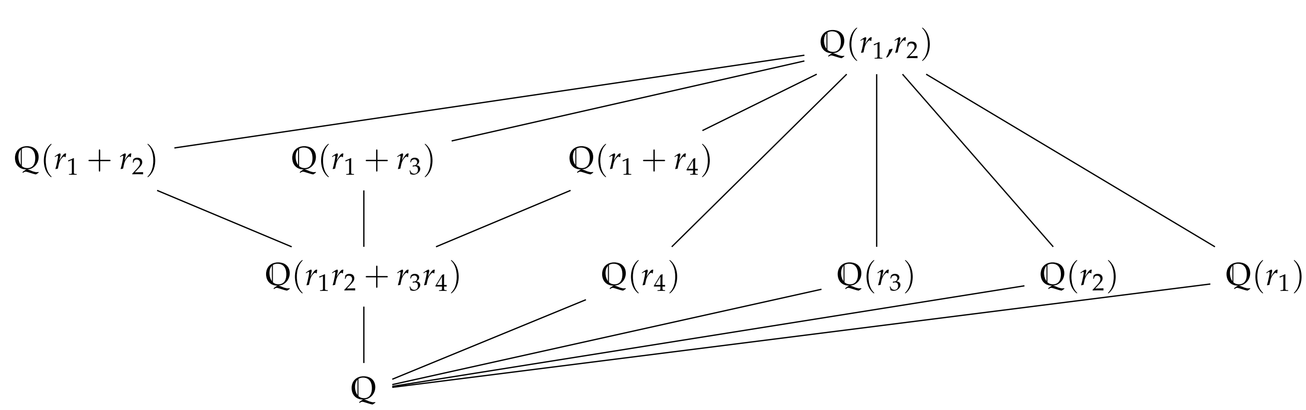
Again, we arbitrarily focused on the field $\mathbb{Q}(r_1r_2 + r_3r_4)$, but notice this time that the subgroup which corresponds to this field extension is normal in A_4, thus we get the nonobvious fact that:

$$\mathbb{Q}(r_1r_2 + r_3r_4) = \mathbb{Q}(r_1r_3 + r_2r_4) = \mathbb{Q}(r_1r_4 + r_2r_3)$$

Below is the lattice of subgroups of A_4:



And here is the corresponding lattice of fields:



Example 2.6. In D_6, where $|D_6| = 12 = 2^2 \cdot 3$, there are three 2-Sylow subgroups:

$$\{1, r^3, s, r^3 s\} = \langle r^3, s\rangle, \quad \{1, r^3, rs, r^4 s\} = \langle r^3, rs\rangle, \quad \{1, r^3, r^2 s, r^5 s\} = \langle r^3, r^2 s\rangle$$

The only 3-Sylow subgroup in D_6 is $\{1, r^2, r^4\} = \langle r^2\rangle$.

Example 2.7. In $\mathrm{SL}_2(\mathbb{Z}/3)$, where $|\mathrm{SL}_2(\mathbb{Z}/3)| = (3^2-1)(3^2-3)/2 = 2^3 \cdot 3$, there is only one 2-Sylow subgroup, whose elements are listed below:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$

Note that this subgroup is isomorphic to Q_8 by labeling the matrices in the first row as $1, i, j, k$. There are four 3-Sylow subgroups:

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} \right\rangle$$

2.4.2 Statement and Proof of Sylow Theorems

Before we state and prove the Sylow Theorems, we begin with a very important theorem called the fixed-point congruence.

Theorem 2.8. *Let G be a finite p-group acting on a finite set X. Then*

$$|X| = \sum_{i=1}^{t} |Orb_{x_i}|.$$

Since $|Orb_{x_i}| = [G : Stab_{x_i}]$ and $|G|$ is a power of p, $|Orb_{x_i}| \equiv 0 \bmod p$ unless $Stab_{x_i} = G$, in which case Orb_{x_i} has length 1, i.e. x_i is a fixed point. Thus, when we reduce both sides of the equation above modulo p, all terms on the right side vanish except for a contribution of 1 for each fixed point. That implies

$$|X| \equiv \#\{\text{fixed points}\} \bmod p$$

Now we state the first Sylow theorem.

Theorem 2.9. *(Sylow I). A finite group G has a p-Sylow subgroup for every prime p and any p-subgroup of G lies in a p-Sylow subgroup of G.*

Proof. Let p^k be the highest power of p in $|G|$. We can assume $k \geq 1$, since the result is obvious if $k = 0$, hence $p \mid |G|$. We will prove that there is a subgroup of order p^i for $0 \leq i \leq k$. If $|H| = p^i$ and $i < k$, we will show there is a p-subgroup $H' \supset H$ with $[H' : H] = p$, so $|H'| = p^{i+1}$. Then, starting with H as the trivial subgroup, we can repeat this process with H' in place of H to create a rising tower of subgroups

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots$$

where $|H_i| = p^i$, and after k steps we reach H_k, which is a p-Sylow subgroup of G. Consider the left multiplication action of H on the left cosets G/H:

$$h \cdot \overline{g} = \overline{hg}$$

This is an action of a finite p-group H on the set G/H, and so by the fixed-point congruence for actions of nontrivial p-groups

$$|G/H| \equiv |\mathrm{Fix}_H(G/H)| \bmod p \tag{9}$$

What does it mean for a coset $\overline{g}$ in G/H to be a fixed point by the group H under left multiplication? For all $h \in H$, we need $hg = gh'$, for some $h' \in H$. This happens if and only if $g \in \mathrm{N}(H)$. Thus

$$\mathrm{Fix}_H(G/H) = \{\overline{g} \mid g \in \mathrm{N}(H)\} = \mathrm{N}(H)/H.$$

So (9) becomes

$$[G : H] \equiv [\mathrm{N}(H) : H] \bmod p. \tag{10}$$

Note that H is a normal subgroup of $\mathrm{N}(H)$ and thus $\mathrm{N}(H)/H$ is a group. When $|H| = p^i$ and $i < k$, the index $[G : H]$ is divisible by p, so the congruence 10 implies $[\mathrm{N}(H) : H]$ is divisible by p, so $\mathrm{N}(H)/H$ is a group with order divisible by p. Thus $\mathrm{N}(H)/H$ has a subgroup of order p by Cauchy's theorem. All subgroups of the quotient group $\mathrm{N}(H)/H$ have the form H'/H where H' is a subgroup between H and $\mathrm{N}(H)$. Therefore a subgroup of order p in $\mathrm{N}(H)/H$ is H'/H such that $[H' : H] = p$, so $|H'| = p|H| = p^{i+1}$. $\square$

Theorem 2.10. *(Sylow II). For each prime p, the p-Sylow subgroups of G are conjugate.*

Proof. Pick two p-Sylow subgroups P and Q. We want to show they are conjugate. Consider the action of Q on G/P by left multiplication:

$$q \cdot \overline{g} = \overline{qg}$$

A fixed point $\overline{g}$ under this action means $\overline{qg} = \overline{g}$ for all $q \in Q$, in orther words for each $q \in Q$ there is a $p_q \in P$ such that $qg = gp_q$, or in other words, $q = gp_qg^{-1}$. This implies $Q \subseteq gPg^{-1}$, which further implies $Q = gPg^{-1}$ since Q and gPg^{-1} have the same size. So a fixed point under this action corresponds with an element g which conjugates Q to P. So we just need to show that there exists a fixed point in G/P. Since Q is a finite p-group, we have

$$|G/P| \equiv |\mathrm{Fix}_Q(G/P)| \bmod p$$

The left side is nonzero modulo p since P is a p-Sylow subgroup. Thus $|\mathrm{Fix}_Q(G/P)|$ can't be 0, so there is a fixed point in G/P. □

If g conjugates P to Q, then so too does gh, for any $h \in N(P)$:

$$ghPh^{-1}g^{-1} = gPg^{-1} = Q$$

It's natural to wonder if the number of p-Sylow subgroups of G equals $[G : N(P)]$. This is indeed true, but before we tackle that, we prove the third Sylow theorem.

Theorem 2.11. *(Sylow III). For each prime p, let n_p be the number of p-Sylow subgroups of G. Write $|G| = p^k m$, where p doesn't divide m. Then*

$$n_p \equiv 1 \bmod p \qquad \textit{and} \qquad n_p \mid m.$$

Proof. We will prove $n_p \equiv 1 \bmod p$ and then $n_p \mid m$. To show $n_p \equiv 1 \bmod p$, consider the action of P on the set $\mathrm{Syl}_p(G)$ by conjugation:

$$P \cdot Q = PQP^{-1}.$$

The size of $\mathrm{Syl}_p(G)$ is n_p. Since P is a finite p-group

$$n_p \equiv |\mathrm{Fix}_P(\mathrm{Syl}_p(G))| \bmod p$$

Fixed points for P acting by conjugation on $\mathrm{Syl}_p(G)$ are $Q \in \mathrm{Syl}_p(G)$ such that $gQg^{-1} = Q$ for all $g \in P$. One choice for Q is P. For any such Q, we have $P \subseteq \mathrm{N}_G(Q)$. Also $Q \subseteq \mathrm{N}_G(Q)$, so P and Q are p-Sylow subgroups in $\mathrm{N}_G(Q)$. Applying Sylow II to the group $\mathrm{N}_G(Q)$, we see that P and Q are conjugate in $\mathrm{N}_G(Q)$. Since Q is a normal subgroup of $\mathrm{N}_G(Q)$, the only subgroup of $\mathrm{N}_Q(Q)$ conjugate to Q is Q, so $P = Q$. Thus P is the only fixed point when P acts on $\mathrm{Syl}_p(G)$, so $n_p \equiv 1 \bmod p$. To show $n_p \mid m$, consider the action of G by conjugation on $\mathrm{Syl}_p(G)$. Since the p-Sylow subgroups are conjugate to each other, there is one orbit. A set on which a group acts with one orbit has size dividing the size of the group, so $n_p \mid |G|$ From $n_p \equiv 1 \bmod p$, the number n_p is relatively prime to p, so $n_p \mid m$. □

Theorem 2.12. *(Sylow III*). For each prime p, let n_p be the number of p-Sylow subgroups of G. Then $n_p = [G : \mathrm{N}_G(P)]$, where P is any p-Sylow subgroup.*

Proof. Let P be a p-Sylow subgroup of G and let G act on $\mathrm{Syl}_p(G)$ by conjugation. By the orbit-stabilizer formula,

$$n_p = [G : \mathrm{Stab}_{\{P\}}] = [G : \mathrm{N}_G(P)].$$

□

2.5 Sylow Applications

Theorem 2.13. *For a prime p, any element of $GL_2(\mathbb{Z}/(p))$ with order p is conjugate to a strictly upper-triangular matrix $e_{12}(a)$. The number of p-Sylow subgroups is $p+1$.*

Proof. The size of $GL_2(\mathbb{Z}/(p))$ is $(p^2-1)(p^2-p) = p(p-1)(p^2-1)$. Therefore a p-Sylow subgroup has size p. The matrix $e_{12}(1)$ has order p, so it generates a p-Sylow subgroup $P = \{e_{12}(*)\}$. Since all p-Sylow subgroups are conjugate, any matrix with order p is conjugate to some power $e_{12}(1)$. The number of p-Sylow subgroups is

$$n_p = [GL_2(\mathbb{Z}/(p)) : N(P)]$$

by Sylow III*. For $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to lie in $N(P)$ means it conjugates $e_{12}(1)$ to some power $e_{12}(*)$. Since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{\Delta} \begin{pmatrix} 1 - ac & a^2 \\ -c^2 & 1 + ac \end{pmatrix}$$

where $\Delta = ad - bc \neq 0$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in N(P)$ precisely when $c = 0$. Therefore $N(P) = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ in $GL_2(\mathbb{Z}/(p))$. The size of $N(P)$ is $(p-1)^2 p$, thus

$$n_p = [GL_2(\mathbb{Z}/(p)) : N(P)] = p + 1$$

□

Corollary 5. *The number of elements of order p in $GL_2(\mathbb{Z}/(p))$ is $p^2 - 1$.*

Proof. Each p-Sylow subgroup has $p - 1$ elements of order p. Different p-Sylow subgroups intersect trivially, so the number of elements of order p is $(p-1)n_p = p^2 - 1$.

□

Theorem 2.14. *There is a unique p-Sylow subgroup of $Aff(\mathbb{Z}/(p^2))$.*

Proof. $Aff(\mathbb{Z}/(p^2))$ has size $p^2\varphi(p^2) = p^3(p-1)$, so a p-Sylow subgroup has order p^3. Letting n_p be the number of p-Sylow subgroups, Sylow III says $n_p | (p-1)$ and $n_p \equiv 1 \mod p$. Therefore $n_p = 1$.

□

Theorem 2.15. *For any prime p, $Heis(\mathbb{Z}/(p))$ is the unique p-Sylow subgroup of the group of invertible upper-triangular matrices*

$$\begin{pmatrix} d_1 & a & b \\ 0 & d_2 & c \\ 0 & 0 & d_3 \end{pmatrix}$$

in $GL_3(\mathbb{Z}/(3))$.

Proof. This matrix group, call it U, has size $(p-1)^3 p^3$, so $Heis(\mathbb{Z}/(p))$ is a p-Sylow subgroup of U. Sylow III tells us $n_p | (p-1)^3$ and $n_p \equiv 1 \mod p$, but it does not follow from this that n_p must be 1. Let's prove $Heis(\mathbb{Z}/(p)) \lhd U$ by showing it is in the kernel of a map out of U: Project a matrix in U to the 3-fold product $(\mathbb{Z}/(p))^\times \times (\mathbb{Z}/(p))^\times \times (\mathbb{Z}/(p))^\times$.

$$\begin{pmatrix} d_1 & a & b \\ 0 & d_2 & c \\ 0 & 0 & d_3 \end{pmatrix} \mapsto (d_1, d_2, d_3)$$

The kernel of this map is $Heis(\mathbb{Z}/(p))$.

□

2.6 Cayley's Theorem

Theorem 2.16. *(Cayley's Theorem) Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.*

Proof. We write S_G for the group of all permutations of G as a set. We have $S_G \cong S_n$, so we just need to show that G is isomorphic to a subgroup of S_G. Define a map $\pi \colon G \to S_G$, denoted $\pi \mapsto \pi_g$, where $\pi_g \colon G \to G$ is given by

$$\pi_g(x) = gx$$

for all $x \in G$. We claim that π is an injective group homomorphism. Indeed, first let us show that it is a group homomorphism. Let $g_1, g_2 \in G$. Then observe that

$$\begin{aligned} \pi_{g_1 g_2}(x) &= g_1 g_2 x \\ &= \pi_{g_1}(g_2 x) \\ &= \pi_{g_1}\pi_{g_2}(x) \end{aligned}$$

for all $x \in G$. It follows that $\pi_{g_1 g_2} = \pi_{g_1}\pi_{g_2}$, and hence π is a group homomorphism. Now let us show that it is injective. Suppose $g \in \ker \pi$. Thus $gx = x$ for all $x \in G$. In particular, $g^2 = g$. Multiplying both sides by g^{-1} implies $g = 1$. Thus $\ker \pi = \{1\}$, which implies π is injective. Finally, by the first isomorphism theorem for groups, we find that $\operatorname{im} \pi$ is a subgroup of S_G, and moreover,

$$\operatorname{im} \pi \cong G / \ker \pi \cong G.$$

It follows that G is isomorphic to a subgroup of S_G which implies G is isomorphic to a subgroup of S_n. □

Theorem 2.17. *Let G be a finite p-group. Then* $\operatorname{Aut} G$ *is isomorphic to a subgroup of a tree automorphism group.*

Proof. Let $T_0 = \{1\}$ and for each $n \geq 1$ let $T_n = \{\text{elements in } G \text{ of order } p^n\}$. Also for each $n \geq 1$, define $f_n \colon G \to G$ by

$$f_n(x) = x^p$$

for all $x \in G$. Then $T = (T_n, f_n)$ has the structure of a tree in G such that

$$G = \bigcup_{n=1}^{\infty} T_n.$$

Furthermore, if $\sigma \in \operatorname{Aut} G$, then observe that σ induces a tree automorphism of T. Indeed, suppose $x \in T_n$ and $y \in T_{n+1}$ such that

$$y^p = x. \tag{11}$$

Then note that $\sigma(y) \in T_{n+1}$ since σ preserves the order of an element, and applying σ to both sides of (11) shows

$$\sigma(y)^p = \sigma(x).$$

It follows that σ induces a tree automorphism of T. □

2.7 Semidirect Product

Let N and H be two groups and let $\varphi \colon H \to \operatorname{Aut} N$ be a group homomorphism. We define the **outer semidirect product** of N and H with respect to φ, denoted $N \rtimes_\varphi H$, to be the group whose underlying set is $N \times H$ and whose multiplication is defined by

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2)$$

for all $h_1, h_2 \in H$ and $n_1, n_2 \in N$. We often simplify notation by writing elements in $N \times_\varphi H$ by nh instead of (n, h). Furthermore, if the action φ is understood from context, then we simplify notation further by writing $h \cdot n$ instead of $\varphi_h(n)$. In this case, multiplication looks like:

$$(n_1 h_1)(n_2 h_2) = (n_1 (h_1 \cdot n_2))(h_1 h_2).$$

2.8 Wreath Product

Let A and H be groups and let Ω be a set with H acting on it (from the left). Let K be the direct product

$$K = \prod_{\omega \in \Omega} A_\omega$$

of copies of $A_\omega = A$ indexed by the set Ω. The elements of K can be seen as arbitrary sequences (a_ω) of elements of A indexed by Ω with component-wise multiplication. Then the action of H on Ω extends in a natural way to an action of H on the group K by

$$h(a_\omega) = (a_{h^{-1}\omega}).$$

The **unrestricted wreath product** $A \operatorname{Wr}_\Omega H$ of A by H with respect to φ is the semidirect product $K \rtimes H$. If action of H on Ω is understood from context, then we simplify our notation by writing $A \wr H$ instead of $A \operatorname{Wr}_\Omega H$. The subgroup K of $A \operatorname{Wr}_\Omega H$ is called the **base** of the wreath product.

Example 2.8. Let G and H be finite groups. When we write $G \wr H$, then it is understood that this is the unrestricted wreath product of G by H with respect to $\mathrm{m} \colon H \to \operatorname{Aut} H$, denoted $h \mapsto \mathrm{m}_h$, where m_h is just multiplication by h:

$$\mathrm{m}_h(x) = hx$$

for all $x \in H$. Let us understand what $G \wr H$ looks like. Every element in $G \wr H$ has the form

$$(g_x)h$$

where $(g_x) = (g_x)_{x \in H}$ is a sequence in G indexed by H and where $h \in H$. Multiplicaiton $G \wr H$ is defined by

$$h(g_x) = (g_{h^{-1}x})h.$$

We have a short exact sequence of groups

$$1 \to \prod_{x \in H} G_x \to G \wr H \to H \to 1.$$

If $|G| = n$ and $|H| = m$, then this tells us, in particular, that

$$|G \wr H| = |H||G|^{|H|} = mn^m.$$

Now suppose we have three finite groups G_1, G_2, and G_3 of orders n_1, n_2, and n_3 respectively. Then on the one hand, we have

$$\begin{aligned}|(G_3 \wr G_2) \wr G_1| &= n_1 |G_3 \wr G_2|^{n_1} \\ &= n_1 (n_2 n_3^{n_2})^{n_1} \\ &= n_1 n_2^{n_1} n_3^{n_1 n_2}.\end{aligned}$$

On the other hand, we have

$$\begin{aligned}|G_3 \wr (G_2 \wr G_1)| &= |(G_2 \wr G_1)| n_3^{|(G_2 \wr G_1)|} \\ &= n_1 n_2^{n_1} n_3^{(n_1 n_2^{n_1})} \\ &= n_1 n_2^{n_1} n_3^{n_1 n_2^{n_1}}.\end{aligned}$$

Thus clearly the wreath product need not be associative (up to isomorphism).

2.9 Composition Series and the Hölder program

Definition 2.3. A group G is said to be **simple** if $|G| > 1$ and if its only normal subgroups are $\{e\}$ and G itself.

Example 2.9. Let p be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is simple. By lagrange's theorem, the order of any subgroup of $\mathbb{Z}/p\mathbb{Z}$ must divide p. So we only have two options for subgroups of $\mathbb{Z}/p\mathbb{Z}$: $\{e\}$ and $\mathbb{Z}/p\mathbb{Z}$.

The Hölder program initiated the classification all finite simple groups, which was accomplished in the 1980s.

Theorem 2.18. *There are* 18 *families of finite simples groups, and* 26 *sporadic finite simple groups.*

Example 2.10. $\{\mathbb{Z}_p \mid p \text{ prime}\}$ and $\{\mathrm{PSL}_m(\mathbb{F}_p) \mid m \geq 2\}$

Definition 2.4. In a group G a sequence of subgroups

$$1 = H_0 \leq H_1 \leq \cdots \leq H_r = G$$

is called a **composition series** if $H_i \trianglelefteq H_{i+1}$ and H_{i+1}/H_i is simple for all $i \in \{0, \ldots, r-1\}$. The groups H_{i+1}/H_i are called the **composition factors**.

Example 2.11. A composition series for S_3 is

$$1 \trianglelefteq \langle (1,2,3) \rangle \trianglelefteq S_3,$$

with composition factors $\mathbb{Z}_3$ and $\mathbb{Z}_2$.

Example 2.12. A composition series for S_4 is

$$\{(1)\} \trianglelefteq U \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4,$$

where $V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ and $U = \{(1), (1,2)(3,4)\}$, and three factors being C_2 and one factor being C_3.

Theorem 2.19. *Let G be a finite group. Then G has a composition series*

$$1 = H_0 \leq H_1 \leq \cdots \leq H_r = G,$$

and the composition factors are unique up to isomorphism, i.e. if

$$1 = G_0 \leq G_1 \leq \cdots \leq G_s = G$$

is another composition series of G, then $r = s$ and there exists $\pi \in S_r$ such that $G_{i+1}/G_i \cong H_{\pi(i)+1}/H_{\pi(i)}$.

Proof. We can always construct a normal series of G. Let r be the length of the longest such sequence. We need to check that this is a composition series (i.e. H_{i+1}/H_i is simple for all i). Suppose not: there is a some i such that H_{i+1}/H_i is not simple. Then there exists $N \trianglelefteq H_{i+1}/H_i$ such that $N \neq H_i/H_i$ and $N \neq H_{i+1}/H_i$. But then $N = A/H_i$ with $H_i \trianglelefteq A \trianglelefteq H_{i+1}$. So we have a sequence of subgroups of G

$$1 = H_0 \leq H_1 \leq \cdots \leq H_i \leq A \leq H_{i+1} \cdots \leq H_r = G.$$

which is a contradiction because this has length $r+1$.

Lemma: Let G be a finite group. If $M \trianglelefteq G$, $N \trianglelefteq G$, with $M \neq N$ and both G/M and G/N are simple groups, then $G/M \cong N/M \cap N$ and $G/N \cong M/M \cap N$. Now we prove the second part of the theorem using induction on $|G|$. If $|G| = 1$ then $G = \{1\}$. Assume the statement is true for all groups of order less than $|G|$. Let $M = G_{s-1}$ and $N = H_{r-1}$. If $M = N$, then use the induction hypothesis to show $r-1 = s-1$ $(H_1/H_0, \cdots, H_{r-1}/H_{r-2}) \sim (G_1/G_0, \cdots, G_{s-1}/G_{s-2})$. So assume $M \neq N$, then use the lemma. Let $K = M \cap N$. Consider a composition series for K:

$$1 = K_0 \leq K_1 \leq \cdots \leq K_{t-1} \leq K_t = K$$

Composition series for M

$$1 = G_0 \leq G_1 \leq \cdots \leq G_{s-3} \leq G_{s-2} \leq M$$

$$1 = K_0 \leq K_1 \leq \cdots \leq K_{t-1} \leq K \leq M$$

So $(G_1/G_0, \cdots, G_{s-2}/G_{s-3}, M/G_{s-2}) \sim (K_1/K_0, \cdots, K/K_{t-1}, M/K)$ and

□

Serre

Definition 2.5. Let G be a group.

1. A **filtration** of G is a finite sequence of subgroups $(G_i)_{0 \leq i \leq n}$ of G such that

$$G_0 = G \supset G_1 \supset \cdots \supset G_n = 1 \tag{12}$$

   with G_{i+1} normal in G_i for $0 \leq i \leq n-1$. Given a filtration $(G_i)_{0 \leq i \leq n}$, the successive quotients G_i/G_{i+1} are denoted $\mathrm{gr}_i(G)$. The sequence of the $\mathrm{gr}_i(G)$ is denoted by $\mathrm{gr}(G)$.

2. A filtration $(G_i)_{0 \leq i \leq n}$ of G is called a **Joran-Hölder filtration** (or a **Joran-Hölder series** or a **composition series**) if $\mathrm{gr}_i(G)$ is simple all $0 \leq i < n$. The number n is called the **length** of the filtration.

Example 2.13. Let F be a field. A filtration for the group $\mathrm{Aff}(F)$ is given by

$$\mathrm{Aff}(F) \trianglerighteq \{e_{12}(*)\} \trianglerighteq \{1\},$$

with factors isomorphic to F and $F^\times$. Compare this with the following sequence of field extensions:

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[5]{2}, \zeta_5) \arrow[d, dash, "\mathbb{F}_5"] \arrow[d, bend right, dash, "e_{12}(*)"'] \arrow[dd, bend left, dash, "\mathrm{Aff}(\mathbb{F}_5)"] \\
\mathbb{Q}(\zeta_5) \arrow[d, dash, "\mathbb{F}_5^\times"] \\
\mathbb{Q}
\end{tikzcd}$$

Example 2.14. A composition series for S_4 is

$$S_4 \trianglerighteq A_4 \trianglerighteq V \trianglerighteq U \trianglerighteq \{(1)\},$$

where $V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ and $U = \{(1), (1,2)(3,4)\}$, with three factors being C_2 and one factor being C_3. Compare this with the following sequence of field extensions:

$$\begin{tikzcd}
\mathbb{Q}(r_1) \arrow[d, dash, "C_2"] \arrow[d, dash, bend right, "U"'] \arrow[dd, dash, bend left, "V"] \arrow[ddd, dash, bend right=60, "A_4"'] \arrow[dddd, dash, bend left=60, "S_4"] \\
\mathbb{Q}(r_1+r_2) \arrow[d, dash, "C_2"] \\
\mathbb{Q}(r_1r_2+r_3r_4) \arrow[d, dash, "C_3"] \\
\mathbb{Q}(\prod_{i<j}(r_i-r_j)) \arrow[d, dash, "C_2"] \\
\mathbb{Q}
\end{tikzcd}$$

where r_1, r_2, r_3 and r_4 are roots of the polynomial $f(x) = x^4 - x - 1$.

Example 2.15. A composition series for D_4 is

$$D_4 \trianglerighteq \langle r^2, s\rangle \trianglerighteq \langle s\rangle \trianglerighteq \langle 1\rangle,$$

with all three factors being C_2.

2.9.1 Every Finite Group has a Jordan-Hölder Filtration

A group need not have a Jordan-Hölder filtration. Indeed, consider the group of integers $\mathbb{Z}$. It turns out that however, that finite groups always have Jordan-Hölder filtrations.

Proposition 2.2. *Let G be a finite group. Then there exists a Jordan-Hölder filtration of G.*

Proof. If $G = 1$, take the trivial Jordan-Hölder filtration with $n = 0$ in (12). If G is simple, take $n = 1$ in (12). Suppose G is neither 1 nor simple. Use induction on the order of G. Let N be a normal subgroup of G , distinct from G, and of maximal order. Then G/N is simple. Since $|N| < |G|$, we apply the induction hypothesis to N and we obtain a Jordan-Hölder filtration $(N_i)_{0\le i\le n}$ for N. Then $(G_i)_{0\le i\le n+1}$ is a Jordan-Hölder filtration for G, where $G_0 = G$ and $G_i = N_{i-1}$ for all $1 \le i \le n+1$. $\square$

2.9.2 Uniqueness of $\mathrm{gr}_i(G)$

Theorem 2.20. *(Jordan-Hölder). Let $(G_i)_{0\le i\le n}$ be a Jordan-Hölder filtration of a group G. Then the $gr_i(G)$ do not depend on the choice of filtration, up to the permutation of the indices. In particular, the length of the filtration is independent of the filtration.*

Remark 9. The length of the filtration is called the **length** of G, and is denoted $\ell(G)$; when G has no Jordan-Hölder filtration, we write $\ell(G) = \infty$.

Proof. Let S be a simple group, and let $n(G,(G_i),S)$ be the number of j such that G_j/G_{j+1} is isomorphic to S. What we have to prove is that $n(G,(G_i),S)$ does not depend on the chosen filtration (G_i).

Note first that, if H is a subgroup of G, a filtration (G_i) of G incudes a filtration (H_i) of H by putting $H_i = G_i \cap H$. Similarly, if N is a normal subgroup of G, we obtain a filtration of G/N by putting $(G/N)_i = G_i/(G_i \cap N) = G_iN/N$. The exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

gives an exact sequence

$$1 \longrightarrow N_i/N_{i+1} \longrightarrow G_i/G_{i+1} \longrightarrow (G/N)_i/(G/N)_{i+1} \longrightarrow 1$$

i.e.

$$1 \longrightarrow \mathrm{gr}_i(N) \longrightarrow \mathrm{gr}_i(G) \longrightarrow \mathrm{gr}_i(G/N) \longrightarrow 1$$

If (G_i) is a Jordan-Hölder filtration, all the $\mathrm{gr}_i(G)$ are simple; thus, $\mathrm{gr}_i(N)$ is either 1 or $\mathrm{gr}_i(G)$. Let us partition $I = \{1, \ldots, n\}$ into two sets:

$$I_1 = \{i \in I \mid \mathrm{gr}_i(N) = \mathrm{gr}_i(G)\} \quad \text{and} \quad I_2 = \{i \in I \mid \mathrm{gr}_i(N) = 1\}.$$

By reindexing I_1 (resp. I_2) we obtain a Jordan-Hölder filtration of N (resp. of G/N) of length $|I_1|$ (resp. of length $|I_2|$); note that $|I_1| + |I_2| = n$.

We now prove the theorem by induction on the length n of the filtration (G_i). If $n = 0$, then $G = 1$, and if $n = 1$, then G is simple and only one filtration is possible. Assume $n \geq 2$. Choose a normal subgroup N of G distinct from 1 and G. The sets I_1 and I_2 defined above are non-empty, hence their number of elements is $< n$, and we can apply the induction hypothesis to N and G/N; it shows that $n(N, (N_i)_{i \in I_1}, S)$ and $n(G/N, ((G/N)_i)_{i \in I_2}, S)$ are independent of the filtrations since

$$n(G, (G)_{ii \in I}, S) = n(N, (N_i)_{i \in I_2}, S) + n(G/N, ((G/N)_i)_{i \in I_2}, S),$$

this implies that $n(G, (G_i)_{i \in I}, S)$ is independent of the choice of filtration, as wanted. □

Example 2.16. Illustration of proof for $D_4 = \langle r, s \rangle$.

$$\begin{tikzcd}
\langle s \rangle \arrow[r, dash, "C_1"] \arrow[d, dash] & \langle s \rangle \arrow[r, dash, "C_1"] \arrow[d, dash] & \langle s \rangle \arrow[r, dash, "C_2"] \arrow[d, dash] & \langle 1 \rangle \arrow[d, dash] \\
\langle r, s \rangle \arrow[r, dash, "C_2"] \arrow[d, dash] & \langle r^2, s \rangle \arrow[r, dash, "C_2"] \arrow[d, dash] & \langle s \rangle \arrow[r, dash, "C_2"] \arrow[d, dash] & \langle 1 \rangle \arrow[d, dash] \\
\langle r \rangle \arrow[r, dash, "C_2"] & \langle r^2 \rangle \arrow[r, dash, "C_2"] & \langle 1 \rangle \arrow[r, dash, "C_1"] & \langle 1 \rangle
\end{tikzcd}$$

3 Group Actions

3.1 Definition of Group Action

Definition 3.1. Let G be a group and let X be a set. An **action of** G **on** X is a group homomorphism $\pi \colon G \to \mathrm{Sym}\, X$, denoted $g \mapsto \pi_g$. In other words, an action of G on X is a choice for each $g \in G$, of a permutation $\pi_g \colon X \to X$ such that the following two conditions hold:

1. If e is the identity element in G, then $\pi_e(x) = x$ for all $x \in X$.

2. We have $\pi_{g_1} \circ \pi_{g_2} = \pi_{g_1 g_2}$ for all $g_1, g_2 \in G$.

In practice, one dispenses with the notation π_g and writes $\pi_g(x)$ simply as $g(x)$ or $g \cdot x$ or even just gx. This is *not* meant to be an actual multiplication of elements from two possibly different sets G and X. It is just the notation for the effect permutation associated to g on the element x. In this notation, the axioms for a group action take the following form:

1. $ex = x$ for all $x \in X$.

2. $g_1(g_2 x) = (g_1 g_2)x$ for all $g_1, g_2 \in G$ and $x \in X$.

The basic idea in any group action is that the elements of a group are viewed as permutations of a set in such a way that composition of the corresponding permutations matches multilpication in the original group.

3.2 Examples of Group Actions

3.2.1 Permutation Action

Example 3.1. Let S_n act on $X = \{1, 2, \ldots, n\}$ in the usual way. Here $\pi_\sigma(i) = \sigma(i)$ in the usual notation.

Example 3.2. Any group G acts on itself $(X = G)$ by left multilpication functions. That is, we set $\pi_g \colon G \to G$ by

$$\pi_g(h) = gh$$

for all $g, h \in G$. Then the conditions for π being a group action are satisfied since e is the identity and multiplication in G is associative.

Example 3.3. The group S_n acts on polynomials $f(T_1, \dots, T_n)$, by permuting variables:

$$(\sigma \cdot f)(T_1, \dots, T_n) = f(T_{\sigma(1)}, \dots, T_{\sigma(n)}).$$

This is a change of variables $T_i \mapsto T_{\sigma(i)}$ in $f(T_1, \dots, T_n)$. For example, $(12)(23) = (123)$ in S_3 and

$$\begin{aligned}(12) \cdot ((23) \cdot (T_2 + T_3^2)) &= (12) \cdot (T_3 + T_2^2) \\ &= T_3 + T_1^2 \\ &= (123) \cdot (T_2 + T_3^2)\end{aligned}$$

giving the same result both ways. It's also obvious that $(1) \cdot f = f$. To check $\sigma \cdot (\sigma' \cdot f) = (\sigma\sigma') \cdot f$ for all $\sigma, \sigma' \in S_n$, we compute

$$\begin{aligned}(\sigma \cdot (\sigma' \cdot f))(T_1, \dots, T_n) &= (\sigma \cdot f)(T_{\sigma'(1)}, \dots, T_{\sigma'(n)}) \\ &= f(T_{\sigma(\sigma'(1))}, \dots, T_{\sigma(\sigma'(n))}) \\ &= f(T_{(\sigma\sigma')(1)}, \dots, T_{(\sigma\sigma')(n)}) \\ &= ((\sigma\sigma') \cdot f)(T_1, \dots, T_n)\end{aligned}$$

Lagranges study of this group action marked the first systematic use of symmetric groups in algebra. Lagrange wanted to understand why nobody had found an analogue of the quadratic formula for roots of a polynomial in degree greater than four.

Example 3.4. Here is a tricky example, so pay atttenion. Let S_n act on $\mathbb{R}^n$ by permuting coordinates: for $\sigma \in S_n$ and $v = (c_1, \dots, c_n) \in \mathbb{R}^n$, set $\sigma \cdot v = (c_{\sigma(1)}, \dots, c_{\sigma(n)})$. Is this a group action? No. The reason is because $c_{\sigma(i)}$ is treated as the i'th position, whereas in conrast to the previous example, $T_{\sigma(i)}$ is treated as the $\sigma(i)$'th position.

3.2.2 Conjugation Action

Example 3.5. Let G be a group and let N be a normal subgroup. Then G acts on N by conjugation: let $x \in G$ and $y \in N$. We set

$$x \cdot y = xyx^{-1}. \tag{13}$$

To see that this is in fact an action, first note that (13) lands in N since N is normal in G. Next, let $x_1, x_2 \in G$ and let $y \in N$. Then

$$\begin{aligned}x_1 \cdot (x_2 \cdot y) &= x_1 \cdot (x_2 y x_2^{-1}) \\ &= x_1 (x_2 y x_2^{-1}) x_1^{-1} \\ &= (x_1 x_2) y (x_1 x_2)^{-1} \\ &= (x_1 x_2) \cdot y.\end{aligned}$$

Also if $e \in G$ is the identity, then

$$\begin{aligned}e \cdot y &= eye^{-1} \\ &= y.\end{aligned}$$

It follows that (13) gives an action of G on N.

3.3 Orbit-Stabilizer Theorem

An action of a group G on a set X gives rise to an equivalence relation on X. Namely, for $x, y \in X$ we say $x \sim y$ if there exists $g \in G$ such that $gx = y$. One readily checks that this is indeed an equivalence relation. The equivalence classes are called G**-orbits** (or more simply just **orbits** if G is understood). Let us make the following definitions.

Definition 3.2. Let G be a group and suppose G acts on a set X. For each $x \in X$, we define

1. The **orbit of** x, denoted $\mathrm{Orb}_G(x)$, is the subset of X given by

$$\mathrm{Orb}_G(x) = \{gx \in X \mid g \in G\}$$

2. The **stabilizer of** x, denoted $\mathrm{Stab}_G(x)$, is the subgroup of G given by

$$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}.$$

Exercise 3. Verify that $\mathrm{Stab}_G(x)$ is a subgroup of G.

Theorem 3.1. *(Orbit-Stabilizer Theorem) Let G be a group and suppose G acts on a set X. Then for each $x \in X$, we have*

$$|\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)].$$

Proof. Define $\varphi \colon G \to \mathrm{Orb}_G(x)$ be given by

$$\varphi(g) = gx$$

for all $g \in G$. The map φ induces a map $\overline{\varphi} \colon G/\mathrm{Stab}_G(x) \to \mathrm{Orb}_G(x)$, given by

$$\overline{\varphi}(\overline{g}) = gx$$

for all $\overline{g} \in \mathrm{Stab}_G(x)$. We claim that $\overline{\varphi}$ is a bijection. Indeed, it is surjective since φ is surjective. To see that it is injective, suppose $\overline{\varphi}(\overline{g}) = \overline{\varphi}(\overline{h})$ for some $\overline{g}, \overline{h} \in G/\mathrm{Stab}_G(x)$. Then $gx = hx$ implies $g^{-1}h \in \mathrm{Stab}_G(x)$. Therefore

$$\begin{aligned} \overline{g} &= \overline{gg^{-1}h} \\ &= \overline{h}. \end{aligned}$$

This implies $\overline{\varphi}$ is injective. □

3.3.1 Stabilizers and Conjugate Subgroups

Proposition 3.1. *Let G be a group and suppose G acts on a set X. Let $g \in G$ and $x \in X$. Then*

$$gStab_G(x)g^{-1} = Stab_G(g(x))$$

Proof. Suppose $h \in \mathrm{Stab}_G(x)$. Then

$$\begin{aligned} ghg^{-1}(g(x)) &= gh(g^{-1}g)(x) \\ &= gh(x) \\ &= g(x). \end{aligned}$$

Therefore $g\mathrm{Stab}_G(x)g^{-1} \subseteq \mathrm{Stab}_G(g(x))$. Converesely, if $h \in \mathrm{Stab}_G(g(x))$, then $h = g(g^{-1}hg)g^{-1}$, where $g^{-1}hg \in \mathrm{Stab}_G(x)$ since

$$\begin{aligned} g^{-1}hg(x) &= g^{-1}h(g(x)) \\ &= g^{-1}(g(x)) \\ &= (g^{-1}g)(x) \\ &= x. \end{aligned}$$

Therefore $g\mathrm{Stab}_G(x)g^{-1} \supseteq \mathrm{Stab}_G(g(x))$. □

3.4 Fixed-Point Congruence

The fixed-point congruence theorem is very useful when dealing with p-groups. To state this theorem, we first need the following definition.

Definition 3.3. Let G be a finite p-group and suppose G acts on a finite set X. We define

$$\mathrm{Fix}_G(X) := \{x \in X \mid g \cdot x = x \text{ for all } g \in G\}.$$

Theorem 3.2. *Let G be a finite p-group and suppose G acts on a finite set X. Then*

$$|X| \equiv \mathrm{Fix}_G(X) \ mod \ p.$$

Proof. After partitioning X into its G-orbit classes. We have

$$|X| = |\mathrm{Fix}_G(X)| + |\mathrm{Orb}_G(x_1)| + \cdots + |\mathrm{Orb}_G(x_n)|. \tag{14}$$

where $x_1, \ldots, x_n$ are representatives whose G-orbit classes have size ≥ 2. By the orbit-stabilizer theorem, we have $\mathrm{Orb}_G(x_i) = [G : \mathrm{Stab}_G(x_i)]$ for all $i = 1, \ldots, n$. Since $x_i \notin \mathrm{Fix}_G(X)$, we must have $\mathrm{Stab}_G(x_i)$ is a *proper* subgroup of G. In particular, this implies p divides $\mathrm{Orb}_G(x_i)$. Thus, we obtain our desired reults after reduce both sides of (14) modulo p. □

Theorem 3.3. *If G acts on X and H is a subgroup of G, then the following are equivalent:*

1. *H acts transtivitely on X*

2. *G acts transitively on X and $G = H\text{Stab}_x$ for every $x \in X$.*

Proof. If H is transitive, then clearly G is transitive too. For $g \in G$, $gx = hx$ for some $h \in H$, so $h^{-1}g \in$Stab$_x$. Thus $g = h\left(h^{-1}g\right) \in H\text{Stab}_x$, so $G = H\text{Stab}_x$. Conversely, given $x, y \in X$, choose $g \in G$ such that $gx = y$. Write $g = hs$, where $h \in H$ and $s \in$Stab$_x$. Then $hx = y$, so H acts transitively on X. □

If G is a group that acts on A then the action defines an equivalence relation on A: $a \sim b$ if there exists $g \in G$ such that $ga = b$. The equivalence class of $a \in A$ is $C_a = \{ga \mid g \in G\}$. We say C_a is the **orbit** of G containing a. Recall $|C_a| = |G : G_a|$ where $G_a = \{g \in G \mid ga = a\}$.

Definition 3.4. The action of G on A is **transitive** if there is exactly one orbit, i.e. $C_a = A$ for any $a \in A$.

Example 3.6. Let $n \geq 2$. S_n acts transitively on $A = \{1, 2, \ldots, n\}$ by $\sigma \cdot i = \sigma(i)$ for all $\sigma \in S_n$ and for all $i \in \{1, 2, \ldots, n\}$.

Example 3.7. Let G be a group and let A be a nonempty set. Consider the trivial action of G on $A : ga = a$ for all $g \in G$ and for all $a \in A$. This action is transitive if and only if A has exactly one element since $C_a = \{a\}$ for all $a \in A$.

Let π be an action of G on a finite set X. We can express X as a disjoint union of orbits, say

$$X = \coprod_{i=1}^{n} \text{Orb}_G(x_i).$$

For each $1 \leq i \leq n$, set $X_i = \text{Orb}_G(x_i)$. Observe that π restricts an action of G on X_i. For each $1 \leq i \leq n$, set $\pi_i = \pi|_{X_i}$. Then note that

$$\pi = \bigoplus_{i=1}^{n} \pi_i$$

where each π_i is a transitive action.

3.5 Groups Acting by Left Multiplication

Let G be a group with identity 1. Recall that G acts on itself by left multiplication by $g \cdot h = gh$ for all $g, h \in G$. The associated permutation representation $\varphi : G \to S_G$ given by $\varphi(g) = \sigma_g$ where $\sigma_g : G \to G$ given by $\sigma_g(a) = ga$ for all $a \in G$. So Ker$\varphi = \{g \in G \mid \sigma_g = 1_g\} = \{g \in G \mid ga = a, \forall a \in G\} = \{1\}$.

Theorem 3.4. *(Cayley) Every group is isomorphic to a subgroup of a group of permutations.*

Proof. G acts on G by left multiplication. This gives a homomorphism $\varphi : G \to S_G$ with Ker$\varphi = \{1\}$. By the first isomorphism theorem, $G \cong G/\text{Ker}\varphi \cong \varphi(G) \leq S_G$. □

Proposition 3.2. *Let G be a group, let $H \leq G$, and let $A = \{aH \mid a \in G\}$. Then*

1. *G acts transitively on A by left multiplication: $g \cdot aH = gaH$ for all $g \in G$, $aH \in A$.*

2. *Ker $= \bigcap_{x \in G} xHx^{-1}$ and Ker $\leq H$.*

Proof. (1) : We have

$$\begin{aligned} g_1 \cdot (g_2 \cdot aH) &= g_1 \cdot (g_2 a)H) \\ &= g_1(g_2 a)H \\ &= (g_1 g_2)aH \\ &= g_1 g_2 \cdot aH \end{aligned}$$

for all $g_1, g_2 \in G$ and $aH \in A$. We also have $1 \cdot aH = aH$ for all $aH \in A$. Therefore this is a group action. Now we check that the action is transitive. Let aH and bH be two elements in A. Then $ba^{-1} \cdot aH = bH$. Therefore this action is transitive.

(2) : By definition, Ker $= \{g \in G \mid g \cdot xH = xH, \forall x \in G\}$. This means $g = xh_x x^{-1}$ for all $x \in G$ where $h_x \in H$. □

Proposition 3.3. *Let G be a group of finite order. If p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.*

Proof. Let $H \leq G$ such that $[G : H] = p$ and let $A = \{aH \mid a \in G\}$. Then $|A| = p$. We've just shown G acts on A. Let $\pi : G \to S_A$ be the permutation representation and let $K = \mathrm{Ker}\pi$. We know that K is a normal subgroup of G and that $K \leq H$. We show that $K = H$. By the first isomorphism theorem, $G/K \cong \pi(G) \leq S_A$. So $|\pi(G)|$ divides $|S_A| = p!$, and $|\pi(G)| = [G : K]$. Since $K \leq H \leq G$ we have $[G : K] = [G : H][H : K] = p[H : K]$. Suppose $[H : K] > 1$. Then $[H : K]$ divides $(p-1)!$, and this implies any prime dividing $[H : K] < p$. But $[H : K]$ divides $|H|$ which implies $[H : K]$ divides $|G|$. By hypothesis, any prime dividing $[H : K]$ is greater than or equal to p. Contradiction. So $[H : K] = 1$. Then $H = K = \mathrm{Ker}\pi \trianglelefteq G$. □

3.6 Groups Acting on Themselves by Conjugation and the Class Equation

Let G act on itself by conjugation, i.e. $g \cdot a = gag^{-1}$ for all $g, a \in G$. The equivalence relation induced on G is: $a \sim b$ if there exists $g \in G$ such that $b = gag^{-1}$. In this case, a and b are **conjugate**. The orbit containing $a \in G$ is $C_a = \{gag^{-1} \mid g \in G\}$ and the stabilizer of a is $G_a = \{g \in G \mid gag^{-1} = a\} = C_G(a)$. So $|C_a| = [G : C_G(a)]$.

Lemma 3.5. $C_a = \{a\}$ *if and only if* $a \in Z(G)$.

Proof. $C_a = \{a\}$ if and only if $gag^{-1} = a$ for all $g \in G$. This implies $a \in Z(G)$. Conversely, if $a \in Z(G)$, then $gag^{-1} = a$ for all $g \in G$. This implies $C_a = \{a\}$. □

Theorem 3.6. *(The Class Equation) Let G be a group. Let $g_1, \ldots, g_k$ be representatives of all distinct conjugacy classes not contained in $Z(G)$. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)].$$

Proof. Let $Z(G) = \{1 = z_1, z_2, \ldots, z_\ell\}$. By the lemma, $C_{z_\ell} = \{z_\ell\}$. The distinct conjugacy classes of G are

$$C_{z_1}, \ldots, C_{z_\ell}, C_{g_1}, \ldots, C_{g_k}.$$

Then

$$G = C_{z_1} \cup \cdots \cup C_{z_\ell} \cup C_{g_1} \cup \cdots \cup C_{g_k}$$

is a disjoint union of these conjugacy classes. So

$$\begin{aligned} |G| &= |C_{z_1}| \cup \cdots \cup |C_{z_\ell}| \cup |C_{g_1}| \cup \cdots \cup |C_{g_k}| \\ &= |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)]. \end{aligned}$$

□

Example 3.8. In S_3, the class equation says

$$\begin{aligned} |S_3| &= |Z(S_3)| + [S_3 : C_{S_3}((1,2))] + [S_3 : C_{S_3}((1,2,3))] \\ &= 1 + 3 + 2 \end{aligned}$$

Theorem 3.7. *Let p be a prime and let G be a p-group. Then $Z(G) \neq \{1\}$.*

Proof. Let $g_1, \ldots, g_k$ be representatives of all distinct conjugacy classes which are not contained in $Z(G)$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)]. \tag{15}$$

First note that $C_G(g_i)$ is a proper subgroup of G since $g_i \notin Z(G)$ for each $i = 1, \ldots, k$. Therefore, reducing both sides of (15) mod p, we see that $|Z(G)| \equiv 0 \mod p$, which implies the theorem. □

Corollary 6. *Any group G of order p^2 is abelian.*

Proof. By the previous theorem, we have $|Z(G)| \in \{p, p^2\}$. If $|Z(G)| = p^2$, then G is abelian. If $|Z(G)| = p$, then $|G/Z(G)| = p$, which implies $G/Z(G)$ is cyclic. This implies G is abelian. □

Proposition 3.4. *Let G be a group. If $H \trianglelefteq G$ and if K is a conjugacy class of G, then either $H \cap K = \emptyset$ or $K \subseteq H$.*

Proof. If $H \cap K = \emptyset$ we're done. If $H \cap K \neq \emptyset$ then there exists an a in $H \cap K$. This implies $K = C_a = \{gag^{-1} \mid g \in G\} \subseteq H$ since H is normal in G. □

Corollary 7. *If $H \trianglelefteq G$ then H is a union of conjugacy classes ($H = \cup_{a \in H} C_a$).*

Example 3.9. We list all conjugacy classes and their sizes in S_4 in the table below

Representative	Size
(1)	1
$(1,2)$	6
$(1,2,3)$	8
$(1,2)(3,4)$	3
$(1,2,3,4)$	6

Suppose $H \trianglelefteq S_4$. By Lagrange's Theorem, $|H|$ divides $|S_4| = 2^3 \cdot 3$. Therefore $|H| = \{1,2,3,4,6,8,12,24\}$. Since $H \trianglelefteq S_4$, it must be a union of conjugacy classes. This implies $|H| = 1 + \ell_1 + \cdots + \ell_k$ with $\ell_i \in \{6,8,3,6\}$. From this we see that $|H| \in \{1,4,12,24\}$. Clearly there are normal subgroups of S_4 with orders $1, 12$, and 24, namely the trivial group, A_4, and S_4. There is also a normal subgroup of S_4 with size 4: $V = \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$.

Example 3.10. We list all conjugacy classes and their sizes in A_5 in the table below

Representative	Size
(1)	1
$(1,2,3)$	20
$(1,2,3,4,5)$	12
$(2,1,3,4,5)$	12
$(1,2)(3,4)$	15

Suppose $H \trianglelefteq S_4$. By Lagrange's Theorem, $|H|$ divides $|S_4| = 2^3 \cdot 3$. Therefore $|H| = \{1,2,3,4,6,8,12,24\}$. Since $H \trianglelefteq S_4$, it must be a union of conjugacy classes. This implies $|H| = 1 + \ell_1 + \cdots + \ell_k$ with $\ell_i \in \{6,8,3,6\}$. From this we see that $|H| \in \{1,4,12,24\}$. Clearly there are normal subgroups of S_4 with orders $1, 12$, and 24, namely the trivial group, A_4, and S_4. There is also a normal subgroup of S_4 with size 4: $V = \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$.

Sylow's Theorem

In this section, let p be a prime and let G be a group of order $p^\alpha m$ where $\alpha \geq 0$ and $p \not| m$.

Definition 3.5. Let p be a prime. A **p-group** is a group of order p^m for some $m \geq 0$. A **Sylow p-subgroup** of G is a subgroup P of G with $|P| = p^\alpha$. We use the notation $\mathrm{Syl}_p(G) = \{P \leq G \mid |P| = p^\alpha\}$ to denote the set of all Sylow p-subgroups of G and we also use the notation $n_p = |\mathrm{Syl}_p(G)|$ to denote the number of Sylow p-subgroups of G.

Theorem 3.8. *Let p be a prime and let G be a group of order $p^\alpha m$ where $\alpha \geq 0$ and $p \not| m$. Then*

1. *$Syl_p(G) \neq \emptyset$.*

2. *If Q is a p-subgroup of G and if $P \in Syl_p(G)$, then $Q \leq gPg^{-1}$ for some $g \in G$.*

3. *For all $P \in Syl_p(G)$, we have $n_p \equiv 1 \bmod p$, $n_p \mid m$, and $n_p = [G : N_G(P)]$.*

Corollary 8. *The following are equivalent.*

1. *$n_p = 1$.*

2. *P is a characteristic subgroup of G.*

3. *$P \trianglelefteq G$.*

Example 3.11. We show that any group of order 15 is cyclic. Let G be a group of order 15. We have $n_5 \mid 3$ and $n_5 \equiv 1 \bmod 5$, thus $n_5 = 1$. Similarly $n_3 = 1$. This implies $\mathrm{Syl}_3(G) = \{P\}$ where $|P| = 3$. Thus, $P = \langle x \rangle$ where $\mathrm{ord}(x) = 3$. Similarly $\mathrm{Syl}_5(G) = \{Q\}$ and $Q = \langle y \rangle$ where $\mathrm{ord}(y) = 5$. Since P and Q are normal subgroups of G and $P \cap Q = \{e\}$, we have $xy = y^k x$ and $xy = yx^\ell$ for some k and ℓ. So $y^k x = yx^\ell$ or $y^{k-1}x^{1-\ell} = 1$, which implies $k = \ell = 1$. So x commutes with y and this implies $\mathrm{ord}(xy) = \mathrm{ord}(x)\mathrm{ord}(y) = 15$.

Lemma 3.9. *If Q is a p-subgroup of G and if $P \in Syl_p(G)$, then $Q \cap N_G(P) = Q \cap P$.*

Example 3.12. We show that any group of order 105 is not simple. Let G be a group such that $|G| = 105 = 3 \cdot 5 \cdot 7$. Suppose G is simple. Then $n_3, n_5, n_7 > 1$. Since $n_p \mid m$, we have $n_3 \in \{1, 5, 7, 35\}$, $n_5 \in \{1, 3, 7, 21\}$, and $n_7 \in \{1, 3, 5, 15\}$. Since $n_p \equiv 1 \bmod p$, we have $n_3 \in \{1, 7\}$, $n_5 \in \{1, 21\}$, and $n_7 \in \{1, 15\}$. Since $n_p > 1$, we have $n_3 = 7$, $n_5 = 21$, and $n_7 = 15$. This is a contradiction though because this would imply there are $2 \cdot 7$ elements of order 3, $4 \cdot 21$ elements of order 5, $6 \cdot 15$ elements of order 7, and $2 \cdot 7 + 4 \cdot 21 + 6 \cdot 15 = 188 > 105$.

Example 3.13. Let G be a group of order $30 = 2 \cdot 3 \cdot 5$. We show that G has a normal subgroup of order 15. Since $n_p \mid m$ and $n_p \equiv 1 \bmod p$, we have $n_2 \in \{1, 3, 5, 15\}$, $n_3 \in \{1, 10\}$, $n_5 \in \{1, 6\}$. We want to show that one of n_3, n_5 has to be 1. If $n_3, n_5 > 1$, then $n_3 = 10$ and $n_5 = 6$. This is a contradiction though since $2 \cdot 10 + 4 \cdot 6 = 44 > 30$. So either n_3 or n_5 is equal to 1. Assume $n_3 = 1$. Let P be the 3-Sylow Subgroup and let Q be a 5-Sylow Subgroup. Then since P is normal, PQ is a subgroup of G. Since $|P \cap Q| = 1$, $|PQ| = |P| \cdot |Q|$. So PQ is a group of order 15, hence it is cyclic. So $\mathrm{Syl}_5(PQ) = \{Q\}$ and Q is a characteristic subgroup of PQ, and $PQ \trianglelefteq G$ because $[G : PQ] = 2$, so $Q \trianglelefteq G$. The same idea works when $n_5 = 1$.

Sylows's Theorem Applications

Recall, if $|G| = 15$ then G is cyclic. In particular, $n_5 = 1$. If $|G| = 30$, then $n_3 = n_5 = 1$.

Example 3.14. If G is a group of order 6 then $n_3 = 1$.

Example 3.15. If G is a group of order 20 then $n_5 = 1$.

Proposition 3.5. *Any group of order* 12 *has either* $n_2 = 1$ *or* $n_3 = 1$.

Proof. Let G be a group of order $12 = 3 \cdot 2^2$. If $n_3 = 1$ then we are done. So assume $n_3 > 1$. Then by Sylow's Theorems, $n_3 = 4$. So $\mathrm{Syl}_3(G) = \{P_1, P_2, P_3, P_4\}$ with $|P_i| = 3$. Each P_i is cyclic of order 3 and $P_i \cap P_j = \{e\}$ for $i \neq j$, so there are 8 elements of order 3 in G. Now G acts on $\mathrm{Syl}_3(G)$ by conjugation: $g \cdot P_i = gP_ig^{-1}$. This gives a homomorphism $\varphi : G \to S_4$ with

$$\mathrm{Ker}\varphi = \{g \in G \mid gP_ig^{-1} = P_i, \quad 1 \leq i \leq 4\} = \bigcap_{i=1,2,3,4} \mathrm{N}_G(P_i).$$

Since

$$\begin{aligned} 4 &= n_3 \\ &= [G : \mathrm{N}_G(P_i)] \\ &= \frac{|G|}{\mathrm{N}_G(P_i)} \\ &= \frac{12}{\mathrm{N}_G(P_i)}. \end{aligned}$$

$\mathrm{N}_G(P_i) = 3$. So $P_i \leq \mathrm{N}_G(P_i)$ and $|P_i| = |\mathrm{N}_G(P_i)|$ implies $P_i = \mathrm{N}_G(P_i)$. So

$$\mathrm{Ker}\varphi == \bigcap_{i=1,2,3,4} P_i = \{e\}.$$

Then $G \cong \varphi(G) \leq S_4$. Since G has 8 elements of order 3, $\varphi(G)$ also has 8 elements of order 3. So $|\varphi(G) \cap A_4| \geq 8$ and $\varphi(G) \cap A_4 \leq \varphi(G)$ implies $|\varphi(G) \cap A_4| = 12 = \varphi(G)$. So if $n_3 = 4$, then $\varphi(G) \cong A_4$ and $n_2(A_4) = 1$. $\square$

Proposition 3.6. *If G is a group of order* 60 *and* $n_5 > 1$, *then G is simple.*

Proof. To obtain a contradiction, suppose G is a group of order $60 = 2^2 \cdot 3 \cdot 5$ such that G is not simple. By Sylow's Theorems, we have $n_5 \in \{1, 6\}$. Since G is not simple, we must have $n_5 = 6$. So $\mathrm{Syl}_6(G) = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ with $|P_i| = 5$. Each P_i is cyclic of order 5 and $P_i \cap P_j = \{e\}$ for $i \neq j$, so there are 24 elements of order 5 in G. Since G is not simple, there exists $H \trianglelefteq G$ such that $H \neq 1, G$. Now

$$|H| \mid 60 \implies |H| \in \{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}.$$

If $5 \mid |H|$, then H contains a subgroup of order 5. Thus there is some P_i such that $P_i \leq H$. For any other $P_j \in \mathrm{Syl}_5(G)$, we have $P_j = gP_ig^{-1}$ for some $g \in G$. So $P_j = gP_ig^{-1} \leq gHg^{-1} = H$. So H contains all the Sylow 5-subgroups of G. Thus $|H| \geq 1 + 24 = 25$, this implies $|H| = 30$. But if $|H| = 30$, then $n_5(H) = 1$, which is a contradiction. So

$$|H| \in \{2, 3, 4, 6, 12\}.$$

If $|H| \in \{6, 12\}$, then there exists K char H with $K \in \mathrm{Syl}_3(H)$ or $K \in \mathrm{Syl}_2(H)$. Since K is characteristic in H and H is normal in G, K is normal in G. So there is a normal subgroup K of G with $|K| \in \{2, 3, 4\}$. So it suffices to assume

$$|H| \in \{2, 3, 4\}$$

leads to a contradiction. Then $|G/H| \in \{30, 20, 15\}$. Now $n_5(G/H) = 1$ implies there exists $H \trianglelefteq T \trianglelefteq G$ such that $T/H \trianglelefteq G/H$ with $|T/H| = 5$. So there exists $T \trianglelefteq G$ such that $|T|/|H| = 5$ implies $|T| = 5 \cdot |H|$. But this leads to the first case where $5 \mid |T|$ and T is normal. This leads to a contradiction.

□

Corollary 9. *A_5 is simple in S_5.*

Proof. We have $|A_5| = 60$ and $n_5 > 1$ since $\langle (1, 2, 3, 4, 5) \rangle \neq \langle (2, 1, 3, 4, 5) \rangle$. □

Proposition 3.7. *If G is a simple group of order 60 then $G \cong A_5$.*

Theorem 3.10. *A_n is a simple group for all $n \geq 5$.*

Example 3.16. Let G be a group of order $231 = 3 \cdot 7 \cdot 11$. We will show $Z(G)$ contains a Sylow 11-sybgroup and $n_7 = 1$. From the Sylow theorems, we obtain $n_{11} = 1$ and $n_7 = 1$. Let P be the Sylow 11 -subgroup of G. Consider the action of G on P by conjugation $\varphi : G \to \mathrm{Aut}(P)$, $\varphi(g) = \sigma_g$ where $\sigma_g(x) = gxg^{-1}$ for $x \in P$. The kernel of φ is $C_G(P)$. By the Isomorphism theorems, we have $G/C_G(P) \cong \varphi(G) \leq \mathrm{Aut}(P)$. Since $|\mathrm{Aut}(P)| = 10$, we must have $|G/C_G(P)| \mid 10$. The only possibility is when $|G/C_G(P)| = 1$, so $C_G(P) = G$. That is, P is contained in $Z(G)$.

Example 3.17. Let G be a group of order $105 = 3 \cdot 5 \cdot 7$ and suppose $n_3 = 1$. We will show G is abelian. Let P be the Sylow 3-subgroup and consider the action of G on P by conjugation. Again, we find that $|G/C_G(P)|$ divides $|\mathrm{Aut}(P)| = 2$. The only possibility is $|G/C_G(P)| = 1$, so $G = C_G(P)$.

Direct Products of Abelian Groups

Proposition 3.8. *Let $G_1, G_2, \ldots, G_n$ be groups and let $G = \{(a_1, \ldots, a_n) \mid a_i \in G_i,\ 1 \leq i \leq n\}$. Then G is a group with multiplication defined by*

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Proof. The multiplicaiton operation is clearly an associative binary operation. We also have an identity element $(e_1, \ldots, e_n)$ where e_i is the identity element in G_i. And the inverse of an element $(a_1, \ldots, a_n) \in G$ is $(a_1^{-1}, \ldots, a_n^{-1})$. □

Definition 3.6. A group G is **finitely generated** if $G = \langle A \rangle$ for some $\emptyset \neq A \subset G$ such that $|A| < \infty$.

The Fundamental Theorem of Finitely Generated Abelian Groups

Let G be a finitely generated abelian group. Then

1. $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cdots \times \mathbb{Z}_{n_k}$ for $r \geq 0$, $n_i \geq 2$ such that $n_{i+1} \mid n_i$ for all $1 \leq i \leq k-1$. We say n_i are the **invariant factors** of G and r is the **Betti number** of G.

2. The decomposition in (1) is unique i.e. if $G \cong \mathbb{Z}^\ell \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \cdots \times \mathbb{Z}_{m_t}$ with $\ell \geq 0$, $m_j \geq 2$ such that $m_{j+1} \mid m_j$ for all $1 \leq j \leq t-1$, then $r = \ell$, $k = t$, and $n_i = m_i$ for all $1 \leq i \leq k$.

Remark 10. If $|G| < \infty$ then $r = 0$. So $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ with $n_i \geq 2$ and such that $n_{i+1} \mid n_i$ for all $1 \leq i \leq k-1$. In this case, $|G| = n_1 n_2 \cdots n_k$.

Remark 11. If G is a finite abelian group, then every prime divisor of $|G|$ must divide n_1. This is because $p \mid n_1 n_2 \cdots n_k$ implies $p \mid n_i \mid n_{i-1} \mid \cdots \mid n_2 \mid n_1$.

Example 3.18. We find (up to isomorphism) all abelian groups of order 180. Let G be a group of order $180 = 2^2 \cdot 3^2 \cdot 5$. Then $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ with $n_i \geq 2$ and such that $n_{i+1} \mid n_i$ for all $1 \leq i \leq k-1$. So we have by the second remark, $2, 3, 5 \mid n_1$ implies n_1 equals $2 \cdot 3 \cdot 5$, or $2^2 \cdot 3 \cdot 5$, or $2 \cdot 3^2 \cdot 5$, or $2^2 \cdot 3^2 \cdot 5$.

In the case $n_1 = 2 \cdot 3 \cdot 5$,

$$n_2 \mid n_1 \qquad \text{and} \qquad n_1 n_2 \mid 2^2 \cdot 3^2 \cdot 5 \qquad \Longrightarrow \qquad n_2 \in \{2, 3, 2 \cdot 3\}.$$

Suppose $n_2 = 2$. Then $n_1 n_2 = 2^2 \cdot 3 \cdot 5 < |G|$. So $n_3 \mid n_2$ and $n_1 n_2 n_3 \mid 180$ implies $n_3 = 3$ which is a contradiction. So $n_2 \neq 2$. Again we get a contradiction if we assume $n_2 = 3$. So for $n_1 = 2 \cdot 3 \cdot 5$, the only possibility is for $n_2 = 2 \cdot 3$. Then $n_1 n_2 = 2^2 \cdot 3^2 \cdot 5$ and $n_3 = 1$. So $G \cong \mathbb{Z}_{30} \times \mathbb{Z}_6$.

In the case $n_2 = 2^2 \cdot 3 \cdot 5$,

$$n_2 \mid n_1 \qquad \text{and} \qquad n_1 n_2 \mid 2^2 \cdot 3^2 \cdot 5 \qquad \Longrightarrow \qquad n_2 = 3.$$

So $G \cong \mathbb{Z}_{60} \times \mathbb{Z}_3$.

In the case $n_1 = 2 \cdot 3^2 \cdot 5$,

$$n_2 \mid n_1 \qquad \text{and} \qquad n_1 n_2 \mid 2^2 \cdot 3^2 \cdot 5 \qquad \Longrightarrow \qquad n_2 = 2.$$

So $G \cong \mathbb{Z}_{90} \times \mathbb{Z}_2$.

The last case to consider is $n_1 = 180$. In this case, $G \cong \mathbb{Z}_{180}$.

Theorem 3.11. *Let G be a finite abelian group of order n. Write the prime factorization of n as $n = p_1^{e_1} \cdots p_k^{e_k}$. Then*

1. *$G \cong A_1 \times A_2 \times \cdots \times A_k$ with $|A_i| = p_i^{e_i}$ for all $1 \le i \le k$.*
2. *If $A \in \{A_1, \ldots, A_k\}$ and $|A| = p^e$, then $A \cong \mathbb{Z}_{p^{f_1}} \times \cdots \times \mathbb{Z}_{p^{f_\ell}}$ where $f_1 \ge f_2 \ge \cdots \ge f_\ell \ge 1$. The $p_i^{f_i}$ are called the* ***elementary divisors*** *of G.*
3. *The decomposition of G is unique.*

Example 3.19. We find all abelian groups (up to isomorphism) of order 8.

Partitions of 3	Abelian Groups of order 2^3
3	$\mathbb{Z}_{2^3}$
$2+1$	$\mathbb{Z}_{2^2} \times \mathbb{Z}_2$
$1+1+1$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Theorem 3.12. *Let $m, k \in \mathbb{Z}$. Then $\mathbb{Z}_m \times \mathbb{Z}_k \cong \mathbb{Z}_{mk}$ if and only if $\gcd(m,k) = 1$.*

We list all abelian groups of order 180 in the table below

Abelian Groups of Order 180	Isomorphic Group
$\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_{36} \times \mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_{60} \times \mathbb{Z}_3$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_{90} \times \mathbb{Z}_2$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_{180}$

3.7 Class Equation of a Group Action

Suppose G is a group and X is a finite set. Suppose we are given a group action of G on X. Let X_0 denote the set of those points in S that are fixed under the action of all elements of G. Let $O_1, O_{2,}, \ldots, O_r$ be the orbits of size greater than one under this action. For each orbit O_i, let x_i be an element of O_i and let G_i denote the stabilizer of x_i in G. The class equation for this action is given as follows:

$$|X| = |X_0| + \sum_{i=1}^{r} [G : G_i]$$

This follows from Orbit-Stabilizer.

4 Group Cohomology

4.1 Basic Terminology

Throughout this subsection, let G be a group.

4.1.1 Group Rings and G-Modules

The **group ring** $\mathbb{Z}[G] = \mathbb{Z}G$ corresponding to G is defined as follows: the underlying set of $\mathbb{Z}G$ is given by the set of all elements of the form $\sum_{g \in G} m_g g$ where $m_g \in \mathbb{Z}$ and $m_g = 0$ for all but finitely many $g \in G$. Addition in $\mathbb{Z}G$ is defined by

$$\sum_{g \in G} m_g g + \sum_{g \in G} m'_g g = \sum_{g \in G} (m_g + m'_g) g$$

and multiplication in $\mathbb{Z}G$ is defined by

$$\left(\sum_{g\in G} m_g g\right)\left(\sum_{g\in G} m'_g g\right) = \sum_{g\in G}\left(\sum_{g'\in G} m_{g'} m'_{g'^{-1}g}\right) g.$$

It is straightforward to check that addition and multiplication defined above gives $\mathbb{Z}G$ the structure of a ring with 1 being the identity element. A G**-module** is just a $\mathbb{Z}G$-module in the usual sense. In particular, if A is a G-module, then A is an abelian group on which $\mathbb{Z}G$ acts by additive maps, so

$$\begin{aligned}(gg')a &= g(g'a)\\ 1a &= a\\ g(a+a') &= ga+ga'\\ (g+g')a &= ga+g'a\end{aligned}$$

for all $g, g' \in G$ and $a, a' \in A$.

Example 4.1. We have $\mathbb{Z}[\mathbb{Z}] = \mathbb{Z}[x, x^{-1}]$ and $\mathbb{Z}[\mathbb{Z}/n\mathbb{Z}] = \mathbb{Z}[x]/\langle x^n - 1\rangle$.

Example 4.2. For each $n \geq 2$, we define a $\mathbb{Z}G$-module $\mathbb{Z}[G^{n+1}]$ as follows: the underlying set of $\mathbb{Z}[G^{n+1}]$ is given by all elements of the form

$$\sum_{\boldsymbol{g}\in G^{n+1}} m_{\boldsymbol{g}}\boldsymbol{g} = \sum_{(g_0,\dots,g_n)\in G^{n+1}} m_{(g_0,\dots,g_n)}(g_0,\dots,g_n),$$

where we often simplify notation by writing $\boldsymbol{g} = (g_0, \dots, g_n)$ when context is clear. Addition and scalar-multiplication in $\mathbb{Z}[G^{n+1}]$ are defined pointwise, thus

$$g\boldsymbol{g} = (gg_0,\dots,gg_n) \quad \text{and} \quad \boldsymbol{g}+\boldsymbol{g}' = (g_0+g'_0,\dots,g_n+g'_n)$$

for all $g \in G$ and $\boldsymbol{g}, \boldsymbol{g}' \in G^{n+1}$.

By definition, $\mathbb{Z}[G^{n+1}]$ is a free $\mathbb{Z}$-module with basis given by $\{(g_0, \dots, g_n) \mid g_0, \dots, g_n \in G\}$. Let us now show that $\mathbb{Z}[G^{n+1}]$ is in fact a free $\mathbb{Z}G$-module, with basis given by

$$\mathcal{G}_n := \{(1, g_1, \dots, g_n) \mid g_1, \dots, g_n \in G\}. \tag{16}$$

Proposition 4.1. *$\mathbb{Z}[G^{n+1}]$ is a free $\mathbb{Z}G$-module with basis given by (16).*

Proof. First note that

$$\sum_{\boldsymbol{g}\in G^{n+1}} m_{\boldsymbol{g}}\boldsymbol{g} = \sum_{\boldsymbol{g}\in G^{n+1}} m_{\boldsymbol{g}} g_0(1, g_0^{-1}g_1\dots, g_0^{-1}g_n)$$

shows that $\mathrm{span}_{\mathbb{Z}G}(\mathcal{G}_n) = \mathbb{Z}[G^{n+1}]$. It remains to show that $\mathcal{G}_n$ is $\mathbb{Z}G$-linearly independent. Suppose

$$\sum_{i=1}^{k}\left(\sum_{g\in G} m_{g,i}g\right)(1, g_{1,i}, \dots, g_{n,i}) = 0,$$

where $\sum_{g\in G} m_{g,i}g \in \mathbb{Z}G$ for each $1 \leq i \leq k$ and $(1, g_{1,i}, \dots, g_{n,i}) \neq (1, g_{1,i'}, \dots, g_{n,i'})$ whenever $i \neq i'$. Then

$$\begin{aligned}0 &= \sum_{i=1}^{k}\left(\sum_{g\in G} m_{g,i}g\right)(1, g_{1,i}, \dots, g_{n,i})\\ &= \sum_{i=1}^{k}\sum_{g\in G} m_{g,i}(g, gg_{1,i}, \dots, gg_{n,i})\\ &= \sum_{\substack{g\in G\\ 1\leq i\leq k}} m_{g,i}(g, gg_{1,i}, \dots, gg_{n,i})\end{aligned}$$

implies $m_{g,i} = 0$ for all $g \in G$ and $1 \leq i \leq k$ since

$$\{(g, gg_{1,i}, \dots, gg_{n,i}) \mid g \in G \text{ and } 1 \leq i \leq k\}$$

is $\mathbb{Z}$-linearly independent. Here we are using the fact that $(g, gg_{1,i}, \dots, gg_{n,i}) \neq (g', g'g_{1,i'}, \dots, g'g_{n,i'})$ whenever $g \neq g'$ or $i \neq i'$. To see why this is the case, first note that if $g \neq g'$, then clearly $(g, gg_{1,i}, \dots, gg_{n,i}) \neq (g', g'g_{1,i'}, \dots, g'g_{n,i'})$ since they do not agree in the first component, so assume $g = g'$. Then if $i \neq i'$, then there exists a $1 \leq j \leq n$ such that $g_{j,i} \neq g_{j,i'}$, in which case $gg_{j,i} \neq gg_{j,i'}$. $\square$

Remark 12. There is another way of indexing the elements $\mathcal{G}_n$ which will be useful, namely

$$\{(1, g_1, g_1 g_2, \ldots, g_1 g_2 \cdots g_n) \mid g_1, \ldots, g_n \in G\}.$$

Indeed, we recover our previous description by setting $\widetilde{g}_k = g_1 \cdots g_k$ for each $1 \leq k \leq n$ and noting that

$$\{(1, g_1, g_1 g_2, \ldots, g_1 g_2 \cdots g_n) \mid g_1, \ldots, g_n \in G\} = \{(1, \widetilde{g}_1, \widetilde{g}_2, \ldots, \widetilde{g}_n) \mid \widetilde{g}_1, \widetilde{g}_2, \ldots, \widetilde{g}_n \in G\} = \mathcal{G}_n.$$

4.1.2 The Standard Free Resolution of $\mathbb{Z}$ over $\mathbb{Z}G$

We now construct a complex, denoted $\mathbb{F}_G = \mathbb{F}$, which we call the **standard free resolution of $\mathbb{Z}$ over** $\mathbb{Z}G$. To do this, we first describe the underlying graded module structure of $\mathbb{F}$: the component in homological degree n is given by

$$\mathbb{F}_n = \mathbb{F}^{-n} = \begin{cases} \mathbb{Z}[G^{n+1}] & \text{if } n \geq 0 \\ 0 & \text{else} \end{cases},$$

where n in the subscript is homological notation and n in the superscript is cohomologial notation. We've already shown that each homogeneous component of $\mathbb{F}$ is a free $\mathbb{Z}G$-module. Next we give $\mathbb{F}$ the structure of a $\mathbb{Z}G$-complex by defining a differential $\mathrm{d}\colon \mathbb{F} \to \mathbb{F}$. We do this by defining d on the $\mathbb{Z}$-basis $\{(g_0, \ldots, g_n) \mid n \in \mathbb{N}\}$ and then extend it $\mathbb{Z}$-linearly everywhere else (the reason we define it in terms of the $\mathbb{Z}$-basis first is because it will be easy to show that $\mathrm{d}^2 = 0$). We then show that d is $\mathbb{Z}G$-linear (it preserves the G-action). For any $\mathbb{Z}$-basis element $(g_0, \ldots, g_n)$ in $\mathbb{F}$, we set

$$\mathrm{d}(g_0, \ldots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \ldots, \widehat{g}_i, \ldots, g_n).$$

It is easy to check that $\mathrm{d}^2 = 0$ and is homogeneous of degree -1. Let us show that d is $\mathbb{Z}G$-linear. First note that d is additive since it is $\mathbb{Z}$-linear, so we just need to show that is preserves the $\mathbb{Z}G$-scalar multiplication; it suffices to show this on the $\mathbb{Z}G$-basis elements. Let $g \in G$ and let $(1, g_1 \ldots, g_n)$ be any $\mathbb{Z}G$-basis element of $\mathbb{F}$. We have

$$\begin{aligned} \mathrm{d}\left(g(1, g_1 \ldots, g_n)\right) &= \mathrm{d}(g, gg_1 \ldots, gg_n) \\ &= (gg_1, \ldots, gg_n) + \sum_{i=1}^{n} (-1)^i (g, gg_1, \ldots, \widehat{gg_i}, \ldots, gg_n) \\ &= g\left((g_1 \ldots, g_n) + \sum_{i=1}^{n} (-1)^i (1, g_1, \ldots, \widehat{g}_i, \ldots, g_n) \right) \\ &= g\mathrm{d}(1, g_1 \ldots, g_n). \end{aligned}$$

It follows that d is $\mathbb{Z}G$-linear, and since d is graded of degree -1 and satisfies $\mathrm{d}^2 = 0$, we see that d is a $\mathbb{Z}G$-differential, thus giving $\mathbb{F}$ the structure of a $\mathbb{Z}G$-complex as claimed.

Thus far we've constructed a $\mathbb{Z}G$-complex $\mathbb{F}$ whose homogeneous components are free $\mathbb{Z}G$-modules, however we want to show more: we want to show that $\mathbb{F}$ can be viewed as a resolution of $\mathbb{Z}$, where we view $\mathbb{Z}$ is a trivial $\mathbb{Z}G$-complex (in particular, $\mathbb{Z}$ sits in homological degree 0 and G acts trivially on $\mathbb{Z}$, i.e. $g \cdot m = m$ for all $m \in \mathbb{Z}$ and $g \in G$). This is what we do in the next theorem:

Theorem 4.1. *$\mathbb{F}$ is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}G$.*

Proof. Each $\mathbb{F}_n$ is a free $\mathbb{Z}G$-module by Proposition (4.1). To show that $\mathbb{F}$ is a $\mathbb{Z}G$-free resolution of $\mathbb{Z}$, it suffices to check that the augmented $\mathbb{Z}G$-complex $\widetilde{\mathbb{F}}$ is exact, where the augmented complex $\widetilde{\mathbb{F}}$ is defined as follows: as a graded module, the homogeneous component in homological degree n is

$$\widetilde{\mathbb{F}}_n = \begin{cases} \mathbb{Z}[G^{n+1}] & \text{if } n \geq 0 \\ \mathbb{Z} & \text{if } n = -1 \\ 0 & \text{if } n \leq -1 \end{cases}$$

and the differential $\widetilde{\mathrm{d}}$ in homological degree n is defined by

$$\widetilde{\mathrm{d}}_n = \begin{cases} \mathrm{d}_n & \text{if } n > 0 \\ \varepsilon & \text{if } n = 0 \\ 0 & \text{if } n < 0 \end{cases}$$

where $\varepsilon\colon \mathbb{Z}G \to \mathbb{Z}$, called the **augmentation map**, is defined by

$$\varepsilon\left(\sum_{g\in G} m_g g\right) = \sum_{g\in G} m_g.$$

To show $\widetilde{\mathbb{F}}$ is exact, we will show that the identity map $1\colon \widetilde{\mathbb{F}} \to \widetilde{\mathbb{F}}$ is null-homotopic where we view $\widetilde{\mathbb{F}}$ as a $\mathbb{Z}$-complex. Note that whether we view $\widetilde{\mathbb{F}}$ as a $\mathbb{Z}$-complex or as a $\mathbb{Z}G$-complex, we obtain the same homology at the end of the day. Choose any $g \in G$ and define $\mathrm{m}_g\colon \widetilde{\mathbb{F}} \to \widetilde{\mathbb{F}}$ as follows: given $m \in \mathbb{Z}$ and $(g_0, \dots, g_n) \in G^{n+1}$, we set

$$\mathrm{m}_g(m) = mg \quad \text{and} \quad \mathrm{m}_g(g_0, \dots, g_n) = (g, g_0, \dots, g_n)$$

and we extend m_g everywhere else $\mathbb{Z}$-linearly. We claim that $\widetilde{\mathrm{d}}\mathrm{m}_g + \mathrm{m}_g\widetilde{\mathrm{d}} = 1$. Indeed, if $m \in \mathbb{Z}$, then we have

$$\begin{aligned}(\widetilde{\mathrm{d}}\mathrm{m}_g + \mathrm{m}_g\widetilde{\mathrm{d}})(m) &= \widetilde{\mathrm{d}}\mathrm{m}_g(m) + \mathrm{m}_g\widetilde{\mathrm{d}}(m) \\ &= \widetilde{\mathrm{d}}(mg) + 0 \\ &= m\widetilde{\mathrm{d}}(g) \\ &= m.\end{aligned}$$

Similarly, if $(g_0, \dots, g_n) \in G^{n+1}$, then we have

$$\begin{aligned}(\widetilde{\mathrm{d}}\mathrm{m}_g + \mathrm{m}_g\widetilde{\mathrm{d}})(g_0, \dots, g_n) &= \widetilde{\mathrm{d}}\mathrm{m}_g(g_0, \dots, g_n) + \mathrm{m}_g\widetilde{\mathrm{d}}(g_0, \dots, g_n) \\ &= \widetilde{\mathrm{d}}(g, g_0, \dots, g_n) + \mathrm{m}_g \sum_{i=0}^{n} (-1)^i (g_0, \dots, \widehat{g_i}, \dots, g_n) \\ &= (g_0, \dots, g_n) - \sum_{i=0}^{n} (-1)^i (g, g_0, \dots, \widehat{g_i}, \dots, g_n) + \sum_{i=0}^{n} (-1)^i (g, g_0, \dots, \widehat{g_i}, \dots, g_n) \\ &= (g_0, \dots, g_n).\end{aligned}$$

It follows that the identity map $1\colon \widetilde{\mathbb{F}} \to \widetilde{\mathbb{F}}$ is null-homotopic, and thus $\widetilde{\mathbb{F}}$ is exact. □

4.1.3 Definition of Group Cohomology

Let A be a G-module. We define the **group cohomology of** G **with coefficients in** A to be the Ext module:

$$\mathrm{H}(G, A) := \mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A).$$

We can compute $H = \mathrm{H}(G, A)$ using the fact that $\mathbb{F}$ is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}G$, namely

$$H = \mathrm{H}(\mathrm{Hom}^{\star}_{\mathbb{Z}G}(\mathbb{F}, A)),$$

where $M = \mathrm{Hom}^{\star}_{\mathbb{Z}G}(\mathbb{F}, A)$ is the $\mathbb{Z}G$-complex whose underlying graded module in degree $n \in \mathbb{Z}$ is given by

$$M^n := \begin{cases} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}[G^{n+1}], A) & \text{if } n \geq 0 \\ 0 & \text{else} \end{cases}$$

and whose differential $\mathrm{d}^{\star}$ is defined by $\mathrm{d}^{\star}(\varphi) = \varphi\mathrm{d}$ for all homogeneous $\varphi \in M$. Now let $C = \mathrm{C}(G, A)$ be the graded module whose component in degree n is given by

$$C^n := \begin{cases} A & \text{if } n = 0 \\ \{\text{functions from } G^n \text{ to } A\} & \text{if } n \geq 1 \\ 0 & \text{else} \end{cases}$$

Note that M and C are isomorphic as graded $\mathbb{Z}$-modules. Indeed, define $\theta\colon M \to C$ as follows: in cohomological degree 0, the map θ is given by the canonical isomorphism $M^0 = \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \simeq A = C^0$ given by $\varphi \mapsto \varphi(1)$. In cohomological degree 1, the map θ is defined by sending $\varphi \in M^1 = \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}[G^2], A)$ to the function $\theta(\varphi)\colon G \to A$ given by $\theta(\varphi)(g) = \varphi(1, g)$ for all $g \in G$. More generally, in cohomological degree $n > 1$, the map θ is defined by sending $\varphi \in M^n$ to the function $\theta(\varphi)\colon G^n \to A$ given by

$$\theta(\varphi)(g_1, \dots, g_n) = \varphi(1, g_1, g_1g_2, \dots, g_1g_2\cdots g_n).$$

Conversely if $\alpha \in C^n$, then we set $\theta^{-1}(\alpha)$ to be the $\mathbb{Z}G$-module homomorphism from $\mathbb{Z}[G^{n+1}]$ to A which is uniquely determined by

$$\theta^{-1}(\alpha)(1, g_1, g_1g_2, \dots, g_1g_2\cdots g_n) = \alpha(g_1, g_2, \dots, g_n).$$

We give C^n a $\mathbb{Z}G$-module structure using the isomorphism θ (so that θ becomes an isomorphism of graded $\mathbb{Z}G$-modules). In particular, the scalar-multiplication is given by

$$\begin{aligned}(g\alpha)(g_1, \dots, g_n) &= \theta(g\theta^{-1}(\alpha))(g_1, \dots, g_n) \\ &= (g\theta^{-1}(\alpha))(1, g_1, g_1g_2, \dots, g_1g_2\cdots g_n) \\ &= \theta^{-1}(\alpha)(g, g_1g, g_1g_2g, \dots, g_1g_2\cdots g_ng) \\ &= g\theta^{-1}(\alpha)(1, g^{-1}g_1g, g^{-1}g_1g_2g, \dots, g^{-1}g_1g_2\cdots g_ng) \\ &= g\alpha(g^{-1}g_1g, \dots, g^{-1}g_ng).\end{aligned}$$

Similarly, we give C a $\mathbb{Z}G$-complex structure using the isomorphism θ (so that θ becomes an isomorphism of $\mathbb{Z}G$-complexes). In particular, the differential of C is $\delta := \theta \mathrm{d}^\star \theta^{-1}$. Thus if $\alpha \in C^n$, then $\delta\alpha \in \mathrm{C}^{n+1}$ is given by

$$(\delta\alpha)(g_0, \dots, g_n) = g_0\alpha(g_1, \dots, g_n) + \sum_{i=1}^{n}(-1)^i \alpha(g_0, \dots, \widehat{g_i}, \dots, g_n).$$

Thus with the notation as above, we have

$$\mathrm{H}(G, A) = \mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A) = \mathrm{H}(\mathrm{Hom}^\star_{\mathbb{Z}G}(\mathbb{F}, A)) = \mathrm{H}(\mathrm{C}(G, A)).$$

In the literature, one often sees $\mathrm{H}(\mathrm{C}(G, A))$ as the definition of group cohomology, however the more "correct" definition is $\mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A)$. There are in fact many ways of computing $\mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A)$, where we described the "standard" way (i.e. we consider the standard free resolution $\mathbb{F}$ of $\mathbb{Z}$ over $\mathbb{Z}G$ and we calculate $\mathrm{H}(\mathrm{Hom}^\star_{\mathbb{Z}G}(\mathbb{F}, A))$). First, we can replace $\mathbb{F}$ with any projective resolution F of $\mathbb{Z}$ over $\mathbb{Z}G$ and calculate $\mathrm{H}(\mathrm{Hom}^\star_{\mathbb{Z}G}(F, A))$ instead. The standard resolution works for all G but often times there are better choices one can use depending on the group G. Alternatively, one can calculate $\mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A)$ by finding an injective resolution E of A over $\mathbb{Z}G$ and calculate $\mathrm{H}(\mathrm{Hom}^\star_{\mathbb{Z}G}(\mathbb{Z}, E))$. This is often nice because $\mathrm{Hom}^\star_{\mathbb{Z}G}(\mathbb{Z}, E)$ often has a simple description, namely it is the set of all fixed points of E by G:

$$E^G := \{e \in E \mid ge = e \text{ for all } g \in G\} = \mathrm{Hom}^\star_{\mathbb{Z}G}(\mathbb{Z}, E).$$

Finally, note that if we replace $\mathbb{Z}$ with an arbitrary commutative ring R when defining group cohomology, then we'd obtain the same underlying abelian groups. Indeed, the canonical ring homomorphism $\mathbb{Z}G \to RG$ is flat and we have $\mathbb{Z} \otimes_{\mathbb{Z}G} RG \simeq R$, so by flat base change in Ext, we have a canonical isomorphism

$$\mathrm{H}(G, A) := \mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A) \simeq \mathrm{Ext}_{RG}(R, A).$$

4.2 Relation to subgroups

Let H be a subgroup of G and let A be an H-module. We can transport A up to a G-module by setting

$$\mathrm{M}^G_H(A) := \mathrm{Hom}_H(\mathbb{Z}G, A)$$

and defining an action of G on an H-homomorphism $\varphi\colon \mathbb{Z}G \to A$ by $(g\varphi)(x) = \varphi(xg)$ for all $x \in \mathbb{Z}G$. In the case where $H = 1$, then A is just abelian group, and in this case we simplify notation by writing $\mathrm{M}^G(A) = \mathrm{M}^G_1(A)$ and we call this the **coinduced** module associated to A. A G-module B is called **coinduced** if it is isomorphic to $\mathrm{M}^G(A)$ for some abelian group A. For instance, $\mathbb{Z}G$ itself is co-induced since $\mathbb{Z}G \cong \mathrm{M}^G(\mathbb{Z})$. Let $n\varphi_g\colon \mathbb{Z}G \to \mathbb{Z}$ be the homomorphism defined by $n\varphi_g(g) = n$ and $n\varphi_g(g') = 0$ for all $g' \neq g$ in G. Then note that

$$g' \cdot n\varphi_g = n\varphi_{gg'^{-1}}.$$

So the left action of $\mathbb{Z}G$ on $\mathrm{M}^G(\mathbb{Z})$ is given by $g \cdot x = xg^{-1}$. Consider the map $\psi\colon \mathbb{Z}G \to \mathrm{M}^G(\mathbb{Z})$ induced by $x \mapsto x^{-1}$ for all $x \in G$. Then note that

$$\psi(gx) = x^{-1}g^{-1} = g \cdot x^{-1} = g \cdot \psi(x).$$

Let us now make a few remarks:

1. If A is divisible (meaning $nA = A$ for every nonzero $n \in \mathbb{Z}$), then $\mathrm{M}^G(A)$ is an injective G-module.

2. If A is a G-module, then we have a natural injective map $A \to \mathrm{M}^G(A)$ given by sending $a \in A$ to the homomorphism $\mu_a \colon \mathbb{Z}G \to A$ defined by $\mu_a(x) = xa$ for all $x \in \mathbb{Z}G$. Note that μ_a is a G-module homomorphism since if $g \in G$ then
$$\mu_a(gx) = (gx)a = g(xa) = g\mu_a(x).$$
3. If G/H is finite, say $|G/N| = n$, then we have non-canonical H-isomorphisms
$$\mathrm{M}_H^G(A) \cong Ax_1 \oplus \cdots \oplus Ax_n \cong A \otimes_H \mathbb{Z}G$$
where $x_1, \dots, x_n \in G$ is some choice of coset representatives. This follows from the fact that $\mathbb{Z}G$ is a finite free H-module:
$$\mathbb{Z}G = \mathbb{Z}Hx_1 \oplus \cdots \oplus \mathbb{Z}Hx_n$$
In this case, we can say that a G-module B is coinduced if and only if it is G-isomorphic to $A \otimes_{\mathbb{Z}} \mathbb{Z}G$ for some abelian group A. One immediately sees from this that if B and B' are G-modules with B coinduced, then $B \otimes_{\mathbb{Z}} B'$ is coinduced also.

The following proprosition is often referred to as Shapiro's Lemma and is a consequence of tensor-hom adjointness and the fact that the property of being projective is stable under composition:

Proposition 4.2. *(Shapiro's Lemma) Let A be an H-module. We have a canonical isomorphism*
$$\mathrm{H}(G, \mathrm{M}_H^G(A)) \simeq \mathrm{H}(H, A)$$
of graded modules. In particular, if $H = 1$ (so A is just an abelian group), then we have an isomorphism
$$\mathrm{H}^i(G, \mathrm{M}^G(A)) = \begin{cases} A & \text{if } i = 0 \\ 0 & \text{else} \end{cases}$$

Proof. Let P be a projective resolution of $\mathbb{Z}$ over $\mathbb{Z}G$. Since $\mathbb{Z}G$ is a free $\mathbb{Z}H$-module, it follows that P is a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}H$-module as well. Thus
$$\begin{aligned} \mathrm{H}(G, \mathrm{M}_H^G(A)) &= \mathrm{Ext}_G(\mathbb{Z}, \mathrm{Hom}_H(\mathbb{Z}G, A)) \\ &= \mathrm{H}(\mathrm{Hom}_G(P, \mathrm{Hom}_H(\mathbb{Z}G, A))) \\ &\simeq \mathrm{H}(\mathrm{Hom}_H(P \otimes_G \mathbb{Z}G, A)) \\ &\simeq \mathrm{H}(\mathrm{Hom}_H(P, A)) \\ &= \mathrm{Ext}_H(\mathbb{Z}, A) \\ &= \mathrm{H}(H, A). \end{aligned}$$
□

Let us work out the action of G on $\mathrm{M}_H^G(A)$ in the case where H has finite index n in G. Let $x_1, \dots, x_n$ be a choice of left coset representatives. Every element in G can be expressed in the form hx_i for unique $h \in H$ and unique $1 \le i \le n$. Now let $a\varepsilon_i \colon \mathbb{Z}G \to A$ be the H-linear map induced by
$$(a\varepsilon_i)(hx_j) = \begin{cases} 0 & \text{if } j \neq i \\ ha & \text{if } j = i \end{cases}$$
Clearly $a\varepsilon_i$ is H-linear and every H-linear map $\varphi \colon \mathbb{Z}G \to A$ can be expressed as
$$\varphi = a_1\varepsilon_1 + \cdots + a_n\varepsilon_n$$
for unique $a_1, \dots, a_n \in A$. This gives us a decomposition $\mathrm{M}_H^G(A) \cong A^n$ as abelian groups. To see how the G-action looks, note that for each $g \in G$ and $1 \le i \le n$, there exists a unique $1 \le g(i) \le n$ and a unique $h_{g,i} \in H$ such that $x_{g(i)}g = h_{g,i}x_i$. This implies
$$g(a\varepsilon_i) = h_{g,i}(a)\varepsilon_{i_g}.$$
Note if we set $h_g = h_{g,1}h_{g,2} \cdots h_{g,n}$, then the map $g \mapsto h_g$ gives a well-defined group homomorphism $G \to H^{\mathrm{ab}}$ which is called the **transfer** map.

Now let us work out the action of G on $\mathbb{Z}G \otimes_H A$ in the case where $[G : H] = n$. Let us set $y_i = x_i^{-1}$ for all $1 \le i \le n$. Then $y_1, \dots, y_n$ is a complete set of right coset representatives. Every element in G can be expressed in the form y_ih for unique $h \in H$ and unique $1 \le i \le n$. Furthermore, every element in $\mathbb{Z}G \otimes_H A$ can be expressed in the form
$$y_1 \otimes a_1 + \cdots + y_n \otimes a_n$$

for unique $a_1, \ldots, a_n \in A$. This gives us a decomposition $\mathbb{Z}G \otimes_H A \cong A^n$. To see how the G-action looks, note that for each $g \in G$ and $1 \leq i \leq n$, we have $gy_i = y_{g^{-1}(i)} h^{-1}_{g^{-1}, g^{-1}(i)}$. Therefore

$$\begin{aligned} g(y_i \otimes a) &= gy_i \otimes a \\ &= y_{g^{-1}(i)} h^{-1}_{g^{-1}, g^{-1}(i)} \otimes a \\ &= y_{g^{-1}(i)} \otimes h^{-1}_{g^{-1}, g^{-1}(i)}(a) \end{aligned}$$

Proposition 4.3. *Let A be a G-module and let N be a normal subgroup of finite index in G. Then we have an isomorphism*

$$\Phi\colon \mathrm{Hom}_H(\mathbb{Z}G, A) \to A \otimes_{\mathbb{Z}} \mathbb{Z}[G/H],$$

given by

$$\Phi(\varphi) = \sum_{i=1}^{n} x_i \varphi(x_i^{-1}) \otimes \overline{x}_i,$$

where $x_1, \ldots, x_n$ is a choice of coset representatives of G/N and where the G-action on the tensor product on the right is the diagonal action via the rule $g(a \otimes \overline{x}_i) = ga \otimes \overline{gx_i}$.

Proof. We have

$$\begin{aligned} \Phi(g\varphi) &= \sum_{i=1}^{n} x_i (g\varphi)(x_i^{-1}) \otimes \overline{x}_i \\ &= \sum_{i=1}^{n} x_i (\varphi(x_i^{-1} g)) \otimes \overline{x}_i \\ &= \sum_{i=1}^{n} g x_i (\varphi(g x_i)^{-1} g) \otimes \overline{g x_i} \\ &= g \sum_{i=1}^{n} x_i (\varphi(x_i^{-1})) \otimes \overline{x}_i \\ &= g\Phi(\varphi). \end{aligned}$$

This shows that Φ is G-linear. Note in particular that

$$\Phi(a\varepsilon_j) = a \otimes \overline{x}_j,$$

so clearly Φ is an isomorphism. $\square$

4.2.1 Resriction and Corestriction Maps

Using Shapiro's Lemma, we define two basic maps relating the cohomology of a group with the cohomology of one of its subgroups.

1. Let A be a G-module and let H be a subgroup of G. The **restriction** map is given by

   $$\mathrm{Res}\colon \mathrm{H}(G, A) \to \mathrm{H}(G, \mathrm{M}_H^G(A)) \simeq \mathrm{H}(H, A),$$

   where the first map is induced by the inclusion $A \hookrightarrow \mathrm{M}_H^G(A)$ and where the isomorphism comes from Shapiro's Lemma. In particular, the restriction map in cohomological degree 0 is just the natural inclusion $A^G \hookrightarrow A^H$.

2. Let A be a G-module and let H be a subgroup of G of finite index n. Given an H-homorphism $\varphi\colon \mathbb{Z}G \to A$ we define a G-homomorphism $\varphi_H^G\colon \mathbb{Z}G \to A$ by setting $\varphi_H^G = \sum_{i=1}^n x_i(\varphi x_i^{-1})$ where $x_1, \ldots, x_n$ is a system of left coset representatives for H in G. Note that if $(x_i h_i)$ were another choice of representatives where $h_i \in H$, then we'd have

   $$x_i h_i (\varphi h_i^{-1} x_i^{-1}) = x_i h_i h_i^{-1} (\varphi x_i^{-1}) = x_i (\varphi x_i^{-1})$$

   for all i since φ is an H-homomorphism. Furthermore, φ_H^G is a G-module homomorphism since if $g \in G$ and $z \in \mathbb{Z}G$ then

   $$\sum_{i=1}^{n} x_i \varphi(x_i^{-1} g z) = g \left(\sum_{i=1}^{n} (g^{-1} x_i) \varphi((g^{-1} x_i)^{-1} z) \right) = g \left(\sum_{i=1}^{n} x_i \varphi(x_i^{-1} z) \right),$$

as the $(g^{-1}x_i)$ forms another system of left coset representatives. Thus the assignment $\varphi \mapsto \varphi_H^G$ gives a well-defined map $\mathrm{M}_H^G(A) \to \mathrm{M}_G^G(A) \simeq A$. Taking cohomology and applying Shapiro's lemma we thus get a map

$$\mathrm{Cor}\colon \mathrm{H}(H, A) \simeq \mathrm{H}(G, \mathrm{M}_H^G(A)) \to \mathrm{H}(G, A)$$

called the **corestriction map**. In particular, note that if $\varphi = \mu_a$ for some $a \in A$, then $\varphi_H^G = n\mu_a$.

Proposition 4.4. *Let A be a G-module and let H be a subgroup of G of finite index n. Then the composite*

$$\mathrm{Cor} \circ \mathrm{Res}\colon \mathrm{H}(G, A) \to \mathrm{H}(G, A)$$

are given by multiplication by n.

Proof. If $\varphi\colon \mathbb{Z}G \to A$ is a G-homomorphism, then for all $x \in \mathbb{Z}G$ we have

$$\varphi_H^G(x) = \sum g_i \varphi(g_i^{-1}x) = \sum g_i g_i^{-1} \varphi(x) = n\varphi(x).$$

□

Corollary 10. *Assume G is a finite group of order n. Then the elements of $\mathrm{H}^i(G, A)$ have finite order dividing n for all G-modules A and all integers $i > 0$.*

4.2.2 Inflation Maps

Let N be a normal subgroup of G. The canonical quotient homomorphism $G \to G/N$ induces a ring homomorphism $\mathbb{Z}G \to \mathbb{Z}[G/N]$. If A is a G-module, then we can transport it to a G/N-module via the ring homomorphism $\mathbb{Z}G \to \mathbb{Z}[G/N]$ in two ways. The first way involves taking a tensor product:

$$\mathbb{Z}[G/N] \otimes_{\mathbb{Z}G} A \simeq A_N = A/\langle \{xa - a \mid a \in A \text{ and } x \in N\}\rangle,$$

where the isomorphism is given by $\overline{1} \otimes a \mapsto \overline{a}$. The second way involves taking hom:

$$\mathrm{Hom}_G(\mathbb{Z}[G/N], A) \simeq A^N = \{a \in A \mid xa = a \text{ for all } x \in N\},$$

where the isomorphism is given by $\varphi \mapsto \varphi(\overline{1})$. This way is related to cohomology whereas the first way is related to homology, thus for the moment we will focus on the second way. Here we transported A to the G/N-module A^N where the G/N scalar-multiplication is given by $\overline{g}a = ga$ (this is well-defined since $a \in A^N$). In particular, if $N = G$, then this transports the G-module A to the abelian group $\mathrm{H}^0(G, A)$.

Now the group homomorphism $G \to G/N$ together with the G-module homomorphism $A^N \to A$ induces a canonical base change map in Ext:

$$\mathrm{Inf}\colon \mathrm{H}(G/N, A^N) = \mathrm{Ext}_{\mathbb{Z}[G/N]}(\mathbb{Z}, A^N) \to \mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A^N) \to \mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A) := \mathrm{H}(G, A),$$

which we call the **inflation map**. In more detail, this map is constructed as follows: let P be a projective resolution of $\mathbb{Z}$ over G and let Q be a projective resolution of $\mathbb{Z}$ over G/N. Lift the identity map $\mathbb{Z} \to \mathbb{Z}$ to a comparison map $P \to Q$ of G-complexes. Then from this comparison map together with the G-module homomorphism, we obtain the following sequence of complexes:

$$\mathrm{Hom}_{G/N}(Q, A^N) = \mathrm{Hom}_G(Q, A^N) \to \mathrm{Hom}_G(P, A^N) \to \mathrm{Hom}_G(P, A) \tag{17}$$

Taking cohomology of (17) gives us the inflation map. In particular, calculating the inflation map in terms of the standard resolutions of $\mathbb{Z}$ amounts to inflating an i-cocycle $\mathbb{Z}[(G/N)^{i+1}] \to A^N$ to the map $\mathbb{Z}[G^{i+1}] \to A^N \subseteq A$ induced by the projection $G \to G/N$. Similarly, the restriction of a cocycle $\mathbb{Z}[G^{i+1}] \to A$ to a subgroup H is given by restricting it to a map $\mathbb{Z}[H^{i+1}] \to A$.

4.2.3 Completed Resolution

4.3 Group Extensions

Let G and A be groups. An **extension** of G by A is a group E, together with an exact sequence:

$$1 \longrightarrow A \xrightarrow{\alpha} E \xrightarrow{\beta} G \longrightarrow 1$$

We shall denote such an extension by (α, E, β). If G and A are understood from context, then we simply say (α, E, β) is an extension. We denote by $\mathrm{E}(G, A)$ to be the set of extensions of G by A. Given two extensions (α, E, β) and (α', E', β') of G by A, we say they are **isomorphic**, denoted $(\alpha, E, \beta) \cong (\alpha', E, \beta')$, if there exists an isomorphism $\varphi\colon E \to E'$ such that $\varphi\alpha = \alpha'$ and $\beta = \beta'\varphi$. In other words, we say they are isomorphic if the following diagram is commutative

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "1_A"] & E \arrow[r, "\beta"] \arrow[d, "\varphi"] & G \arrow[r] \arrow[d, "1_G"] & 1 \\
1 \arrow[r] & A \arrow[r, "\alpha'"] & E' \arrow[r, "\beta'"] & G \arrow[r] & 1
\end{tikzcd}$$

where 1_A and 1_G denote the identity maps on A and G respectively. Clearly $\cong$ gives an equivlance relation on $\mathrm{E}(G, A)$, and so we may consider the set of all isomorphism classes of extensions of G by A which we denote by

$$[\mathrm{E}(G, A)] := \mathrm{E}(G, A)/\cong .$$

The set of all extensions of G by A which are isomorphic to the extension (α, E, β) is called the **isomorphism class** of (α, E, β) and is denoted by $[\alpha, E, \beta]$.

Remark 13. Let (α, E, β) and (α', E', β') be extensions of G by A. If $\varphi \colon E \to E'$ is an isomorphism of groups, then it does not necessarily give rise to an isomorphism $\varphi \colon (\alpha, E, \beta) \to (\alpha', E', \beta')$ of extensions. Indeed, in order for φ to be an isomorphism of extensions, it needs to satisfy the extra constraints, namely $\alpha\varphi = \alpha'$ and $\beta'\varphi = \beta$.

Proposition 4.5. *Let $A \cong A'$ and $G \cong G'$ be isomorphisms of groups. Then we have* $[\mathrm{E}(G, A)] \cong [\mathrm{E}(G', A')]$.

Proof. Let $\varepsilon \colon A \to A'$ and $\delta \colon G' \to G$ be isomorphisms. Define $\Psi_{\varepsilon,\delta} \colon \mathrm{E}(G', A') \to \mathrm{E}(G, A)$ by

$$\Psi_{\varepsilon,\delta}((\alpha', E, \beta')) = (\alpha'\varepsilon, E, \delta\beta')$$

for all $(\alpha', E, \beta') \in \mathrm{E}(G, A)$. Then $\Psi_{\varepsilon,\delta}$ is a bijection whose inverse is defined by

$$\Psi_{\varepsilon,\delta}((\alpha, E, \beta)) = (\alpha\varepsilon^{-1}, E, \delta^{-1}\beta)$$

for all $(\alpha, E, \beta) \in \mathrm{E}(G, A)$. Furthermore, suppose $\varphi \colon (\alpha', E, \beta') \to (\widetilde{\alpha}', \widetilde{E}, \widetilde{\beta}')$ is an isomorphism of extensions of G' by A' (so $\alpha'\varphi = \widetilde{\alpha}'$ and $\widetilde{\beta}'\varphi = \beta'$). Then observe that $\varphi\widetilde{\alpha}'\varepsilon = \alpha'\varepsilon$ and $\delta\widetilde{\beta}'\varphi = \delta\beta'$. Thus $\varphi \colon (\alpha'\varepsilon, E, \delta\beta') \to (\widetilde{\alpha}'\varepsilon, E, \delta\widetilde{\beta}')$ is an isomorphism of extensions of G by A. It follows that $\Psi_{\varepsilon,\delta}$ preserves the isomorphism classes and thus passes to a bijection $[\Psi_{\varepsilon,\delta}] \colon [\mathrm{E}(G, A)] \to [\mathrm{E}(G', A')]$ defined by

$$[\Psi_{\varepsilon,\delta}]([\alpha', E, \beta']) = [\alpha'\varepsilon, E, \delta\beta']$$

for all $[\alpha, E, \beta] \in [\mathrm{E}(G, A)]$. $\square$

Oftentimes we will know a short exact sequence of the form

$$1 \longrightarrow N \xrightarrow{\iota} E \xrightarrow{\pi} E/N \longrightarrow 1$$

where N is a normal subgroup of E where $A \cong N$ and $G \cong G/N$. Note that (ι, E, π) is not yet an extension of G by A. In order to for us to truly get an extension of G by A, we must specify the isomorphisms $A \cong N$ and $G \cong G/N$. In particular, let $\varepsilon \colon A \to N$ and $\delta \colon E/N \to G$ be our specificed isomorphisms. Then $(\iota\varepsilon, E, \delta\pi)$ is an extension of G by A:

$$1 \longrightarrow A \xrightarrow{\iota\varepsilon} E \xrightarrow{\delta\pi} G \longrightarrow 1$$

We can obtain different extensions of G by A by varying the isomorphisms ε and δ. In particular, every such extension has the form $(\iota\varepsilon\sigma, E, \tau\delta\pi)$ for unique $\sigma \in \operatorname{Aut} A$ and $\tau \in \operatorname{Aut} G$. It may be possible that there exists $\sigma \neq \sigma'$ and $\tau \neq \tau'$ such that $(\iota\varepsilon\sigma, E, \tau\delta\pi) \ncong (\iota\varepsilon\sigma', E, \tau'\delta\pi)$. Thus it is important to keep track of these automorphisms. For instance, consider the special case where $A = N$ and where $G = E/N$. Let $(\iota\sigma, E, \tau\pi)$ be an extension of G by A for some $\sigma \in \operatorname{Aut} A$ and $\tau \in \operatorname{Aut} G$. Then $\varphi \colon (\iota, E, \pi) \to (\iota\sigma, E, \tau\pi)$ is an isomorphism if and only if $\varphi \in \operatorname{Aut} E$ such that $\varphi|_A = \sigma$ and $\overline{\varphi} = \tau$. Such automorphisms need not exist.

Example 4.3. Consider the case where $A = C_2 = \langle a \rangle$ and where $G = C_2^2 = \langle b, c \rangle$. The quaternion qroup $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ fits in the short exact sequence

$$1 \longrightarrow \{\pm 1\} \xrightarrow{\iota} Q_8 \xrightarrow{\pi} Q_8/\{\pm 1\} \longrightarrow 1$$

We must specify the isomorphisms $\{\pm 1\} \cong C_2$ and $Q_8/\{\pm 1\} \cong C_2^2$ in order for us to truly get an extension of C_2^2 by C_2. With that said, let $\varepsilon \colon C_2 \to \{\pm 1\}$ be the unique homorphism such that $\varepsilon(a) = -1$ and let $\delta \colon Q_8/\{\pm 1\} \to C_2^2$ be the unique homorphism such that $\delta(\bar{i}) = b$ and $\delta(\bar{j}) = c$. Then $(\iota\varepsilon, Q_8, \delta\pi)$ is an extension of C_2^2 by C_2:

$$1 \longrightarrow C_2 \xrightarrow{\iota\varepsilon} Q_8 \xrightarrow{\delta\pi} C_2^2 \longrightarrow 1$$

Let's get a different extension of C_2^2 by C_2 by changing δ, say by $\widetilde{\delta}\colon Q_8/\{\pm 1\} \to C_2^2$ where $\widetilde{\delta}$ is the unique homomorphism such that $\widetilde{\delta}(\bar{i}) = c$ and $\widetilde{\delta}(\bar{j}) = b$. We ask, is $(\iota\varepsilon, Q_8, \delta\pi)$ isomorphic to $(\iota\varepsilon, Q_8, \widetilde{\delta}\pi)$? The answer is yes. Indeed, let $\varphi\colon Q_8 \to Q_8$ be the unique homorphism such that $\varphi(i) = j$ and $\varphi(j) = i$. Then it's to check that φ is gives rise to such an isomorphism.

Another short exact sequence we are familiar with is given by

$$1 \longrightarrow \langle r^2 \rangle \xrightarrow{\ \iota\ } D_4 \xrightarrow{\ \pi\ } D_4/\langle r^2 \rangle \longrightarrow 1$$

where D_4 is the Dihedral group of order 8. Again, to make this an extension of C_2^2 by C_2, we choose isomorphisms $\varepsilon'\colon C_2 \to \langle r^2 \rangle$ and $\delta'\colon D_4/\langle r^2 \rangle \to C_2^2$. Then $(\iota\varepsilon', D_4, \delta'\pi)$ is an extension of C_2^2 by C_2. Now we ask, is $(\iota\varepsilon, Q_8, \delta\pi)$ isomorphic to $(\iota\varepsilon', D_4, \delta'\pi)$? The answer is no, but for a somewhat trivial reason: Q_8 and D_4 are not isomorphic groups.

4.3.1 Sections

Definition 4.1. Let (α, E, β) be an extension of G by A.

1. A **right section** of (α, E, β) is a function $\widetilde{\beta}\colon G \to E$ such that $\beta\widetilde{\beta} = 1_G$. If $\widetilde{\beta}$ is a homomorphism, then we say $\widetilde{\beta}$ is a **right splitting section** and that it **splits** (α, E, β) **on the right**.

2. A **left section** of (α, E, β) is a function $\widetilde{\alpha}\colon E \to A$ such that $\widetilde{\alpha}\alpha = 1_A$. If $\widetilde{\alpha}$ is a homomorphism, then we say $\widetilde{\alpha}$ is a **left splitting section** and that it **splits** (α, E, β) **on the left**.

Proposition 4.6. *Let (α, E, β) be be an extension of G by A. Then there exists a right splitting section of (α, E, β) if and only if there exists a homomorphism $\rho\colon G \to \mathrm{Aut}(A)$ such that $(\alpha, E, \beta) \cong (\iota_1, A \rtimes_\rho G, \pi_2)$.*

Proof. To keep notation clean we identify A with $\alpha(A)$. In particular, we assume that A is a normal subgroup of E and that α is the inclusion map. Let $\widetilde{\beta}\colon G \to E$ be a right splitting section of (α, E, β). Define $\rho\colon G \to \mathrm{Aut}(A)$ by $\rho(g) = \mathrm{c}_{\widetilde{\beta}(g)}$ for all $g \in G$, where $\mathrm{c}_{\widetilde{\beta}(g)}$ is conjugation map given by

$$\mathrm{c}_{\widetilde{\beta}(g)}(a) = \widetilde{\beta}(g)a\widetilde{\beta}(g)^{-1}$$

for all $a \in A$. Note that $\mathrm{c}_{\widetilde{\beta}(g)}$ lands in A since A is a normal subgroup. Since conjugation and $\widetilde{\beta}$ are both homomorphisms, it follows that ρ is a homomorphism. Now define $\varphi\colon (\alpha, E, \beta) \to (\iota_1, A \rtimes G, \pi_2)$ by

$$\varphi(x) = (x\widetilde{\beta}\beta(x)^{-1}, \beta(x))$$

for all $x \in E$. Observe that $x\widetilde{\beta}\beta(x)^{-1}$ really does belong to A since

$$\begin{aligned}
\beta(x\widetilde{\beta}\beta(x)^{-1}) &= \beta(x)\beta\widetilde{\beta}\beta(x)^{-1} \\
&= \beta(x)\beta(x)^{-1} \\
&= e
\end{aligned}$$

and $A = \ker\beta$. Also φ is a group homomorphism. Indeed, let $x, y \in E$. Then we have

$$\begin{aligned}
\varphi(x)\varphi(y) &= (x\widetilde{\beta}\beta(x)^{-1}, \beta(x)) \cdot (y\widetilde{\beta}\beta(y)^{-1}, \beta(y)) \\
&= (x\widetilde{\beta}\beta(x)^{-1}\mathrm{c}_{\widetilde{\beta}\beta(x)}(y\widetilde{\beta}\beta(y)^{-1}), \beta(x)\beta(y)) \\
&= (x\widetilde{\beta}\beta(x)^{-1}\widetilde{\beta}\beta(x)y\widetilde{\beta}\beta(y)^{-1}\widetilde{\beta}\beta(x)^{-1}, \beta(xy)) \\
&= (xy\widetilde{\beta}\beta(y)^{-1}\widetilde{\beta}\beta(x)^{-1}, \beta(xy)) \\
&= (xy\widetilde{\beta}\beta(xy)^{-1}, \beta(xy)) \\
&= \varphi(xy).
\end{aligned}$$

It is straightforward to check that the map $\psi\colon A \rtimes G \to E$, defined by

$$\psi(a, g) = a\widetilde{\beta}(g)$$

for all $a \in A$ and $g \in G$, is the inverse to φ. In particular, this implies φ is an isomorphism. It is also straightforward to check that φ is an isomorphism of extensions, that is, $\varphi\alpha = \iota_1$ and $\pi_2\varphi = \beta$. We leave the details as an exercise. $\square$

Proposition 4.7. *Let (E, α, β) be be an extension of G by A. Then there exists a left splitting section of (E, α, β) if and only if $(E, \alpha, \beta) \cong (A \times G, \iota_1, \pi_2)$ where $\iota_1 \colon A \to A \times G$ and $\pi_2 \colon A \times G$ are defined by*

$$\iota_1(a) = (a, e) \quad \text{and} \quad \pi_2(a, g) = g$$

for all $a \in A$ and $g \in G$.

Proof. The proof is similar in nature to the one above. $\square$

4.4 Conjugation Action of G on $\mathrm{Z}(A)$

Let (α, E, β) be a group extension of G by A. To simplify notation in what follows, we assume that A is a normal subgroup of G (so α is just the inclusion map). In this case, we will write E instead of (ι, E, β) to denote this extension. We define an action of G on $\mathrm{Z}(A)$ as follows: for each $g \in G$ we choose $e_g \in E$ such that $\beta(e_g) = g$. Thus the map $g \mapsto e_g$ is a right section of (α, E, β). Note that each element in E can be expressed in the form ae_g for unique $a \in A$ and unique $g \in G$, where by uniqueness, we mean that $ae_g = a'e_{g'}$ if and only if $a = a'$ and $g = g'$. Now, for each $g \in G$ and $x \in \mathrm{Z}(A)$, we define

$$g \cdot x = e_g x e_g^{-1}. \tag{18}$$

In a moment, we will show that (18) is well-defined, but first let us check that $e_g x e_g^{-1} \in \mathrm{Z}(A)$. Let $a \in A$. Then since A is normal in E, we have $ae_g = e_g a_g$ for some $a_g \in A$. Therefore

$$\begin{aligned} ae_g x e_g^{-1} &= e_g a_g x e_g^{-1} \\ &= e_g x a_g e_g \\ &= e_g x e_g a. \end{aligned}$$

It follows that $e_g x e_g^{-1} \in \mathrm{Z}(A)$. Thus (18) at least lands in $\mathrm{Z}(A)$. Now let us show that it is well-defined. Let ae_g be another lift of g with respect to β, where $a \in A$. Then we have

$$\begin{aligned} ae_g x (ae_g)^{-1} &= ae_g x e_g^{-1} a^{-1} \\ &= e_g x e_g^{-1} a a^{-1} \\ &= e_g x e_g^{-1}, \end{aligned}$$

where the last equality follows since $e_g x e_g^{-1} \in \mathrm{Z}(A)$. Thus (18) is well-defined. Finally, let us show that this map is a group action of G on $\mathrm{Z}(A)$. Clearly the identity element 1 in G fixes all of $\mathrm{Z}(A)$. Let $g, h \in G$ and $x \in \mathrm{Z}(A)$. Then there exists a unique $a_{g,h} \in A$ such that $e_g e_h = a_{g,h} e_{gh}$. Thus we have

$$\begin{aligned} g \cdot (h \cdot x) &= g \cdot e_h x e_h^{-1} \\ &= e_g e_h x e_h^{-1} e_g^{-1} \\ &= e_g e_h x (e_g e_h)^{-1} \\ &= a_{g,h} e_{gh} x (a_{g,h} e_{gh})^{-1} \\ &= a_{g,h} e_{gh} x e_{gh}^{-1} a_{g,h}^{-1} \\ &= e_{gh} x e_{gh}^{-1} a_{g,h} a_{g,h}^{-1} \\ &= e_{gh} x e_{gh}^{-1} \\ &= gh \cdot x. \end{aligned}$$

It follows that (18) defined a group action.

Remark 14. Let K_A denote the set of conjugacy classes of elements of A. If $a \in A$, then we denote its conjugacy class by $[a] = \{bab^{-1} \mid b \in A\}$. For each $g \in G$ and $a \in A$, we define

$$g \cdot [a] = [e_g a e_g^{-1}]. \tag{19}$$

One can check that (19) gives a well-defined action of G on K_A. Note that the conjugacy classes which consist of only one element correspond to the elements in $\mathrm{Z}(A)$, and the action (19) restricted to $\mathrm{Z}(A)$ can be viewed as the action (18) described above. Furthermore, one can view (19) as defining a homomorphism $G \to \operatorname{Out} A$. In general, there may be other homomorphisms $G \to \operatorname{Out} A$ which are not of the form (19). Later on, we will see how to associate to any homomorphism $\psi \colon G \to \operatorname{Out} A$ an element $c(\psi)$ of $\mathrm{H}^3(G, \mathrm{Z}(A))$. We will then show that ψ is a homomorphism coming from (19) if and only if $c(\psi) = 0$. Thus $\mathrm{H}^3(G, \mathrm{Z}(A))$ can be seen as measuring the obstruction for a homomorphism $\psi \colon G \to \operatorname{Out} A$ to be a homomorphism coming from (19).

4.5 Interpreting $\mathrm{H}^2(G, A)$ as Isomorphism Classes of Extensions of G by A

Now we assume A is abelian (so $A = \mathrm{Z}(A)$). For each $g, h \in G$ there exists a unique $a_{g,h} \in A$ such that

$$e_g e_h = a_{g,h} e_{gh}.$$

What can we say about the $a_{g,h}$? Well since E is a group, the associativity law tells us that

$$\begin{aligned} a_{g,h} a_{gh,k} e_{ghk} &= a_{g,h} e_{gh} e_k \\ &= (e_g e_h) e_k \\ &= e_g (e_h e_k) \\ &= e_g a_{h,k} e_{hk} \\ &= e_g a_{h,k} e_g^{-1} e_g e_{hk} \\ &= (g \cdot a_{h,k}) a_{g,hk} e_{ghk}. \end{aligned}$$

It follows that

$$(g \cdot a_{h,k}) a_{gh,k}^{-1} a_{g,hk} a_{g,h}^{-1} = 1.$$

Thus the map $a_{(-,-)} \colon G^2 \to A$ is a 2-cocycle. Note that if we had chosen a different section, say $g \mapsto b_g e_g$, then

$$\begin{aligned} (b_g e_g)(b_h e_h) &= b_g e_g b_h e_h \\ &= b_g e_g b_h e_g^{-1} e_g e_h \\ &= b_g (g \cdot b_h) e_g e_h \\ &= b_g (g \cdot b_h) a_{g,h} e_{gh} \\ &= (\delta b_{g,h}) a_{g,h} e_{gh}. \end{aligned}$$

Thus choosing a different section would give us a 2-cocycle which is cohomologous to $a_{(-,-)}$. Thus if E is an extension we arrive at the following theorem:

Theorem 4.2. *With the notation above, we have a bijection*

$$\left\{ \begin{array}{c} \textit{isomorphism classes} \\ \textit{of extensions of G by A} \end{array} \right\} \cong \mathrm{H}^2(G, A).$$

Moreover, in this bijection, the split extensions correspond to the zero element in $\mathrm{H}^2(G, A)$.

Proof. Let (α, E, β) be an extension of G by A. From the discussion above, a right section of the extension (α, E, β) gives rise to a well-defined element in $\mathrm{H}^2(G, A)$. Furthermore, this element does not depend on the choice of a right section of (α, E, β). Indeed, choose a right section of the extension E, say $\widetilde{\beta} \colon G \to E$. Then given $g, h \in G$, we have

$$\widetilde{\beta}(g)\widetilde{\beta}(h) = \alpha(a_{g,h})\widetilde{\beta}(gh)$$

for a unique $a_{g,h} \in A$. As noted above, the function $a_{(-,-)} \colon G^2 \to A$ is a 2-cocycle. A different right section of (α, E, β) has the form $b_{(-)}\widetilde{\beta}$ where $b_{(-)} \colon G \to A$ is a function. Then as noted above, the corresponding 2-cocyle that $b_{(-)}\widetilde{\beta}$ induces is $\delta b_{(-)}\widetilde{\beta}$. Thus (α, E, β) induces a well-defined element in $\mathrm{H}^2(G, A)$, which we shall denote by $\{\alpha, E, \beta\}$. Thus we have a map $\Phi \colon \mathrm{E}(G, A) \to \mathrm{H}^2(G, A)$ given by

$$\Phi(\alpha, E, \beta) = \{\alpha, E, \beta\}$$

for all $(\alpha, E, \beta) \in \mathrm{E}(G, A)$. Note that if $\varphi \colon (\alpha, E, \beta) \to (\alpha', E', \beta')$ is an isomorphism of extensions of G by A, then $\varphi\widetilde{\beta}$ is a right section of (α', E', β'). Given $g, h \in G$, we have

$$\begin{aligned} \varphi\widetilde{\beta}(g)\varphi\widetilde{\beta}(h) &= \varphi(\widetilde{\beta}(g)\widetilde{\beta}(h)) \\ &= \varphi(\alpha(a_{g,h})\widetilde{\beta}(gh)) \\ &= \varphi(\alpha(a_{g,h}))\varphi\widetilde{\beta}(gh)) \\ &= \alpha'(a_{g,h})\varphi\widetilde{\beta}(gh). \end{aligned}$$

Thus the right section $\varphi\widetilde{\beta}$ of (α', E', β') induces the same 2-cocyle $a_{(-,-)}$ as the right section $\widetilde{\beta}$ of (α, E, β). It follows that the map Φ preserves the isomorphism classes of extensions of G by A, and thus induces a map $[\Phi] \colon [\mathrm{E}(G, A)] \to \mathrm{H}^2(G, A)$ given by

$$[\Phi][\alpha, E, \beta] = \{\alpha, E, \beta\}$$

for all $[\alpha, E, \beta] \in [\mathrm{E}(G, A)]$. We claim that this map is a bijection:

This map is surjective: let $\overline{a_{(-,-)}}$ be an element in $\mathrm{H}^2(G, A)$ where $a_{(-,-)}$ is a normalized a 2-cocycle, where by "normalized" we mean $a_{1,1} = 1$ (every element in $\mathrm{H}^2(G, A)$ can be represented by a normalized 2-cocycle). Let $E = A \times G$ and defined a multiplication law on E by

$$(a, g)(b, h) = (a(g \cdot b)a_{g,h}, gh).$$

The 2-cocyle condition $a_{(-,-)}$ ensures that this multiplication is associative. Then noramlized condition on $a_{(-,-)}$ ensures that this multiplication is unital with identity element being $(1, 1)$. It is easy to see that (ι, E, π) is an extension of G by A where $\iota\colon A \to E$ and $\pi\colon E \to G$ are the obvious inclusion and projection maps. The right section $G \to E$ defined by $g \mapsto (1, g)$ clearly induces the same 2-cocycle $a_{(-,-)}$.

This map is injective: suppose (α, E, β) and (α', E', β') are two extensions of G by A such that $[\alpha, E, \beta] = [\alpha', E', \beta']$. Choose a right section $e_{(-)}\colon G \to E$ of (α, E, β) and choose a right section $e'_{(-)}\colon G \to E'$ of (α', E', β'). The corresponding 2-cocycles induced by $e_{(-)}$ and $e'_{(-)}$ are cohomologous; by changing $e'_{(-)}$ if necessary, we may assume that they are equal. In that case, the bijection $E \to E'$ defined by $ae_g \mapsto ae'_g$ is easily seen to induce an isomorphism of extensions. □

4.6 Interpreting $\mathrm{H}^1(G, A)$

Theorem 4.3. *Conjugacy classes of splittings of E are in bijective corresondence with the elements of* $\mathrm{H}^1(G, A)$.

Consider the short exact sequence

$$0 \longrightarrow A \longrightarrow A \rtimes G \longrightarrow G \longrightarrow 0 \tag{20}$$

A right splitting section of (20) has the form $g \mapsto (a_g, g)$. Note that

$$(a_g, g)(a_h, h) = (a_g + ga_h, gh)$$

implies $a_{gh} = ga_h + a_g$ for all $g, h \in G$. in particular that a_- is a 1-cocycle.

Proposition 4.8. *An automorphism $\varphi\colon E \to E$ which induces the identity on A and on E/A is of the form*

$$ae_g \mapsto a\beta_g e_g$$

where β is a 1-cocycle. It is an inner automorphism if and only if β is a coboundary.

Since φ induces the identity on E/A, it must map e_g to $\beta_g e_g$, where $\beta_g \in A$. Since φ induces the identity on A, we must have

$$\varphi(ae_g) = \varphi(a)\varphi(e_g) = a\beta_g e_g$$

We need to check that α is a 1-cocycle, i.e.

$$\beta_{gh} = \beta_g(g \cdot \beta_h)$$

We compute $\varphi(e_{gh})$ in two ways.

$$\varphi(e_{gh}) = \beta_{gh}e_{gh} = \beta_{gh}\alpha_{g,h}e_g e_h$$

4.7 The existence problem and its obstruction in $\mathrm{H}^3(G, \mathrm{Z}(A))$

Recall that if $E = (\alpha, E, \beta)$ is an extension of G by A, then we can obtain a group homomorphism $\phi\colon G \to \operatorname{Out} A$ as follows: we choose a right section of $\widetilde{\beta}\colon G \to E$ of E and define $\phi(g) \in \operatorname{Out} A$ by $\phi(g) = \overline{\mathrm{c}}_{\widetilde{\beta}(g)}$, that is,

$$\phi(g)[a] = [e_g a e_g^{-1}]. \tag{21}$$

Notice that if we had chosen a different section, say $g \mapsto b_g e_g$, then we'd have

$$\phi(g)[a] = [b_g e_g a e_g^{-1} b_g^{-1}] = [e_g a e_g^{-1}],$$

so this map is well-defined. It is also a group homomoprhism since

$$\begin{aligned}\phi(gh)[a] &= [e_{gh}ae_{gh}^{-1}] \\ &= [a_{g,h}e_g e_h a e_h^{-1} e_g^{-1} a_{g,h}^{-1}] \\ &= [e_g e_h a e_h^{-1} e_g^{-1}] \\ &= \varphi(g)\varphi(h)[a]\end{aligned}$$

for all $a \in A$. Whenever any $\phi\colon G \to \operatorname{Out} A$ is defined via (21), then we say it comes from the extension E. Now suppose $\psi\colon G \to \operatorname{Out} A$ is any group homomorphism. The question we ask now is, does ψ comes from an extension of G by A? What Eilenberg and Mac Lane did is to associate to ψ and element $c(\psi)$ of $\mathrm{H}^3(G, \mathrm{Z}(A))$ and to prove:

Theorem 4.4. *There exists an extension of G by A corresponding to ψ if and only if $c(\psi) = 0$.*

For every $g, h \in G$, choose $s_{g,h} \in A$ such that $s_{g,h}xs_{g,h}^{-1} = s_g s_h s_{gh}^{-1} x$. We can think of this equations like this: We can switch $s_{g,h}$ and x, where $s_{g,h}$ is to the left of x, at the cost of $s_g s_h s_{gh}^{-1} x$.

$$s_{g,h}x = s_g s_h s_{gh}^{-1} x s_{g,h}$$

Now define a 3-cocycle as follows

$$s_{g,h,k} = s_g s_{h,k} s_{g,hk} s_{gh,k}^{-1} s_{g,h}^{-1}$$

Let's show that $s_{g,h,k}$ is an element of $Z(A)$. We do this by showing the associated conjugation map by $s_{g,h,k}$ is trivial.

$$\begin{aligned}s_{g,h,k}xs_{g,h,k}^{-1} &= s_g s_{h,k} s_{g,hk} s_{gh,k}^{-1} s_{g,h}^{-1} x s_{g,h} s_{gh,k} s_{g,hk}^{-1} s_g s_{h,k}^{-1} \\ &= s_g s_{h,k} s_{g,hk} s_{gh,k}^{-1} s_{gh} s_h^{-1} s_g^{-1} x s_{gh,k} s_{g,hk}^{-1} s_g s_{h,k}^{-1} \\ &= s_g s_{h,k} s_{g,hk} s_{ghk} s_k^{-1} s_{gh}^{-1} s_{gh} s_h^{-1} s_g^{-1} x s_{g,hk}^{-1} s_g s_{h,k}^{-1} \\ &= s_g s_{h,k} s_{ghk} s_k^{-1} s_{gh}^{-1} s_{gh} s_h^{-1} s_g^{-1} x s_g s_{h,k}^{-1} \\ &= s_g s_{h,k} s_{hk} s_{ghk}^{-1} s_{ghk} s_k^{-1} s_{gh}^{-1} s_{gh} s_h^{-1} s_g^{-1} x s_{h,k}^{-1} \\ &= s_g s_h s_k s_{hk}^{-1} s_{hk} s_{ghk}^{-1} s_{ghk} s_k^{-1} s_{gh}^{-1} s_{gh} s_h^{-1} s_g^{-1} x \\ &= x\end{aligned}$$

4.8 Group Cohomology of Cyclic Group

Theorem 4.5. *Let G be a cyclic group and let A be a G-module. Then*

$$\mathrm{H}^i(G, A) \cong \mathrm{H}^{i+2}(G, A)$$

for all $i \in \mathbb{Z}$.

Proof. It suffices to specify an isomorphism $\mathrm{H}^{-1}(G, A) \cong \mathrm{H}^1(G, A)$. Given this, the general case follow from this by dimension shifting since

$$\mathrm{H}^i(G, A) \cong \mathrm{H}^{-1}(G, A^{i+1}) \cong \mathrm{H}^1(G, A^{i+1}) \cong \mathrm{H}^{i+2}(G, A).$$

The group Z_1 of 1-cocycles consists of all the crosed homomorphisms of G in A. Thus if $x \in Z_1$, then

$$x(g^k) = gx(g^{k-1}) + x(g) = \sum_{i=0}^{k-1} g^i x(g) \quad \text{and} \quad x(1) = 0.$$

It follows that

$$\mathrm{N}_G x(g) = \sum_{i=0}^{n-1} g^i x(g) = x(g^n) = x(1) = 0.$$

In other words, $x(g) \in_{\mathrm{N}_G} A$. Conversely, it is easy to see that if $a \in_{\mathrm{N}_G} A = Z_{-1}$ is a (-1)-cocycle, then

$$x(g) = a \quad \text{and} \quad x(g^k) = \sum_{i=0}^{k-1} g^i a$$

defines a 1-cocycle. Therefore the map $x \mapsto x(g)$ is an isomorphism from Z_1 to $Z_{-1} =_{\mathrm{N}_G} A$. Under this isomorphism, the group B_1 of 1-coboundaries is mapped to the group B_{-1} of (-1)-coboundaries. □

Example 4.4. Let $M \in \mathrm{GL}_n(\mathbb{Z})$ such that M has order p and let G be the cyclic group generated by M. We wish to calculate $\mathrm{H}^1(G, \mathbb{Z}^n)$ where $\mathbb{Z}^n$ is a G-module via the natural action. Let $\mu = \mu(t)$ be the minimal polynomial of M. Then μ factors at $\mu = (t-1)^k \Phi_p^m$ where

$$\Phi_p = t^{p-1} + t^{p-2} + \cdots + 1$$

is the pth cyclotomic polynomial for some $k, m \in \mathbb{N}$. By conjugating M by an appropriate matrix in $\mathrm{GL}_n(\mathbb{Z})$ if necessary, we may assume that M is expressed in rational normal form:

$$M = \begin{pmatrix} 1^{(k)} & 0 \\ 0 & C^{(m)} \end{pmatrix}$$

where $1^{(k)}$ is the $k \times k$ diagonal matrix with entry 1 and where $C^{(m)}$ is the $(p-1)m \times (p-1)m$ block diagonal matrix with entry C. In this case, one has

$$\Phi_p M = \begin{pmatrix} p^{(k)} & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad (t-1)M = \begin{pmatrix} 0 & 0 \\ 0 & (C-1)^{(m)} \end{pmatrix}.$$

In particular, we see that

$$\begin{aligned} \mathrm{H}^1(G, \mathbb{Z}^n) &\simeq \mathrm{H}_1(G, \mathbb{Z}^n) \\ &= \ker(\Phi_p M)/\mathrm{im}((t-1)M) \\ &\cong \mathrm{coker}((C-1)^{(m)}) \\ &= \mathrm{coker} \begin{pmatrix} 1^{(pm-2m)} & 0 \\ 0 & p^{(m)} \end{pmatrix} \\ &\cong (\mathbb{Z}/p)^m, \end{aligned}$$

where in the second line we used the fact that the smith normal form of $C-1$ is given by $\begin{pmatrix} 1^{(p-2)} & 0 \\ 0 & p \end{pmatrix}$.

4.9 Examples

Example 4.5. We have $\mathrm{Ext}(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2) \cong H^2(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2) \cong \mathbb{Z}_8$.
The quaternion group Q_8 fits in the short exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow Q_8 \longrightarrow Q_8/\{\pm 1\} \longrightarrow 1$$

a corresponding 2-cocycle is given by

f_2	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$(1,-1)$	1	-1	1	-1
$(-1,1)$	1	-1	-1	1
$(-1,-1)$	1	1	-1	-1

Suppose

f_1	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$f_1(g)$	1	1	1	-1

Then $f_2 d f_1$ would be

$f_2 d f_1$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$(1,-1)$	1	-1	-1	1
$(-1,1)$	1	1	-1	-1
$(-1,-1)$	1	-1	1	-1

However, all we did here was switch columns up. The dihedral group D_4 fits in the short exact sequence

$$1 \longrightarrow \langle r^2 \rangle \longrightarrow D_4 \longrightarrow D_4/\langle r^2 \rangle \longrightarrow 1$$

The corresponding 2-cocycle is given by

f_2	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$r=(1,-1)$	1	-1	1	-1
$s=(-1,1)$	1	-1	1	-1
$rs=(-1,-1)$	1	1	1	1

The dihedral group $(\mathbb{Z}/2\mathbb{Z})^2/\mathbb{Z}/2\mathbb{Z}$ fits in the short exact sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow 0$$

The corresponding 2-cocycle is given by

f_2	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$r=(1,-1)$	1	1	1	1
$s=(-1,1)$	1	1	1	1
$rs=(-1,-1)$	1	1	1	1

Example 4.6. The group $H^2(S_n,\{\pm1\})$ is well-known, with the action of S_n on $\{\pm1\}$ being necessarily the trivial one. Since the action is trivial, the signature homomorphism $S_n \to \{\pm1\}$ gives rise to an element $\epsilon_n \in H^1(S_n,\{\pm1\})$. For example, ϵ_3 looks like:

e	(23)	(12)	(123)	(321)	(13)
1	-1	-1	1	1	-1

Now consider the cup product $\epsilon_n \cup \epsilon_n$ induced by the $\mathbb{Z}$-bilinear map:

$B(\cdot,\cdot)$	1	-1
1	1	1
-1	1	-1

For ϵ_3 the resulting cup product looks like:

$B(a_g, g\cdot a_h)$	e	(23)	(12)	(123)	(321)	(13)
e	1	1	1	1	1	1
(23)	1	-1	-1	1	1	-1
(12)	1	-1	-1	1	1	-1
(123)	1	1	1	1	1	1
(321)	1	1	1	1	1	1
(13)	1	-1	-1	1	1	-1

If $n=2,3$, then $H^2(S_n,\{\pm1\}) \simeq \mathbb{Z}/2\mathbb{Z}$ and it is generated by $\epsilon_n \cup \epsilon_n$. If $n \geq 4$, then $H^2(S_n,\{\pm1\}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ and it is generated by $\epsilon_n \cup \epsilon_n$ and another class t_n. Here is part of it, which you can be completed as an exercise:

$(t_4)_{g,h}$	e	(12)	(23)	(34)	(123)	$(12)(34)$	$(13)(24)$	$(14)(23)$	...
e	1	1	1	1	1	1	1	1	
(12)	1	1	1	1	1				
(23)	1	1	1	1	1				
(34)	1	-1	1	1	1				
$(12)(34)$	1	-1	-1	1	1	-1	1	1	
$(13)(24)$	1					-1	-1	1	
$(14)(23)$	1					1	-1	-1	
...									

Notice the corresponding extension will have identities like:

$$e_{(12)(34)} = -e_{(34)(12)} \qquad \text{and} \qquad e_{(123)(23)} = -e_{(23)(123)}$$

More formally, the extension corresponding to t_n is denoted by $\tilde{S}_n$. Here is a presentation of this group:

$$\tilde{S}_n = < s_i, z \mid s_i^2 = 1,\ z^2 = 1,\ s_i z = z s_i,\ (s_i s_{i+1})^3 = 1,\ s_i s_j = z s_j s_i \text{ if } |j-i| \geq 2 >$$

Now $(\epsilon_n \cup \epsilon_n)(t_n)$ will correspond to another extension which we denote $2 \cdot S_n^-$. Here is its presentation (why?):

$$2 \cdot S_n^- =< s_i, z \mid s_i^2 = z,\ z^2 = 1,\ s_i z = z s_i,\ (s_i s_{i+1})^3 = z,\ s_i s_j = z s_j s_i \text{ if } |j-i| \geq 2 >$$

Now, if G is a subgroup of S_n, we can construct central extensions of G by $\{\pm 1\}$ using the restriction map

$$\text{Res: } H^2(S_n, \{\pm 1\}) \to H^2(G, \{\pm 1\})$$

In particular, we can define the extension $\tilde{G}$ corresponding to $\text{Res}(t_n)$. It is then easy to see that we have the following commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \pm 1 \arrow[r] \arrow[d] & \tilde{G} \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \pm 1 \arrow[r] & \tilde{S}_n \arrow[r] & S_n \arrow[r] & 1
\end{tikzcd}$$

For example, identify the group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with the subgroup V of S_4 where

$$V = \{(),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

Then $\tilde{G} = Q_8$. Can you see it in the table above?

Example 4.7. Let us try to calculate $\mathrm{H}^2(\mathbb{C}^\times, \mathbb{Z})$ by calculating the isomorphism classes of extensions of $\mathbb{C}^\times$ by $\mathbb{Z}$. Consider the short exact sequence of abelian groups:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2\pi i} \mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times \longrightarrow 0$$

so $\xi = (2\pi i, \mathbb{C}, \exp)$ is an extension of $\mathbb{C}^\times$ by $\mathbb{Z}$. Note that since all groups are abelian, the conjugation action of $\mathbb{C}^\times$ on $\mathbb{Z}$ induced by the choice of any right section of ξ is trivial. The principal-valued complex logarithm $\text{Log}\colon \mathbb{C}^\times \to \mathbb{C}$ is a right section of ξ, however it is not a right splitting section since Log is not a homomorphism. The right section Log induces a 2-cocyle α defined as follow: let $z, z' \in \mathbb{C}^\times$ and express them in polar coordinate form as $z = re^{i\theta}$ and $z' = r'e^{i\theta'}$ where $r, r' > 0$ and $\theta, \theta' \in (-\pi, \pi]$. For each $x \in \mathbb{R}$, we denote by $\widetilde{x}$ to be the unique $\widetilde{x} \in (-\pi, \pi]$ such that $\widetilde{x} + k = x$ for some $k \in \mathbb{Z}$. Then observe that

$$\begin{aligned}
\text{Log}\, z + \text{Log}\, z' - \text{Log}(zz') &= (\ln r + i\theta) + (\ln r' + i\theta') - \ln(rr') - i(\widetilde{\theta + \theta'}) \\
&= \ln(rr') + i\theta + i\theta' - \ln(rr') - i(\widetilde{\theta + \theta'}) \\
&= i(\theta + \theta' - \widetilde{\theta + \theta'}) \\
&= \left(\frac{\theta + \theta' - \widetilde{\theta + \theta'}}{2\pi} \right) 2\pi i
\end{aligned}$$

It follows that

$$\alpha(z, z') = \frac{\theta + \theta' - \widetilde{\theta + \theta'}}{2\pi}. \tag{22}$$

In particular, we have

$$\alpha(z, z') = \begin{cases} 1 & \text{if } \pi < \theta + \theta' \\ 0 & \text{if } -\pi < \theta + \theta' \leq \pi \\ -1 & \text{if } \theta + \theta' \leq -\pi \end{cases}$$

For instance, we have $\alpha(\zeta_3, 2i) = 1$ and $\alpha(\zeta_3^2, -2i) = -1$ (more generally we have $\alpha(z, z') = -\alpha(\overline{z}, \overline{z}')$). Since α is a 2-cocycle, it satisfies the 2-cocycle identity

$$\alpha(z_2, z_3) - \alpha(z_1 z_2, z_3) + \alpha(z_1, z_2 z_3) - \alpha(z_1, z_2) = 0. \tag{23}$$

Note that it is not immediately obvious why (23) should hold just by looking at the definition of α. Ultimately the 2-cocyle identity holds because the group law coming from the extension ξ is associative (that is, addition on $\mathbb{C}$ is associative). Observe also that α inherits many of the same properties that the complex Logarithm has. For instance, it is holomorphism at (z, z') for all $z, z' \in \mathbb{C} \backslash \{(-\infty, 0]\}$. Thus the principal-valued complex logarithm induces a nice 2-cocycle α which represents an element in $\mathrm{H}^2(\mathbb{C}^\times, \mathbb{Z})$. A different right section of ξ will have the form

$$z \mapsto 2\beta(z)\pi i + \text{Log}\, z,$$

where β is a function from $\mathbb{C}^\times$ to $\mathbb{Z}$. These are called **complex logarithms**. The corresponding 2-cocycle that $2\pi i\beta + \mathrm{Log}$ induces is given by

$$(\alpha+\delta\beta)(z,z') = \alpha(z,z') + \beta(zz') - \beta(z) - \beta(z'),$$

which again represents the same element in $\mathrm{H}^2(\mathbb{C}^\times, \mathbb{Z})$. Can we choose a β such that $\delta\beta + \alpha = 0$? The answer is no! Indeed, this is due to the fact that the extension ξ is not split: if it were, then we'd have an isomorphism $\mathbb{C} \cong \mathbb{Z}\times\mathbb{C}^\times$ of groups, which is definitely not true since $\mathbb{C}$ has elements of finite order but $\mathbb{Z}\times\mathbb{C}^\times$ does not. Now consider the cup product $\alpha\cup\alpha$ induced by the bilinear map $\mu\colon \mathbb{Z}\otimes\mathbb{Z}\to\mathbb{Z}$ given by $\mu(m,m') = mm'$. Thus we have

$$(\alpha\cup\alpha)(z_1,z_2,z_3,z_4) = \left(\frac{\theta_1+\theta_2-\widetilde{\theta_1+\theta_2}}{2\pi}\right)\left(\frac{\theta_3+\theta_4-\widetilde{\theta_3+\theta_4}}{2\pi}\right).$$

Clearly $\alpha\cup\alpha$ also takes values -1, 0, or 1.

Example 4.8. Let $y\in\mathbb{R}$ and consider the short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\iota_y} \mathbb{R} \xrightarrow{\varepsilon_y} S^1 \longrightarrow 0$$

where $\iota_y\colon \mathbb{Z}\to\mathbb{R}$ is defined by $\iota_y(m) = m/y$ and where $\varepsilon_y\colon \mathbb{R}\to S^1$ is defined by $\varepsilon_y(x) = e^{2\pi i x y}$. The map $\widetilde{\varepsilon}_y\colon S^1\to\mathbb{R}$ defined by

$$\widetilde{\varepsilon}_y(\zeta) = \frac{\mathrm{Log}(\zeta)}{2\pi i y} = \frac{\theta}{2\pi y},$$

where $\zeta = e^{i\theta}\in S^1$ with $\theta\in(-\pi,\pi]$, is a right section to $(\iota_y,\mathbb{R},\varepsilon_y)$. Let $\alpha_y\colon S^1\times S^1\to\mathbb{Z}$ be the corresponding 2-cocycle it induces. Note that

$$\begin{aligned}\widetilde{\varepsilon}_y(\zeta)+\widetilde{\varepsilon}_y(\zeta')-\widetilde{\varepsilon}_y(\zeta\zeta') &= \frac{\theta}{2\pi y}+\frac{\theta'}{2\pi y}-\frac{\widetilde{\theta+\theta'}}{2\pi y}\\ &= \left(\frac{\theta+\theta'-\widetilde{\theta+\theta'}}{2\pi}\right)\frac{1}{y}.\end{aligned}$$

Thus we have

$$\alpha(z,z') = \begin{cases} 1 & \text{if } \pi<\theta+\theta' \\ 0 & \text{if } -\pi<\theta+\theta'\leq\pi \\ -1 & \text{if } \theta+\theta'\leq -\pi.\end{cases}$$

Example 4.9. Consider the following matrices M, $M_0\in \mathrm{M}_2(\mathbb{Z})$ given by

$$M_0 = \begin{pmatrix} 0 & -5 \\ 1 & 0\end{pmatrix} \quad\text{and}\quad M = \begin{pmatrix} 0 & 5 \\ -1 & 0\end{pmatrix}$$

It's easy to see that M_0 is the matrix representation for $\sqrt{-5}$ on the $\mathbb{Z}$-basis $\{1,\sqrt{-5}\}$ and M is the matrix representation for $\sqrt{-5}$ on the $\mathbb{Z}$-basis $\{1,-\sqrt{-5}\}$. In particular, M and M_0 are $\mathrm{GL}_2(\mathbb{Z})$-conjugate. On the other hand, they are not $\mathrm{SL}_2(\mathbb{Z})$-conjugate nor are they are not even $\mathrm{SL}_2(\mathbb{Q})$-conjugate. However it turns out that they are $\mathrm{SL}_2(\mathbb{Q}(i))$-conjugate. To see this, first note that the change of basis matrix from $\{1,\sqrt{-5}\}$ to $\{1,-\sqrt{-5}\}$ is given by $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$. Of course, this matrix has determinant -1, so it is not in $\mathrm{SL}_2(\mathbb{Q}(i))$, but if we multiply this matrix by i, then we get a matrix which is in $\mathrm{SL}_2(\mathbb{Q}(i))$. So we have a problem which has no solution in $\mathbb{Q}$, but does have a solution in $\mathbb{Q}(i)$.

Let's describe how to construct something positive out of this non-solution using Galois cohomology. Let $G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ and define $\mathrm{Z}_{\mathrm{SL}_2}(M_0)(\mathbb{Q}(i))$ to be the set of all $Q\in\mathrm{SL}_2(\mathbb{Q}(i))$, such that Q commutes with M_0, and define $\mathrm{SL}_2(\mathbb{Q}(i))\star M_0$ to be the set of all matrices of the form QM_0Q^{-1}. Then observe that we have the following short exact sequence of pointed G-sets:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Z}_{\mathrm{SL}_2}(M_0)(\mathbb{Q}(i)) & \longrightarrow & \mathrm{SL}_2(\mathbb{Q}(i)) & \longrightarrow & \mathrm{SL}_2(\mathbb{Q}(i))\star M_0 & \longrightarrow & 0 \\ & & & & Q & \longmapsto & QM_0Q^{-1} & & \end{array}$$

Now apply the following Galois cohomology functor which maps a G-set X to the G-set $X^G = \{x\in X \mid gx = x\}$ to the short exact sequence above and we obtain a long exact sequence of the form

$$
\begin{tikzcd}
0 \arrow[r] & Z_{\mathrm{SL}_2}(M_0)(\mathbb{Q}) \arrow[r] & \mathrm{SL}_2(\mathbb{Q}) \arrow[r] & \mathrm{SL}_2(\mathbb{Q}) \star M_0 \arrow[dlll, rounded corners, to path={ -- ([xshift=2ex]\tikztostart.east) |- ([yshift=-3ex]\tikztostart.south) node[below]{δ} -| ([xshift=-2ex]\tikztotarget.west) -- (\tikztotarget)}] \\
& \mathrm{H}^1(G, Z_{\mathrm{SL}_2}(M_0)(\mathbb{Q})) \arrow[r] & \mathrm{H}^1(G, \mathrm{SL}_2(\mathbb{Q})) \arrow[r] & \cdots
\end{tikzcd}
$$

What happened here is that we have lost surjectivity after applying the functor: the matrix M is not in the image of anything from $\mathrm{SL}_2(\mathbb{Q})$. Galois cohomology measures the failure of this surjectivity, by constructing a map δ. The way the δ map works is it takes this matrix M and constructs a function from G to $Z_{\mathrm{SL}_2}(M_0)(\mathbb{Q})$ as follows: We go back to the short exact sequence before the functor was applied. Then we lift $M \in SL_2(\mathbb{Q}(i))\star$

Let k^{sep} be a separable closure of a field k, and denote G_k to mean $Gal(k^{sep}/k)$. Let $n \geq 1$ be an integer, and assume that the image of n in k is nonzero. Then associated to the exact sequence

$$
0 \longrightarrow \mu_n \longrightarrow (k^{sep})^* \xrightarrow{n} (k^{sep})^* \longrightarrow 0
$$

we have a long exact sequence

$$
\begin{tikzcd}
0 \arrow[r] & \mu_n \cap k \arrow[r] & k^* \arrow[r, "n"] & k^* \arrow[dll, rounded corners, to path={ -- ([xshift=2ex]\tikztostart.east) |- ([yshift=-3ex]\tikztostart.south) node[below]{δ} -| ([xshift=-2ex]\tikztotarget.west) -- (\tikztotarget)}] \\
& H^1(G_k, \mu_n) \arrow[r] & H^1(G_k, (k^{sep})^*) = 0 &
\end{tikzcd}
$$

4.10 Base Change

The canonical ring homomorphism $\mathbb{Z} \to \mathbb{Z}[G]$ is flat since $\mathbb{Z}[G]$ is a free $\mathbb{Z}$-module, so base change gives us a natural isomorphism

$$
\mathrm{Ext}_{\mathbb{Z}[G]}(A \otimes_{\mathbb{Z}} \mathbb{Z}[G], B) \simeq \mathrm{Ext}_{\mathbb{Z}}(A, B),
$$

where A is a $\mathbb{Z}$-module and where B is a $\mathbb{Z}[G]$-module. Now suppose that G is the cyclic group of order p and let $A = G$. Then we have

$$
\mathrm{Ext}_{\mathbb{Z}[G]}(G, B) \simeq \mathrm{Ext}_{\mathbb{Z}[G]}(G \otimes_{\mathbb{Z}} \mathbb{Z}[G], B) \simeq \mathrm{Ext}_{\mathbb{Z}}(\mathbb{F}_p[G], B),
$$

where we used the fact that $G \otimes_{\mathbb{Z}} \mathbb{Z}[G] \simeq \mathbb{F}_p[G]$. Next consider the case where $G = \mathbb{Z}$. Then we have

$$
\mathrm{H}(\mathbb{Z}, B) := \mathrm{Ext}_{\mathbb{Z}[x,x^{-1}]}(\mathbb{Z}, B)
$$

where we used the fact that $\mathbb{Z}[\mathbb{Z}] = \mathbb{Z}[x, x^{-1}]$ and so $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}[\mathbb{Z}] = \mathbb{Z}[x, x^{-1}]$. Next we want to figure out what $G^{\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ is where G is a non-abelian group.

4.11 Group Cohomology of a Cyclic Group

We now assume that G is the cyclic group of order p. We wish to understand the group cohomology of G in this case.

4.12 Profinite Group Cohomology

Let (Γ_i, φ_{ij}) be an inverse system of finite groups with surjective transition maps, and define $\Gamma = \varprojlim \Gamma_i$ equipped with its "inverse limit" topology (that is, the closed subspace topology inside the compact Hausdorff space $\prod_i \Gamma_i$ in which the finite factors Γ_i are discrete). Elements in $\prod_i \Gamma_i$ are expressed as $\gamma = (\gamma_i)_{i \in I}$ where $\gamma_i \in \Gamma_i$ for each $i \in I$. We refer to γ_i as the i**th component** of γ. The natural maps $\pi_i \colon \Gamma \to \Gamma_i$ are all surjective, and by definition of the topology we see that the kernel $U_i = \ker \pi_i$ is an open normal subgroup with these U_i a base of open neighborhoods of 1. Indeed, the basic opens in the product topology $\prod_i \Gamma_i$ are of them form

$$
U_{J,S_j} = \prod_{i \in I \setminus J} \Gamma_i \times \prod_{j \in J} S_j = \{\gamma \in \prod_i \Gamma_i \mid \gamma_j \in S_j \text{ for all } j \in J\}.
$$

where J is finite and where S_j is a subset of Γ_j for each $j \in J$. Indeed, they clearly cover the topology. Furthermore, note that

$$
U_{J,S_j} \cap U_{J',S'_{j'}} = \prod_{i \in I \setminus (J \cup J')} \Gamma_i \times \prod_{j'' \in J \setminus J'} S_{j''} \times \prod_{j'' \in J' \setminus J} S'_{j''} \times \prod_{j'' \in J \cap J'} S_{j''} \cap S'_{j''} = U_{J'',S''_{j''}}
$$

where $J'' = J \cup J'$ and where

$$S''_{j''} = \begin{cases} S_{j''} & \text{if } j'' \in J \setminus J' \\ S'_{j''} & \text{if } j'' \in J' \setminus J \\ S_{j''} \cap S'_{j''} & \text{if } j'' \in J \cap J' \end{cases}$$

Thus since Γ is the closed subspace topology of $\prod_i \Gamma_i$, we see that the basic opens in Γ are all of the form

$$U_{J,S_j} \cap \Gamma = \{\gamma \in \prod_i \Gamma_i \mid \gamma_j \in S_j \text{ for all } j \in J \text{ and } \varphi_{ik}(\gamma_k) = \gamma_i \text{ for all } k \geq i\} = \{\gamma \in \Gamma \mid \gamma_j \in S_j \text{ for all } j \in J\}.$$

In particular, $\ker \pi_i$ is open since $\ker \pi_i = U_{\{i\},\{1\}} \cap \Gamma$.

Such Γ are called **profinite**, the most important examples being $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n$ and especially Galois groups $\mathrm{Gal}(K/\mathbb{k})$ with the Krull topology, where $K/\mathbb{k}$ is an arbitrary Galois extension (perhaps of infinite degree). In this latter case, the finite groups Γ_i can be taken to be the Galois groups $\mathrm{Gal}(K_i/\mathbb{k})$ for the directed system $\{K_i\}$ of $\mathbb{k}$-finite Galois subextensions of $K/\mathbb{k}$ (with the Galois groups made into an inverse system via "restriction"). We are most interested in the case of absolute Galois groups $\Gamma = \mathrm{Gal}(\mathbb{k}_s/\mathbb{k})$ for a field $\mathbb{k}$, but it clarifies matters below to contemplate a general profinite Γ (equipped with a choice of inverse system presentation via some $\{\Gamma_i\}$).

Proposition 4.9. *Let G be a profinite group. Then G is compact.*

Proof. The idea is to show that G is a closed subspace of $\prod G_i$. Since $\prod G_i$ is compact by Tychonoff, it would then follow that G is compact since a closed subspace of a compact space is compact. To show G is closed, we just need to chow its complement G^c is open, so let $\gamma \in G^c$. Then there exists an i and j such that $\varphi_{ij}\gamma_j \neq \gamma_i$. Let

$$U = \{\gamma_i\} \times \{\gamma_j\} \times \prod_{k \neq i,j} G_k.$$

Clearly U is an open neighborhood of γ which is disjoint from G. It follows that G^c is open, hence G is closed. $\square$

Example 4.10. Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. For each positive prime p set $U_p = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{p}))$. Then the open set $U = \bigcup U_p$ is covered by $\{U_p\}$ and clearly has no finite subcovering by $\{U_p\}$. Thus U isn't compact, so in particular $G \neq U$. Indeed, the automorphism $\sigma\colon \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ given by $\sigma(\sqrt{p}) = -\sqrt{p}$ for all p is an element of G which is not in U.

Proposition 4.10. *Let G be a profinite group. The open subgroups of G are precisely the closed subgroups of finite index.*

Proof. Let U be an open subgroup of G. The complement of U is a union of disjoint open cosets. Since G is compact and is covered by the union of all cosets of U, we see that there can only be finitely many such cosets. Thus U has finite index in G. Clearly the completement of U is open, hence U is closed as well. Conversely, a closed subgroup of finite index is open, because it is the union of finitely many cosets, hence its complement is closed. $\square$

Definition 4.2. A **discrete Γ-module** is a Γ-module A such that each $a \in A$ has open stabilizer in Γ.

Proposition 4.11. *Let A be a Γ-module, let $\mu\colon \Gamma \times A \to A$ be the corresponding action map, and equip A with the discrete topology. Then A is a discrete Γ-module if and only if μ is continuous.*

Proof. First we suppose A is a discrete Γ-module. We will show μ is continuous. Since A is discrete, it suffices to show $\mu^{-1}\{a\}$ is open for $a \in A$. Observe that

$$\mu^{-1}\{a\} = \bigcup_{b \in A} \{(\gamma, b) \in \Gamma \times \{b\} \mid \gamma b = a\} = \bigcup_{b \in A} \Gamma_b,$$

where we set $\Gamma_b = \{(\gamma, b) \in \Gamma \times \{b\} \mid \gamma b = a\}$. If $\Gamma_b \neq \emptyset$, then choose $\gamma \in \Gamma_b$ (so $\gamma b = a$) and observe that $\Gamma_b = \gamma \mathrm{Stab}_\Gamma(a) \times \{b\}$. In particular, since $\mathrm{Stab}_\Gamma(a)$ is open, each Γ_b is open (if $\Gamma_b = \emptyset$ then it is obviously open), and hence $\mu^{-1}\{a\}$ is open. It follows that μ is continuous.

Conversely, suppose μ is continuous. To show $\mathrm{Stab}_\Gamma(a)$, it suffices to find an open neighborhood of $\gamma \in \mathrm{Stab}_\Gamma(a)$ which is contained in $\mathrm{Stab}_\Gamma(a)$. Since μ is continuous, it is continuous at (γ, a). This implies there exists $i \in I$ such that $\mu(\gamma \ker \pi_i \times \{a\}) = \{a\}$. However this itself implies $\gamma \ker \pi_i \subseteq \mathrm{Stab}_\Gamma(a)$. It follows that $\mathrm{Stab}_\Gamma(a)$ is open. $\square$

4.12.1 Discretization

Definition 4.3. Let A be an abstract Γ-module (so no discreteness condition). The **discretization** A^{disc} of A is the subset of elements $a \in A$ such that the stabilizer $\mathrm{Stab}_\Gamma(a)$ is open in Γ (equivalently, one of the open normal subgroups $\ker \pi_i$ acts trivially on a).

It is straightforward to check that A^{disc} is a Γ-submodule of A. Moreover, it is a discrete Γ-module by its very definition.

Lemma 4.6. *For any discrete Γ-module B, we have*

$$\mathrm{Hom}_\Gamma(B, A) = \mathrm{Hom}_\Gamma(B, A^{\mathrm{disc}}).$$

That is, every Γ-equivariant map $\varphi \colon B \to A$ lands inside A^{disc}.

Proof. Pick a φ, so for $b \in B$ we see to prove that $\varphi(b) \in A^{\mathrm{disc}}$. For $\gamma \in \Gamma$ we have $\gamma\varphi(b) = \varphi(\gamma b)$, and by discreteness of B we have $\gamma b = b$ for γ in an open subgroup $H \subseteq \Gamma$. Thus $\varphi(b) \in A^H \subseteq A^{\mathrm{disc}}$. □

The usefulness of discretization is that it provides enough injectives in $\mathrm{Mod}_{\mathrm{disc}}(\Gamma)$. Indeed, for a discrete Γ-module A we can forget the topology and just view A as a $\mathbb{Z}[\Gamma]$-module, so by general nonsense there is a Γ-linear injective $A \hookrightarrow E$ into an injective $\mathbb{Z}[\Gamma]$-module E. But A is discrete, so this injection factors through E^{disc}. To show that $\mathrm{Mod}_{\mathrm{disc}}(\Gamma)$ has enough injectives it is therefore enough to prove:

Proposition 4.12. *If E is an injective $\mathbb{Z}[\Gamma]$-module, then E^{disc} is injective in $\mathrm{Mod}_{\mathrm{disc}}(\Gamma)$. That is, the functor $\mathrm{Hom}_\Gamma(\cdot, E^{\mathrm{disc}})$ on the category $\mathrm{Mod}_{\mathrm{disc}}(\Gamma)$ is exact.*

Proof. By the preceding lemma, if A is a discrete Γ-module, then naturally in A we have

$$\mathrm{Hom}_\Gamma(A, E^{\mathrm{disc}}) = \mathrm{Hom}_\Gamma(A, E).$$

In other words, the functor of interest is the composition of the exact forgetful functor $\mathrm{Mod}_{\mathrm{disc}}(\Gamma) \to \mathrm{Mod}(\mathbb{Z}[\Gamma])$ and the functor $\mathrm{Hom}_{\mathbb{Z}[\Gamma]}(\cdot, E)$ on $\mathrm{Mod}(\mathbb{Z}[\Gamma])$ that is exact due to the assumed injectivity property of E. □

It now makes sense to apply the general theory of derived functors:

Definition 4.4. The δ-functor $\mathrm{H}(\Gamma, \cdot) \colon \mathrm{Mod}_{\mathrm{disc}}(\Gamma) \to \mathrm{Ab}$ is the right derived functor of $A \rightsquigarrow A^\Gamma$.

4.13 The Brauer Group

Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. We set $\mathrm{CSA}_{L/K}(n)$ to denote the set of K-isomorphism classes of central simple K-algebras of degree n which are split by L. We regard this as a pointed set with the class of $\mathrm{M}_n(K)$ being the base point.

Theorem 4.7. *There is a base point preserving bijection*

$$\mathrm{CSA}_{L/K}(n) \longleftrightarrow \mathrm{H}^1(G, \mathrm{PGL}_n(K)).$$

Proof. □

5 Symmetric Groups

5.1 Transpositions

Proposition 5.1. *S_n is generated by transpositions.*

Proof. We shall prove this in two steps.

Step 1: First we show that any element in S_n can be expressed as a product of disjoint cycles. Let $\sigma \in S_n$. We shall describe an algorithm which expresses σ as a product of disjoint cycles. In the first step of the algorithm, choose any $a_{1,1} \in [n]$. Let k_1 be the least nonnegative integer such that $\sigma^{k_1}(a_{1,1}) = a_{1,1}$. We denote $a_{1,i_1} = \sigma^{i_1 - 1}(a_{1,1})$ for each $1 \leq i_1 \leq k_1$. Observe that $1 \leq k_1 \leq n$ by the pigeonhole principle. Also observe that $a_{1,i_1} \neq a_{1,i_1'}$ whenever $i_1 \neq i_1'$. Indeed, if $a_{1,i_1} = a_{1,i_1'}$ for some $1 \leq i_1 < i_1' \leq k_1$, then

$$\begin{aligned}
\sigma^{i_1'-i_1}(a_{1,1}) &= \sigma^{i_1'}\sigma^{-i_1}(a_{1,1}) \\
&= \sigma^{-i_1}\sigma^{i_1'}(a_{1,1}) \\
&= \sigma^{-i_1}(a_{1,i_1'}) \\
&= \sigma^{-i_1}(a_{1,i_1}) \\
&= a_{1,1},
\end{aligned}$$

which would contradict the minimality of k_1 since $i_1' - i_1 < k_1$. So if we denote $\tau_1 = (a_{1,1} \cdots a_{1,k_1})$ and $\sigma_1 = \tau_1^{-1}\sigma$, then we can express σ as

$$\sigma = \tau_1\sigma_1.$$

where τ_1 is a cycle of length k_1 and where σ_1 fixes $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\}$. Indeed, we have

$$\begin{aligned}
\sigma_1(a_{1,i}) &= \tau_1^{-1}\sigma(a_{1,i_1}) \\
&= \tau_1^{-1}(a_{1,i_1+1}) \\
&= a_{1,i_1},
\end{aligned}$$

where a_{1,i_1+1} is understood to be $a_{1,1}$ if $i_1 = k_1$.

Now we proceed to the second step of the algorithm. If $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\} = [n]$, then the algorithm terminates and we are done. Indeed, in this case, σ_1 is the identity element since it fixes all of $[n]$. Then $\sigma = \tau_1$ shows that σ is a cycle itself. If $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\} \subset n$, where the inclusion is proper, then we choose any $a_{2,1} \in [n] \backslash \{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\}$. Let k_2 be the least nonnegative integer such that $\sigma^{k_2}(a_{2,1}) = a_{2,1}$. We denote $a_{2,i_2} = \sigma^{i_2-1}(a_{2,1})$ for each $1 \leq i_2 \leq k_2$. As in the case of the first step of the algorithm, we observe that $1 \leq k_2 \leq n - k_1$ and we also observe that $a_{2,i_2} \neq a_{2,i_2'}$ whenever $i_2 \neq i_2'$. The proof for these two observations is nearly identical to the ones we did above. We denote $\tau_2 = (a_{2,1} \cdots a_{2,k_2})$ and $\sigma_2 = \tau_2^{-1}\sigma_1$. Then we can express σ_1 as

$$\sigma_1 = \tau_2\sigma_2,$$

where τ_2 is a cycle of length k_2 and where σ_2 fixes $\{a_{1,i_1}, a_{1,i_2} \mid 1 \leq i_1 \leq k_1 \text{ and } 1 \leq i_2 \leq k_2\}$. Indeed, the proof that σ_2 fixes a_{1,i_2} is nearly identical to the proof that σ_1 fixes a_{1,i_1}, and the reason that σ_2 fixes a_{1,i_1} is because both τ_2 and σ_1 fix a_{1,i_1}.

Now we describe the algorithm at the sth step where $s \geq 2$. If $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\} = [n]$, then the algorithm terminates and we are done. Indeed, in this case, σ_{s-1} is the identity element since it fixes all of $[n]$. Then

$$\begin{aligned}
\sigma &= \tau_1\sigma_1 \\
&= \tau_1\tau_2\sigma_2 \\
&\vdots \\
&= \tau_1\tau_2\cdots\tau_{s-1}\sigma_{s-1} \\
&= \tau_1\tau_2\cdots\tau_{s-1}
\end{aligned}$$

shows that σ is a product of distinct cycles. If $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\} \subset [n]$, where the inclusion is proper, then we choose any $a_{s,1} \in [n] \backslash \{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\}$. Let k_s be the least nonnegative integer such that $\sigma^{k_s}(a_{s,1}) = a_{s,1}$. We denote $a_{s,i_s} = \sigma^{i_s-1}(a_{s,1})$ for each $1 \leq i_s \leq k_s$. As in the case of the first and second step of the algorithm, we observe that $1 \leq k_s \leq n - k_1 - \cdots - k_{s-1}$ and we also observe that that $a_{s,i_s} \neq a_{s,i_s'}$ whenever $i_s \neq i_s'$. We denote $\tau_s = (a_{s,1} \cdots a_{s,k_s})$ and $\sigma_s = \tau_s^{-1}\sigma_{s-1}$. Then we can express σ_{s-1} as

$$\sigma_{s-1} = \tau_s\sigma_s,$$

where τ_s is a cycle of length k_s and where σ_s fixes $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\}$.

This algorithm must terminate since $[n]$ is finite and since after the sth step, we produce a strictly increasing sequence of sets

$$(\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\})$$

each of which is contianed in $[n]$.

Step 2: Now we show that any cycle in S_n can be expressed as a product of transposition. Let $(a_1 a_2 \cdots a_k)$ be any in S_n. We claim that

$$(a_1 a_2 \cdots a_k) = \prod_{i=1}^{k-1} (a_i a_{i+1}). \tag{24}$$

Indeed, let $a \in [n]$. If $a \neq a_j$ for any $1 \leq j \leq k$, then applying a to both $(a_1 a_2 \cdots a_k)$ and $\prod_{i=1}^{k-1}(a_i a_{i+1})$ results in a again. In other words, both $(a_1 a_2 \cdots a_k)$ and $\prod_{i=1}^{k-1}(a_i a_{i+1})$ fix a. If $a = a_j$ for some $1 \leq j \leq k$, then applying a_j to $(a_1 a_2 \cdots a_k)$ results in a_{j+1}, where a_{j+1} is understood to be a_1 if $j = k$. Applying a_j to $\prod_{i=1}^{k-1}(a_i a_{i+1})$ also results in a_{j+1}, where a_{j+1} is understood to be a_1 if $j = k$. Indeed,

$$\begin{aligned}
\prod_{i=1}^{k-1}(a_i a_{i+1})(a_j) &= (a_1 a_2) \cdots (a_{j-1} a_j)(a_j a_{j+1}) \cdots (a_k a_{k-1})(a_j) \\
&= (a_1 a_2) \cdots (a_{j-1} a_j)(a_j a_{j+1})(a_j) \\
&= (a_1 a_2) \cdots (a_{j-1} a_j)(a_{j+1}) \\
&= a_{j+1}.
\end{aligned}$$

Combining step 1 with step 2 shows that any permutation can be expressed as a product of transpositions. □

5.1.1 Order of Permutation

In the proof that every permutation can be expressed as a product of transpositions, we also showed that every permutation can be expressed as a product of disjoint cycles.

Proposition 5.2. *Let $\sigma \in S_n$. Express σ as a product of disjoint cycles, say $\sigma = \tau_1 \cdots \tau_k$. Let m denote the order of σ and let m_i denote the order of τ_i for each $1 \leq i \leq k$. Then*

$$m = \operatorname{lcm}(m_1, \dots, m_k)$$

Proof. First we show that m is a common multiple of $m_1, \dots, m_k$. In other words, we first show that $m_i \mid m$ for each $1 \leq i \leq k$. Indeed, first note that $\tau_1, \dots, \tau_k$ all commute with each other since they are all disjoint from each other. Thus

$$\begin{aligned}
1 &= \sigma^m \\
&= (\tau_1 \cdots \tau_k)^m \\
&= \tau_1^m \cdots \tau_k^m.
\end{aligned}$$

Again since $\tau_1, \dots, \tau_k$ are all disjoint from each other, it follows that $\tau_i^m = 1$ for all $1 \leq i \leq k$: if $\tau_i^m(a) \neq a$ for some $a \in [n]$ and $1 \leq i \leq k$, then

$$\begin{aligned}
a &= 1(a) \\
&= \tau_1^m \cdots \tau_i^m \cdots \tau_k^m(a) \\
&= \tau_1^m \cdots \tau_i^m(a) \\
&= \tau_i^m(a)
\end{aligned}$$

would be a contradiction. It follows that $m_i \mid m$ for each $1 \leq i \leq k$. To see that m is the *least* common multiple, we just need to show that if $n \in \mathbb{N}$ such that $m_i \mid n$ for all $1 \leq i \leq k$, then $m \mid n$. Indeed, in this case, we have

$$\begin{aligned}
\sigma^n &= (\tau_1 \cdots \tau_k)^n \\
&= \tau_1^n \cdots \tau_k^n \\
&= 1^n \cdots 1^n \\
&= 1,
\end{aligned}$$

which implies $m \mid n$. □

Definition 5.1. A **transposition** is a 2-cycle $(a, b) \in S_n$

Lemma 5.1. *Every cycle from S_n can be written as a product of transpositions.*

Proof. $(a_1, a_2, \dots, a_k) = (a_1, a_2)(a_2, a_3) \cdots (a_{k-1}, a_k)$ □

Example 5.1. Write $(1,2,3) \in S_3$ as a product of transpositions: $(1,2,3) = (1,2)(2,3) = (1,3)(1,2)$

Proposition 5.3. *Every $\sigma \in S_n$ $(n \geq 2)$ can be written as a product of transpositions.*

Proof. Write σ as a product of disjoint cycles

$$\sigma = \tau_1 \cdots \tau_k$$

Now write τ_i as a product of transpositions for all $1 \leq i \leq k$. □

5.2 Conjugacy Classes in S_n

Lemma 5.2. *For any cycle $(i_1, \ldots, i_k)$ in S_n and any $\sigma \in S_n$,*

$$\sigma(i_1, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k)).$$

Proof. Let $\pi = \sigma(i_1, \ldots, i_k)\sigma^{-1}$. First we show π and takes $\sigma(i_j)$ to $\sigma(i_{j+1})$ for all $1 \leq j \leq k$.

$$\begin{aligned}
\pi(\sigma(i_j)) &= (\sigma(i_1, \ldots, i_k)\sigma^{-1})(\sigma(i_j)) \\
&= (\sigma(i_1, \ldots, i_k)\sigma^{-1}\sigma)(i_j) \\
&= (\sigma(i_1, \ldots, i_k))(i_j) \\
&= \sigma(i_{j+1})
\end{aligned}$$

Next we show π fixes everything else. So pick $x \in \{1, \ldots, n\} \setminus \{\sigma(i_1), \ldots, \sigma(i_k)\}$. Since $x \neq \sigma(i_j)$ for any $1 \leq j \leq k$, $\sigma^{-1}(x)$ is not i_j for any $1 \leq j \leq k$. Therefore, the cycle $(i_1, \ldots, i_k)$ does not move $\sigma^{-1}(x)$. So we have

$$\begin{aligned}
\pi(x) &= (\sigma(i_1, \ldots, i_k)\sigma^{-1})(x) \\
&= \sigma((i_1, \ldots, i_k))(\sigma^{-1}(x))) \\
&= \sigma(\sigma^{-1}(x)) \\
&= x
\end{aligned}$$

□

We show that all cycles of the same length in S_n are conjugate. Pick any two k-cycles, say $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_k)$. Choose $\sigma \in S_n$ such that $\sigma(a_i) = b_i$ for all $1 \leq i \leq k$. Then by Lemma (107.1), we see that conjugation by σ carries the first k-cycle to the second.

Definition 5.2. Let $\sigma \in S_m$. Write σ as a product of disjoint cycles $\sigma = \pi_1\pi_2 \cdots \pi_k$. The **cycle type** of σ is the sequence $(1^{e_1}, 2^{e_2}, \ldots, m^{e_m})$ where e_i is the number of i-cycles in the product factorization of σ.

Example 5.2. Let $\sigma = (1,3,5)(2,7)(9,8,13)(4,6,10,11,12)$. Then the cycle type of σ is $(2, 3^2, 5)$.

For $\sigma, \tau \in S_m$, denote $\sigma^\tau = \tau\sigma\tau^{-1}$. Now write σ as a product of disjoint cycles $\sigma = \pi_1\pi_2 \cdots \pi_k$. Then

$$\begin{aligned}
\sigma^\tau &= \tau\sigma\tau^{-1} \\
&= \tau\pi_1\pi_2 \cdots \pi_k\tau^{-1} \\
&= \tau\pi_1\tau^{-1}\tau\pi_2\tau^{-1} \cdots \tau\pi_k\tau^{-1} \\
&= \pi_1^\tau\pi_2^\tau \cdots \pi_k^\tau.
\end{aligned}$$

So σ^τ has the same cycle type as σ.

Proposition 5.4. *Let $\sigma, \tau \in S_m$. Then σ and τ are conjugate if and only if they have the same cycle type.*

5.3 The Alternating Group

Definition 5.3. A permutation $\sigma \in S_n$ is **even** if σ can be written as a product of an even number of transpositions. A permutation $\tau \in S_n$ is **odd** if τ is a product of an odd number of transpositions. We denote A_n to be the set of all even permutations.

Example 5.3. Any 3-cycle $(a,b,c) = (a,b)(b,c)$ is even. Any 4-cycle $(a,b,c,d) = (a,b)(b,c)(c,d)$ is odd.

Lemma 5.3. *The identity cannot be written as product of an odd number of transpositions.*

Proof. Write the identity as some product of transpositions:

$$(1) = (a_1, b_1)(a_2, b_2)\cdots(a_k, b_k), \tag{25}$$

where $k \geq 1$ and $a_i \neq b_i$ for all i. We will prove k is even.

The product on the right side of (25) can't have $k = 1$ since it is the identity. Suppose by induction that $k \geq 3$ and we know any product of fewer than k transpositions that equals the identity involves an even number of transpositions.

One of the $a_i's$ or $b_i's$ in the transpositions (a_i, b_i) for $i = 2, 3, \ldots, k$ has to be a_1, otherwise the permutation $(a_1, b_1)(a_2, b_2)\cdots(a_k, b_k)$ would map a_1 to b_1, and hence wouldn't be the identity permutation. Since $(a, b) = (b, a)$, we can one of the $a_i's$ in the transpositions (a_i, b_i) for $i = 2, 3, \ldots, k$ has to be a_1. Using different letters to denote different numbers, the formulas

$$(c, d)(a, b) = (a, b)(c, d), \quad (b, c)(a, b) = (a, c)(b, c)$$

show any product of two transpositions in which the second factor moves a and the first factor does not move a can be written as a product of two transpositions in which the first factor moves a and the second factor does not move a. Therefore, without changing the number of transpositions in (25), we can push the position of the second most left transposition in (25) that moves a_1 to the position right after (a_1, b_1), and thus we can assume $a_2 = a_1$.

If $b_2 = b_1$, then the product $(a_1, b_1)(a_2, b_2)$ in (25) is the identity and we can remove it. This reduces (25) to a product of $k - 2$ transpositions. By induction, $k - 2$ is even so k is even.

If instead $b_2 \neq b_1$, then the product $(a_1, b_1)(a_2, b_2)$ is equal to $(a_1, b_2)(b_1, b_2)$. Therefore (25) can be rewritten as

$$(1) = (a_1, b_2)(b_1, b_2)(a_3, b_3)\cdots(a_k, b_k), \tag{26}$$

where only the first two factors on the right have been changed. Now run through the argument again with (26) in place of (25). It involves the same number k of transpositions, but there are fewer transpositions in the product that move a_1 since we used to have (a_1, b_1) and (a_1, b_2) in the product and now we have (a_1, b_2) and (b_1, b_2).[1]

Some transposition other than (a_1, b_2) in the new product (26) must move a_1, so by the same argument as before either we will be able to reduce the number of transpositions by 2 and be done by induction or we will be able to rewrite the product to have the same total number of transpositions but drop by 1 the number of them that move a_1. This rewriting process eventually has to fall into the case where the first two transpositions cancel out, since we can't wind up with (1) as a product of transpositions where only the first one move a_1. Thus we will be able to see that k is even.

□

Proposition 5.5. *A permutation $\sigma \in S_n$ is either even or odd, but not both.*

Proof. Suppose we can write $\sigma = \tau_1 \cdots \tau_k$ and $\sigma = \tau_1' \cdots \tau_m'$ where k is even and m is odd. Then this implies (1) is odd.:$(1) = \tau_1 \cdots \tau_k \tau_1' \cdots \tau_m'$. □

Proposition 5.6. *$A_n \trianglelefteq S_n$ and $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.*

Proof. Let $\varepsilon : S_n \to \{\pm 1\}$ be the map which sends an even permutation to 1 and an odd permutation to -1. First we show this is a homomorphism. Suppose $\sigma, \tau \in S_n$. If both σ, τ are even, then $\sigma\tau$ is even. If σ is even and τ is odd, then $\sigma\tau$ is odd. If σ, τ are both odd, then $\sigma\tau$ is odd. In all cases, we can see that ε is indeed a homomorphism. Now we have $A_n = \mathrm{Ker}\varepsilon = \{\sigma \in S_n \mid \sigma \text{ is even}\}$. By the first isomorphism theorem, we have $S_n / A_n \cong \{\pm 1\}$. This implies $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$. □

Example 5.4. In S_3, we have $A_3 = \{(), (1, 2, 3), (3, 2, 1)\}$.

Simplicity of A_n

Lemma 5.4. *For $n \geq 3$, A_n is generated by 3-cycles. For $n \geq 5$, A_n is generated by permutations of type $(2, 2)$.*

Proof. The identity is $(1, 2, 3)^3$, a product of 3-cycles. Any even permutation σ has the form

$$\sigma = \prod_{k=1}^{m} (i_k, i_{k+1})(i_{k+2}, i_{k+3}),$$

[1]Since (a_1, b_1) and (a_1, b_2) were assumed all along to be honest transpositions, b_1 and b_2 do not equal a_1, so (b_1, b_2) doesn't move a_1.

where $i_k \in \{1, \ldots, n\}$ such that $i_k < i_{k+1}$ and $i_{k+2} < i_{k+3}$. r is even. If $i_{k+1} = i_{k+2}$, then $(i_k, i_{k+1})(i_{k+2}, i_{k+3}) = (i_k, i_{k+1}, i_{k+3})$, so

$$\sigma = \prod_{k=1}^{m} (i_k, i_{k+1}, i_{k+3}).$$

If $i_{k+1} \neq i_k$, then

$$\begin{aligned}(i_k, i_{k+1})(i_{k+2}, i_{k+3}) &= (i_k, i_{k+1})(i_{k+1}, i_{k+2})(i_{k+1}, i_{k+2})(i_{k+2}, i_{k+3}) \\ &= (i_k, i_{k+1}, i_{k+2})(i_{k+1}, i_{k+2}, i_{k+3}).\end{aligned}$$

So

$$\sigma = \prod_{k=1}^{m} (i_k, i_{k+1}, i_{k+2})(i_{k+1}, i_{k+2}, i_{k+3}).$$

In either case, we can write σ as a product of 3-cycles. To show permutations of type $(2, 2)$ generate A_n for $n \geq 5$, it suffices to write any 3-cycle (a, b, c) in terms of such permutations. Pick $d, e \notin \{a, b, c\}$. Then note

$$(a, b, c) = (a, b)(d, e)(d, e)(b, c).$$

□

The 3-cycles in S_n are all conjugate in S_n, since permutations of the same cycle type in S_n are conjugate. Are 3-cycles conjugate in A_n? Not when $n = 4$: (123) and (132) are not conjugate in A_4. But for $n \geq 5$ we do have conjugacy in A_n.

Lemma 5.5. *For $n \geq 5$, any two 3-cycles in A_n are conjugate in A_n.*

Proof. We show every 3-cycle in A_n is conjugate within A_n to $(1, 2, 3)$. Let σ be a 3-cycle in A_n. It can be conjugated to $(1, 2, 3)$ in S_n:

$$(1, 2, 3) = \pi\sigma\pi^{-1}$$

for some $\pi \in S_n$. If $\pi \in A_n$, we're done. Otherwise, let $\pi' = (45)\pi$, so $\pi' \in A_n$ and

$$\pi'\sigma\pi'^{-1} = (1, 2, 3)$$

□

The basic argument to show that the groups A_n is simple for $n \geq 5$ is to show any non-trivial normal subgroup $N \trianglelefteq A_n$ contains a 3-cycle, so N contains every 3-cycle by Lemma (5.5), and therefore N is A_n by Lemma (5.4).

Theorem 5.6. *A_5 is simple.*

Proof. Suppose N is a normal subgroup of A_5. Pick $\sigma \in N$ with $\sigma \neq (1)$. The cycle structure of σ is (a, b, c), $(a, b)(c, d)$, or (a, b, c, d, e), where different letters represent different numbers. Since we want to show N contains a 3-cycle, we may suppose σ has the second or third cycle type. In the second case, N contains

$$((a, b, e)(a, b)(c, d)(a, b, e)^{-1})(a, b)(c, d) = (b, e)(c, d)(a, b)(c, d) = (a, e, b).$$

In the third case, N contains

$$((a, b, c)(a, b, c, d, e)(a, b, c)^{-1})(a, b, c, d, e)^{-1} = (b, c, a, d, e)(e, d, c, b, a) = (a, b, d).$$

Therefore N contains a 3-cycle, so $N = A_5$.

□

6 Finite Matrix Groups

Let q be a power of a prime and let $\mathbb{F}_q$ denote the finite field with q elements.

6.1 The Group $\mathrm{GL}_n(\mathbb{F}_q)$

We define $\mathrm{GL}_n(\mathbb{F}_q)$ to be the group of all invertible matrices with entries in $\mathbb{F}_q$.

Proposition 6.1. *The size of* $\mathrm{GL}_n(\mathbb{F}_q)$ *is given by*

$$\#\mathrm{GL}_n(\mathbb{F}_q) = \prod_{i=0}^{n-1}(q^n - q^i).$$

Proof. Let A be a random matrix in $\mathrm{GL}_n(\mathbb{F}_q)$ and let $v_1, \ldots, v_n$ denote the column vectors of A. Note that counting the number of matrices A in $\mathrm{GL}_n(\mathbb{F}_q)$ is equivalent to counting the number of ordered tuples of linearly independent vectors $(v_1, \ldots, v_n)$, so it suffices to count the latter.

There are $q^n - 1$ different possible vectors in $\mathbb{F}_q^n$ for which v_1 can be. The only vector which is not allowed is the zero vector. This is because the vectors $(v_1, \ldots, v_n)$ must be linearly independent, so no zero vectors are allowed. Now we fix v_1. Then there are $q^n - q$ different possible vectors in $\mathbb{F}_q^n$ for which v_2 can be. Indeed, v_1 and v_2 must be linearly independent, so v_2 cannot equal to any vectors of the form av_1 where $a \in \mathbb{F}_q$. If we had fixed v_1 to be a different vector, then the same counting argument would apply, so altogether, the number of pairs of linearly independent vectors (v_1, v_2) is $(q^n - 1)(q^n - q)$.

More generally, for $1 \leq i \leq n$, if the vectors $v_1, \ldots, v_{i-1}$ are fixed, then there are $q^n - q^{j-1}$ different possible vectors in $\mathbb{F}_q^n$ for which v_j can be. Again, varying the vectors $v_1, \ldots, v_{i-1}$ to a new set of fixed vectors results in the same counting argument, so altogether the number of i-tuples of linearly independent vectors $(v_1, v_2, \ldots, v_i)$ is $(q^n - 1)(q^n - q) \cdots (q^n - q^{i-1})$. In particular, taking $i = n$ gives us

$$\#\mathrm{GL}_n(\mathbb{F}_q) = \prod_{i=1}^{n}(q^n - q^{i-1}) = \prod_{i=0}^{n-1}(q^n - q^i).$$

□

We now consider the case where $n = 2$. Set $G = \mathrm{GL}_2(\mathbb{F}_q)$, $U = \left\{ \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in G \right\}$, and $B = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G \right\}$.

Proposition 6.2. *We have the following assertions:*

1. *U is a p-Sylow subgroup of G.*
2. *$B = \mathrm{N}_G(U)$ where $\mathrm{N}_G(U)$ denotes the normalizer of U in G. In particular, the number of p-Sylow subgroups of G is given by $n_p = q + 1$.*

Proof. 1. First note that $\#G = (q^2 - q)(q^2 - 1) = q(q-1)^2(q+1)$. In particular, the largest power of p which divides $\#G$ is q. Thus every p-Sylow subgroup of G has size q. The set U certainly has size q since every element in U has the form $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ for some $x \in \mathbb{F}_q$. To see that it is a p-Sylow subgroup then, we just need to show that it is a subgroup. It is clearly nonempty. Also, if $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)$ are two matrices in U, then

$$\begin{aligned}
\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & x - y \\ 0 & 1 \end{pmatrix} \\
&\in U.
\end{aligned}$$

It follows that U is a subgroup, and hence a p-Sylow subgroup of G. In fact, it is a cyclic group, generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Another p-Sylow subgroup of G is obtained by simply taking the transpose of all matrices in U. Namely we set $U^\top = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) \in G \right\}$. Again, $U^\top$ has a size q and is a subgroup of G, so it is a p-Sylow subgroup of G. It is different from U becuase, $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in U^\top$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \notin U$.

2. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ and $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in U$. Then we have I

$$\begin{aligned}
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} &= \frac{1}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\
&= \frac{1}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d - cx & -b + ax \\ -c & a \end{pmatrix} \\
&= \frac{1}{\Delta} \begin{pmatrix} \Delta - acx & a^2x \\ c^2x & \Delta + acx \end{pmatrix}
\end{aligned}$$

where $\Delta = ad - bc$. Thus $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ conjugates $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ to another element of U if and only if $c = 0$, that is, if and only if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in B$. It follows that $\mathrm{N}_G(U) = B$. The number of matrices in B is given by $\#B = (q-1)^2 q$ since for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in B$, there are $q-1$ different choices for a and d and there are q different choices b. It follows from the Sylow Theorems that

$$\begin{aligned} n_p &= [G : \mathrm{N}_G(U)] \\ &= [G : B] \\ &= \frac{q(q-1)^2(q+1)}{q(q-1)^2} \\ &= q+1. \end{aligned}$$

□

7 Finite Groups of Order ≤ 100

7.1 Groups of Order p^2

For each prime p, we will show that every group of order p^2 is abelian. In particular, it will then follow from the fundamental theorem of finite abelian groups that every group of order p^2 is isomorphic to one of the two possibilities, namely C_{p^2} or $C_p \times C_p$. First we begin with an important lemma.

Lemma 7.1. *Any p-group has nontrivial center.*

Proof. Suppose G is a p-group, say $|G| = p^n$, and assume for a contradiction that $|\mathrm{Z}(G)| = 1$. Let $x_1, \dots, x_k$ represent the nontrivial conjugacy classes of G: so $|\mathrm{K}_{x_i}| > 1$ and $\mathrm{K}_{x_i} \cap \mathrm{K}_{x_j}$ for each $1 \leq i < j \leq k$ and

$$G = \mathrm{Z}(G) \cup \mathrm{K}_{x_1} \cup \cdots \cup \mathrm{K}_{x_k}.$$

Then the class equation gives us

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} [G : \mathrm{Z}(x_i)]. \tag{27}$$

Note that $p \mid [G : \mathrm{Z}(x_i)]$ for each $1 \leq i \leq k$. Indeed, $\mathrm{Z}(x_i)$ is a proper subgroup (otherwise x_i would not represent a nontrivial conjugacy class). Its order must divide the order of G by Lagrange's Theorem, thus $|\mathrm{Z}(x_i)| = p^{m_i}$ for some $m_i < n$. It follows that $[G : \mathrm{Z}(x_i)] = p^{n-m_i}$. With this understood, we now reduce (27) modulo p to get

$$0 \equiv 1 \bmod p,$$

which is a contradiction. □

Proposition 7.1. *Every group of order p^2 is abelian.*

Proof. Assume for a contradiction that $G \neq \mathrm{Z}(G)$. Since G is a p-group, $\mathrm{Z}(G)$ must be a nontrivial subgroup of G by Lemma (98.1). In particular, we must have $|\mathrm{Z}(G)| = p$. But then $|G/\mathrm{Z}(G)| = p$, which implies $G/\mathrm{Z}(G)$ is cyclic. It follows that G is abelian, which implies $G = \mathrm{Z}(G)$, a contradiction. So our assumption that $G \neq \mathrm{Z}(G)$ leads to a contradiction, which means we must in fact have $G = \mathrm{Z}(G)$. □

7.2 Groups of Order p^3

Let p be a prime. In this subsection, we classify all groups of order p^3. From the cyclic decomposition of finite abelian groups, there are three abelian groups of order p^3 up to isomorphism, namely C_{p^3}, $C_p \times C_{p^2}$, and C_p^3. These are nonisomorphic since they have different maximal orders for their elements: p^3, p^2, and p. We will show that there are two nonabelian groups of order p^3 up to isomorphism. The descriptions of these two groups will be different for $p = 2$ and $p \neq 2$, so we will treat these cases separately. First we need a lemma.

Lemma 7.2. *Let G be a nonabelian group of order p^3. Then*

1. $|\mathrm{Z}(G)| = p$;
2. $G/\mathrm{Z}(G) \cong C_p \times C_p$ *and;*
3. $[G, G] = \mathrm{Z}(G)$

Proof. 1. Since G is a p-group, $Z(G)$ must be a nontrivial subgroup of G by Lemma (98.1). Also since G is nonabelian, $Z(G)$ must be a proper subgroup of G. It follows that $|Z(G)| = p$ or $|Z(G)| = p^2$. Assume for a contradiction that $|Z(G)| = p^2$. Then $|G/Z(G)| = p$, which implies $G/Z(G)$ is cyclic, which is implies G is abelian, a contradiction. Thus $|Z(G)| = p$.

2. Since $|Z(G)| = p$, we have $|G/Z(G)| = p^2$. From the classification of groups of order p^2, we see that either $G/Z(G) \cong C_{p^2}$ or $G/Z(G) \cong C_p \times C_p$. If $G/Z(G) \cong C_{p^2}$, then $G/Z(G)$ is cyclic, which implies G is abelian, a contradiction. Thus $G/Z(G) \cong C_p \times C_p$.

3. Since $G/Z(G)$ is abelian, we see that $Z(G) \supseteq [G,G]$. Thus $|[G,G]| \mid p$, which means either $|[G,G]| = 1$ or $|[G,G]| = p$. We cannot have $|[G,G]| = 1$ since G is nonabelian, and so $|[G,G]| = p$. Thus we have $Z(G) \supseteq [G,G]$ and $|Z(G)| = |[G,G]|$ which implies This implies $Z(G) = [G,G]$. □

7.2.1 Case $p = 2$

Theorem 7.3. *A nonabelian group of order* 8 *is isomorphic to* D_4 *or* Q_8.

Proof. Let G be a nonabelian group of order 8. The nonidentity elements in G have order 2 or 4. If $g^2 = 1$ for all $g \in G$, then G is abelian, so some $x \in G$ must have order 4. Let $y \in G \backslash \langle x \rangle$. The subgroup $\langle x, y \rangle$ properly contains $\langle x \rangle$, so $\langle x, y \rangle = G$. Since G is nonabelian, x and y do not commute.

Since $\langle x \rangle$ has index 2 in G, it is a normal subgroup. Therefore $yxy^{-1} \in \langle x \rangle$, that is

$$yxy^{-1} \in \{1, x, x^2, x^3\}.$$

Since yxy^{-1} has order 4, we must have $yxy^{-1} = x$ or $yxy^{-1} = x^3 = x^{-1}$. Since x and y do not commute, we cannot have $yxy^{-1} = x$. Thus

$$yxy^{-1} = x^{-1}.$$

The group $G/\langle x \rangle$ has order 2. Therefore $y^2 \in \langle x \rangle$, that is

$$y^2 \in \{1, x, x^2, x^3\}.$$

Since y has order 2 or 4, we see that y^2 has order 1 or 2. Thus either $y^2 = 1$ or $y^2 = x^2$. Combining everything together, we see that either

$$G = \langle x, y \mid x^4 = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle$$

in which case $G \cong D_4$, or

$$G = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$$

in which case $G \cong Q_8$. □

7.2.2 Case $p \neq 2$

Now assume $p \neq 2$. The two nonabelian groups of order p^3, up to isomorphism, will turn out to be

$$\mathrm{Heis}(\mathbb{Z}/\langle p \rangle) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/\langle p \rangle \right\} \quad \text{and} \quad G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/\langle p^2 \rangle,\, a \equiv 1 \bmod p \right\}.$$

These two constructions make sense if $p = 2$, but they turn out to be isomorphic to each other in that case. If $p \neq 2$, we can distinguish $\mathrm{Heis}(\mathbb{Z}/\langle p \rangle)$ from G_p by counting elements of order p. In $\mathrm{Heis}(\mathbb{Z}/\langle p \rangle)$, we have

$$\begin{aligned} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^p &= \begin{pmatrix} 1 & na & nb + \frac{p(p-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & \frac{p(p-1)}{2}ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

where the last equality follows since $p \neq 2$. Thus every nonidentity element in $\mathrm{Heis}(\mathbb{Z}/\langle p \rangle)$ has order p. On the other hand, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in G_p$ has order p^2 since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ for all $n \in \mathbb{Z}$. So $G_p \neq \mathrm{Heis}(\mathbb{Z}/\langle p \rangle)$. At the prime

$p = 2$, $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ and G_2 each contain more than one element of order 2, so both $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ and G_2 are isomorphic to D_4.

Let's perform some calculations. First we see what matrix multiplication in $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ looks like. We have

$$\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & a' & b'\\ 0 & 1 & c'\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & a+a' & b+b'+ac'\\ 0 & 1 & c+c'\\ 0 & 0 & 1\end{pmatrix}$$

We can decompose any matrix in $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ as

$$\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}^c \begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}^a \begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}^b$$

and a particular commutator is

$$\left[\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}\right] = \begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Thus we have

$$\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix} = e_{23}^c e_{12}^a [e_{12}, e_{23}]^b$$

where e_{ij} denotes the matrix with 1 along the diagonal and at the (i,j)th spot and zero everywhere else where $1 \le i < j \le 3$.

Matrix multiplication in G_p looks like

$$\begin{pmatrix}1+pm & b\\ 0 & 1\end{pmatrix}\begin{pmatrix}1+pm' & b'\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1+p(m+m') & b+b'+pmb'\\ 0 & 1\end{pmatrix}.$$

We can decompose any matrix in G_p as

$$\begin{pmatrix}1+pm & b\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^b \begin{pmatrix}1+p & 0\\ 0 & 1\end{pmatrix}^m$$

and a particular commutator is

$$\left[\begin{pmatrix}1+p & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right] = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^p.$$

Thus we have

$$\begin{pmatrix}1+pm & b\\ 0 & 1\end{pmatrix} = e_{12}^p x^m$$

where $x = \left(\begin{smallmatrix}1+p & 0\\ 0 & 1\end{smallmatrix}\right)$.

Lemma 7.4. *Let G be a group and let $g, h \in G$. Suppose g and h commute with $[g,h]$. Then for all m and n in $\mathbb{Z}$, we have*

1. $[g^m, h^n] = [g,h]^{mn}$ *and;*
2. $g^n h^n = (gh)^n [g,h]^{\binom{n}{2}}$.

Proof. 1. We just need to show that for all $k \in \mathbb{N}$, we have

$$[g,h]^k = [g^k, h] = [g, h^k]. \tag{28}$$

We shall prove this by induction on k. The base case $k = 1$ is trivial, so assume that we have shown (28) for all $k < n$ for some $n \in \mathbb{Z}_{>1}$. Then we have

$$\begin{aligned}
[g,h]^n &= (ghg^{-1}h^{-1})^n \\
&= (ghg^{-1}h^{-1})(ghg^{-1}h^{-1})[g,h]^{n-2} \\
&= (g^2hg^{-1}h^{-1})(hg^{-1}h^{-1})[g,h]^{n-2} \\
&= (g^2hg^{-2}h^{-1})[g,h]^{n-2} \\
&= (g^2hg^{-2}h^{-1})[g^{n-2},h] \\
&= (g^2hg^{-2}h^{-1})(g^{n-2}hg^{-(n-2)}h^{-1}) \\
&= (g^nhg^{-2}h^{-1})(hg^{-(n-2)}h^{-1}) \\
&= g^nhg^{-n}h^{-1} \\
&= [g^n,h],
\end{aligned}$$

where we used the fact that g^{n-2} commutes with $[g,h]$ (which follows since g commutes with $[g,h]$). A similar computation also shows $[g,h]^n = [g,h^n]$.

2. We prove

$$g^k h^k = (gh)^k [g,h]^{\binom{k}{2}} \tag{29}$$

by induction on $k \in \mathbb{Z}_{\geq 2}$. Let us first work out the base case $k = 2$. We have

$$\begin{aligned} g^2h^2 &= gghh \\ &= ggh(g^{-1}h^{-1}hg)h \\ &= g[g,h]hgh \\ &= (gh)^2[g,h]. \end{aligned}$$

Now assume that we have shown (**??**) for all $k < n$ for some $n \in \mathbb{Z}_{>2}$. We have

$$\begin{aligned} (gh)^n[g,h]^{\binom{n}{2}} &= (gh)^n[g,h]^{\binom{n-1}{2}}[g,h]^{n-1} \\ &= gh(gh)^{n-1}[g,h]^{\binom{n-1}{2}}[g,h]^{n-1} \\ &= gh(g^{n-1}h^{n-1})[g,h]^{n-1} \\ &= gh[g,h]^{n-1}g^{n-1}h^{n-1} \\ &= [g,h]hg[g,h]^{n-1}g^{n-1}h^{n-1} \\ &= [g,h]^n hg^nh^{n-1} \\ &= [g^n,h]hg^nh^{n-1} \\ &= g^nhg^{-n}h^{-1}hg^nh^{n-1} \\ &= g^nhg^{-n}g^nh^{n-1} \\ &= g^nhh^{n-1} \\ &= g^nh^n. \end{aligned}$$

□

Theorem 7.5. *For primes $p \neq 2$, a nonabelian group of order p^3 is isomorphic to* $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ *or G_p.*

Proof. Let G be a nonabelian group of order p^3. Each $g \neq 1$ in G has order p or p^2. By Lemma (7.2), we can write $G/\mathrm{Z}(G) = \langle \overline{x}, \overline{y}\rangle$ and $\mathrm{Z}(G) = \langle z\rangle$. For $g \in G$, we have $g \equiv x^iy^j \bmod \mathrm{Z}(G)$ for some integers i and j, so

$$\begin{aligned} g &= x^iy^jz^k \\ &= z^kx^iy^j \end{aligned}$$

for some $k \in \mathbb{Z}$. If x and y commute, then G is abelian, which is a contradiction. Thus x and y do not commute. Therefore $[x,y] = xyx^{-1}y^{-1} \in \mathrm{Z}(G)$ is nontrivial, so $\mathrm{Z}(G) = \langle [x,y]\rangle$. Therefore we can use $[x,y]$ for z, showing $G = \langle x, y\rangle$.

Let's see what the product of two elements of G looks like. Using Lemma (7.4), we have

$$x^iy^j = y^jx^i[x,y]^{ij} \quad \text{and} \quad y^jx^i = x^iy^j[x,y]^{-ij}.$$

This shows we can move every power of y past every power of x on either side, at the cost of introducing a (commuting) power of $[x,y]$. So every element of $G = \langle x,y\rangle$ has the form $y^jx^i[x,y]^k$. A product of two such terms is

$$\begin{aligned} y^cx^a[x,y]^b \cdot y^{c'}x^{a'}[x,y]^{b'} &= y^c(x^ay^{c'})x^{a'}[x,y]^{b+b'} \\ &= y^c(y^{c'}x^a[x,y]^{ac'})x^{a'}[x,y]^{b+b'} \\ &= y^{c+c'}x^{a+a'}[x,y]^{b+b'+ac'}. \end{aligned}$$

Here the exponents are all integers. It appears that we have a homomorphism $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle) \to G$ by

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto y^cx^a[x,y]^b. \tag{30}$$

After all, we just showed multiplication of such triples $y^c x^a [x,y]^b$ behaves like multiplication in $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$. But there is a catch: the matrix entries a, b, and c in $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ are integers modulo p, so the "function" (30) from $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ to G is only well-defined if x, y, and $[x,y]$ all have pth power 1 (so exponents on them only matter modulo p). Since $[x,y]$ is in the center of G, a subgroup of order p, its exponents only matter modulo p. But maybe x or y could have order p^2.

Well if x and y have both order p, then there is no problem with (30). It is a well-defined function from $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ to G that is a homomorphism. Since its image contains x and y, the image contains $\langle x,y\rangle = G$, so the function is onto. Both $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ and G have order p^3, so our surjective homomorphism is an isomorphism: $G \cong \mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$.

What happens if x or y has order p^2? In this case we anticipate that $G \cong G_p$. In G_p two generators are $g = \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, where g has order p, h has order p^2, and $[g,h] = h^p$. We want to show our abstract G also has a pair of generators like this.

Starting with $G = \langle x,y\rangle$ where x or y has order p^2, without loss of generality let y have order p^2. It may or may not be the case that x has order p. To show we can change generators to make x have order p, we will look at the pth power function on G. For all $g \in G$, we have $g^p \in \mathrm{Z}(G)$ since $G/\mathrm{Z}(G) \cong C_p^2$. Moreover, the pth power function on G is a homomorphism: by Lemma (7.4), we have $(gh)^p = g^p h^p [g,h]^{p(p-1)/2}$ and $[g,h]^p = 1$ since $[G,G] = \mathrm{Z}(G)$ has order p, so

$$(gh)^p = g^p h^p.$$

Since y^p has order p and $y^p \in \mathrm{Z}(G)$, we have $\mathrm{Z}(G) = \langle y^p\rangle$. Therefore $x^p = (y^p)^r$ for some $r \in \mathbb{Z}$ and since the pth power function on G is a homomorphism we get $(xy^{-r})^p = 1$ with $xy^{-r} \neq 1$ since $x \notin \langle y\rangle$. So xy^{-r} has order p and $G = \langle x,y\rangle = \langle xy^{-r}, y\rangle$. We now rename xy^{-r} as x, so $G = \langle x,y\rangle$ where x has order p and y has order p^2.

We are not guaranteed that $[x,y] = y^p$, which is one of the relations for the two generators of G_p. How can we force this relation to occur? Well, since $[x,y]$ is a nontrivial element of $[G,G] = \mathrm{Z}(G)$, we have $\mathrm{Z}(G) = \langle [x,y]\rangle = \langle y^p\rangle$, so

$$[x,y] = (y^p)^k \tag{31}$$

where $k \not\equiv 0 \bmod p$. Let ℓ be a multiplicative inverse for $k \bmod p$ and raise both sides of (31) to the ℓth power: using Lemma (7.4), $[x,y]^\ell = (y^{pk})^\ell$ implies $[x^\ell, y] = y^p$. Since $\ell \not\equiv 0 \bmod p$, we have $\langle x\rangle = \langle x^\ell\rangle$, so we can rename x^ℓ as x: now $G = \langle x,y\rangle$ where x has order p, y has order p^2, and $[x,y] = y^p$.

Because $[x,y]$ commutes with x and y and $G = \langle x,y\rangle$, every element of G has the form

$$y^j x^i [x,y]^k = [x,y]^k y^j x^i = y^{pk+j} x^i.$$

Let's see how such products multiply:

$$\begin{aligned} y^b x^m \cdot y^{b'} x^{m'} &= y^b (x^m y^{b'}) x^{m'} \\ &= y^b (y^{b'} x^m [x,y]^{mb'}) x^{m'} \\ &= y^{b+b'} x^m (y^p)^{mb'} x^{m'} \\ &= y^{b+b'+pmb'} x^{m+m'}. \end{aligned}$$

So we get a homomorphism $G_p \to G$ by

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} \mapsto y^b x^m.$$

This function is well-defined since on the left side m matters modulo p and b matters modulo p^2 which $x^p = 1$ and $y^{p^2} = 1$. This homomorphism is onto since x and y are in the image, so it is an isomorphism since G_p and G have equal order: $G \cong G_p$. □

7.3 Finite Groups of Order 24

Theorem 7.6. *If $|G| = 24$, then G has a normal subgroup of size 4 or 8.*

Proof. Let P be a 2-Sylow subgroup, so $|P| = 8$. Consider the left multiplication map $\ell\colon G \to \mathrm{Sym}(G/P) \cong S_3$, given by $g \mapsto \ell_g$, where

$$\ell_g(\overline{x}) = \overline{gx}$$

for all $\overline{x} \in G/P$. Set K to be the kernel of ℓ. Then $K \subseteq P$, which implies $|K| \mid 8$. Also G/K embeds into S_3, which implies $[G:K] \mid 6$, that is, $4 \mid K$. Thus we have either $|K| = 4$ or $|K| = 8$. Since K is the kernel of ℓ, we see that K is a normal subgroup. □

Example 7.1. Consider the group $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. The order of this group is

$$\#\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) = (3^2-1)(3^2-3) = 48.$$

It has as a normal subgroup $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. Indeed, $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is the kernel of the determinant map

$$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \to (\mathbb{Z}/3\mathbb{Z})^\times.$$

Also, since $\#(\mathbb{Z}/3\mathbb{Z})^\times = 2$, we have

$$\#\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) = 48/2 = 24.$$

It follows from Theorem (7.6) that $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ contains a normal subgroup of size 4 or 8.

Part II
Ring Theory

8 Basic Definitions

8.1 Definition of a Ring

Definition 8.1. A **ring** is a triple $(R, +, \cdot)$ consisting of a set R together with two operations $+$ (addition) and $\cdot$ (multiplication) such that

1. The pair $(R, +)$ forms an abelian group. This means
   (a) Addition is associative: $(a+b)+c = a+(b+c)$ for all $a, b, c \in R$.
   (b) Addition is commutative: $a+b = b+a$ for all $a, b \in R$.
   (c) The identity element exists and is denoted by 0; there is an element 0 in R such that $a+0 = a = 0+a$ for all $a \in R$.
   (d) Inverses exist: For each a in R, there exists an element $-a$ in R such that $a+(-a) = 0$.
2. The pair $(R, \cdot)$ forms a monoid. This means
   (a) Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
   (b) The identity element exists and is denoted by 1; there is an element 1 in R such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$.
3. Multiplication is distributive with respect to addition. This means
   (a) $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.
   (b) $(b+c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.

We say R is a **commutative ring** if multiplication R is commutative: for all $a, b \in R$, we have $ab = ba$.

To clean notation, we abbreviate $(R, +, \cdot)$ to R and $a \cdot b$ to ab. We also denote the identity with respect to addition as 0 and we denote the identity with respect to multiplication as 1. The **zero ring** is the ring whose underlying set is a singleton $\{0\}$. Addition and multiplication are defined by the only way possible: $0+0 = 0$ and $0 \cdot 0 = 0$. This ring is rather trivial and thus we are not really too interested in it. Thus we will always assume that our rings are nonzero (unless otherwise specified of course). A much more interesting ring however is the ring of integers. Indeed, the set of integers equipped with the usual addition and multiplication operations is easily seen to be a ring. We denote this ring by $\mathbb{Z}$.

8.2 Ring Homomorphisms

Now that we've defined rings, we now need to define ring homomorphisms.

Definition 8.2. Let R and S be rings and let $f: R \to S$ be a function. We say f is a **ring homomorphism** if it satisfies the following three properties:

1. It preserves addition, that is, $f(a+b) = f(a) + f(b)$ for all $a, b \in R$.
2. It preserves multiplication, that is, $f(ab) = f(a)f(b)$ for all $a, b \in R$.
3. It preserves the multiplicative identity element, that is, $f(1) = 1$.

We say f is an **isomorphism** if there exists a ring homomorphism $g: S \to R$ such that $f \circ g = 1_S$ and $g \circ f = 1_R$, where $1_R: R \to R$ and $1_S: S \to S$ are the identity map (note that this is equivalent to f being bijective). In this case, we say R is isomrophic to S as rings and we denote this by $R \cong S$.

Note that property 1 is simply saying that f is a group of homomorphism of the underlying abelian groups. This automatically implies f preserves the additive identity, that is, $f(0) = 0$. Since multiplicative inverses do not necessarily exist in a ring, property 3 is not guaranteed from property 2.

Example 8.1. Suppose f is a ring homomorphism from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. Then f is completely determined by where it maps $(1,0)$ and $(0,1)$. Indeed, we have

$$\begin{aligned} f(a,b) &= f((a,0) + (0,b)) \\ &= f(a,0) + f(0,b) \\ &= af(1,0) + bf(0,1). \end{aligned}$$

for all $(a,b) \in \mathbb{Z} \times \mathbb{Z}$. Now since $(1,0) = (1,0)^2$, we have $f(1,0) = f(1,0)^2$. This implies $f(1,0) \in \{0,1\}$. A similar argument shows $f(0,1) \in \{0,1\}$. Thus there are only four possible ring homomorphisms from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$, namely

$$\begin{aligned} f_0(a,b) &= 0 \\ f_1(a,b) &= a \\ f_2(a,b) &= b \\ f_3(a,b) &= a+b \end{aligned}$$

for all (a,b) in $\mathbb{Z} \times \mathbb{Z}$. It's easy to see that f_0, f_1, and f_2 are in fact ring homomorphisms. On the other hand, f_3 is not a ring homomorphism. To see this, note that if $a, b, c, d \in \mathbb{Z}$ such that $ad + bc \neq 0$, then

$$\begin{aligned} f_3(a,b)f_3(c,d) &= (a+b)(c+d) \\ &= ac + ad + bc + bd \\ &\neq ac + bd \\ &= f_3(ac, bd), \end{aligned}$$

8.3 Subrings

Definition 8.3. Let R be a ring and let S be a subset of R. We say S is a **subring** of R if it is a ring which satisfies the following two properties:

1. It shares the same addition and multilpication operations as R.
2. It shares the same multiplicative identity, which we always denote by 1.

Note that we really do need to include property 2 in this definition. This can be seen in the following example:

Example 8.2. In $\mathbb{Z}/\langle 6 \rangle$, the subset $\{0,3\}$ with addition and multiplication mod 6 is a ring in its own right with identity 3 since $3^2 = 9 = 3$. So $\{0,3\}$ is a subset of $\mathbb{Z}/\langle 6 \rangle$ "with a ring structure". Its multiplicative identity is not the multiplicative identity of $\mathbb{Z}/\langle 6 \rangle$, so we do not consider $\{0,3\}$ to be a subring of $\mathbb{Z}/\langle 6 \rangle$.

8.4 Ideals

Definition 8.4. Let R be a ring. A subset $I \subseteq R$ is a **left ideal** of R is I is a subgroup of R under addition and if $rx \in I$ for all $x \in I$ and $r \in R$. A subset $I \subseteq R$ is a **right ideal** of R is I is a subgroup of R under addition and if $xr \in I$ for all $x \in I$ and $r \in R$. If I is both a left and right ideal.

Remark 15. If R is commutative, then left and right ideals are the same. In general though, a left ideal may *not* be a right ideal.

Example 8.3. Let $I = \left\{ \left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right) \mid a, b \in \mathbb{Z} \right\}$. Then I is a left ideal of $M_2(\mathbb{Z})$ but I is not a right ideal of $M_2(\mathbb{Z})$. For instance, $\left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right) \notin I$.

Example 8.4. Let $I = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) \mid a, b \in \mathbb{Z} \right\}$. Then I is a right ideal of $M_2(\mathbb{Z})$ but I is not a left ideal of $M_2(\mathbb{Z})$.

Example 8.5. Let $I = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in 2\mathbb{Z} \right\}$. Then I is a two-sided ideal of $M_2(\mathbb{Z})$.

Example 8.6. The ideals of $\mathbb{Z}$ are of the form $\langle m \rangle = m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$.

Remark 16. Any ideal of R is a subring of R.

Proposition 8.1. *Let R and S be rings and let $\varphi : R \to S$ be a ring homomorphism. Then Kerφ is an ideal of R.*

Proof. We know Kerφ is an abelian subgroup of R, since if $x, y \in \text{Ker}\varphi$, then $\varphi(x - y) = \varphi(x) - \varphi(y) = 0$. So $x - y \in \text{Ker}\varphi$. Now let $r \in R$ and $x \in \text{Ker}\varphi$. Then $\varphi(rx) = \varphi(r)\varphi(x) = 0 = \varphi(x)\varphi(r) = \varphi(xr)$, so rx and xr belong to Kerφ. $\square$

Example 8.7. Let $\pi : \mathbb{Z} \to \mathbb{Z}_m$ be the standard quotient map, denoted $\pi(a) = \bar{a}$. Then Ker$\pi = m\mathbb{Z}$.

8.5 Quotient Rings

Let R be a ring. Let $I \subseteq R$ such that I is a subgroup of R under addition. Since R is abelian, we can form the group R/I. We define multiplication on R/I by $\bar{a} \cdot \bar{b} := \overline{ab}$. Multilpication is well-defined if and only if I is an two-sided ideal. Suppose $\overline{a + x}$ and $\overline{b + y}$ are different representatives. Then

$$\begin{aligned} \overline{a + x} \cdot \overline{b + y} &= \overline{(a + x)(b + y)} \\ &= \overline{ab + ay + xb + xy}. \end{aligned}$$

In order for $\overline{ab + ay + xb + xy} = \overline{ab}$, we need $ay + xb + xy \in I$ for all $x, y \in I$. Setting $x = 0$ tells us I must be a left ideal. Setting $y = 0$ tells us I must be a right ideal. It's easy to see that multipication in R/I is associative and distributive.

Definition 8.5. Let R be a ring and let I be a two-sided ideal of R. Then R/I is called the **quotient ring** of R by I.

Remark 17.

1. If R is commutative, then R/I is commutative.
2. If R has identity, then R/I has identity.

8.6 Properties of Ideals

Definition 8.6. Let R be a ring with identity and let A be a nonempty subset of R. The **left ideal of R generated by A is**

$$\langle A \rangle_\ell = \bigcap_{\substack{I = \textbf{left ideal of } R \\ A \subseteq I}} I$$

Remark 18. This is similarly defined for right ideals and two-sided ideals.

Proposition 8.2. $\langle A \rangle_\ell = RA = \{r_1 a_1 + \cdots + r_n a_n \mid n \in \mathbb{N},\ r_i \in R,\ a_i \in A\}$.

Proof. It is clear RA contains A. We prove that RA is a left ideal in R which contains A. Suppose $r_1 a_1 + \cdots + r_n a_n$ and $r_1' a_1' + \cdots + r_n' a_n'$ are two elements in RA. Then

$$r_1 a_1 + \cdots + r_n a_n - (r_1' a_1' + \cdots + r_n' a_n') = r_1 a_1 + \cdots + r_n a_n - r' a_1' - \cdots - r_n' a_n' \in RA$$

So RA is subgroup of R under addtion. Next suppose $r \in R$ and $r_1 a_1 + \cdots + r_n a_n \in RA$, then

$$r \cdot (r_1 a_1 + \cdots + r_n a_n) = (rr_1) a_1 + \cdots + (rr_n) a_n \in RA.$$

So RA is closed under left scalar multiplication. Finally, the distributivity laws follow from the fact that RA is a subset of R and shares the same addition and scalar multiplication action. Therefore $\langle A \rangle_\ell \subseteq RA$.

Now we show $RA \subseteq \langle A \rangle_\ell$. To do this, we show for any left ideal I containing A, that $RA \subseteq I$. Suppose $r_1 a_1 + \cdots + r_n a_n \in RA$. Since I is an ideal which contains A, $r_i a_i \in I$ for all $1 \le i \le n$. Since I is closed under addition, $r_1 a_1 + \cdots + r_n a_n \in I$. Therefore $RA \subseteq \langle A \rangle_\ell$ and $RA \supseteq \langle A \rangle_\ell$, which implies $RA = \langle A \rangle_\ell$. $\square$

Remark 19. This is similarly proved for right ideals and two-sided ideals, using $AR = \{a_1r_1 + \cdots + a_nr_n \mid n \in \mathbb{N},\ r_i \in R,\ a_i \in A\}$ and $RAR = \{r_1a_1s_1 + \cdots + r_na_ns_n \mid n \in \mathbb{N},\ r_i, s_i \in R,\ a_i \in A\}$.

Definition 8.7. If $A = \{a\}$, then

1. $Ra = \{ra \mid r \in R\}$ is the **left principal ideal generated by** a.
2. $aR = \{ar \mid r \in R\}$ is the **right principal ideal generated by** a.
3. $RaR = \{r_1as_1 + \cdots + r_nas_n \mid r_i, s_i \in R,\ n \in \mathbb{N}\}$ is the **left principal ideal generated by** a

Example 8.8. In $\mathbb{Z}[x]$, the ideal $\langle 2, x\rangle$ is *not* principle.

Definition 8.8. Let R be a ring. A proper ideal $\mathfrak{m}$ of R is called **maximal** if the only ideals of R containing $\mathfrak{m}$ are $\mathfrak{m}$ and R.

Example 8.9. Let $m \in \mathbb{N}$. Then $m\mathbb{Z}$ is maximal in $\mathbb{Z}$ if and only if m is prime.

Proposition 8.3. *Let R be a ring. Then every proper ideal is contained in some maximal ideal.*

Proposition 8.4. *Let R be a commutative ring. A proper ideal $\mathfrak{m}$ of R is maximal if and only if $R/\mathfrak{m}$ is a field.*

Example 8.10. Let p be a prime. We show that $\langle p, x\rangle$ is a maximal ideal in $\mathbb{Z}[x]$ by showing $\mathbb{Z}[x]/\langle p, x\rangle \cong \mathbb{Z}_p$. Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p$ be given by $\varphi(a_0 + a_1x + \cdots + a_nx^n) = \overline{a_0}$. We show φ is a ring homomorphism. It is clearly additive, so we show it is multiplicative:

$$\begin{aligned}
\varphi((a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_nx^n)) &= \varphi(a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + (a_0b_n + \cdots + a_nb_0)x^n) \\
&= \overline{a_0b_0} \\
&= \overline{a_0}\overline{b_0} \\
&= \varphi(a_0 + a_1x + \cdots + a_nx^n)\varphi(b_0 + b_1x + \cdots + b_nx^n)
\end{aligned}$$

By the first isomorphism theorem, $\mathbb{Z}[x]/\mathrm{Ker}\varphi \cong \mathrm{Im}\varphi \cong \mathbb{Z}_p$. Clearly the kernel is $\langle 2, x\rangle$.

Definition 8.9. Let R be a ring. Denote $\mathrm{Max}(R) = \{\mathfrak{m} \mid \mathfrak{m} \text{ is a maximal ideal in } R\}$

Example 8.11. Let R be a ring. Then $R[x]/\langle x\rangle \cong R$. So $\langle x\rangle$ is a maximal ideal in $R[x]$ if and only if R is a field.

Definition 8.10. Let R be a commutative ring. An ideal $\mathfrak{p}$ of R is **prime** if $\mathfrak{p} \neq R$ and if whenever $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Definition 8.11. We denote $\mathrm{Spec}(R) = \{\mathfrak{p} \mid \mathfrak{p} \text{ is a prime ideal in } R\}$.

Example 8.12. The prime ideals in $\mathbb{Z}$ are $\langle 0\rangle$ and $\langle p\rangle$ where p is a prime number.

Proposition 8.5. *Let R be a commutative ring. Then an ideal $\mathfrak{p}$ of R is prime if and only if $R/\mathfrak{p}$ is an integral domain.*

Proof. Suppose $\mathfrak{p}$ is a prime ideal in R and suppose $\overline{a}, \overline{b} \in R/\mathfrak{p}$ such $\overline{ab} = \overline{0}$. This implies $ab \in \mathfrak{p}$, which implies either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, which is exactly the same as saying either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. Conversely, suppose $R/\mathfrak{p}$ and suppose $a, b \in R$ such that $ab \in \mathfrak{p}$. Then $\overline{ab} = 0$ implies either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, which is the same as saying either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. □

Corollary 11. *Maximal ideals are prime ideals.*

Definition 8.12. Let R be a commutative ring. Then R is called a **local ring** if it has a unique maximal ideal.

Proposition 8.6. *Let R be a commutative ring. The following statements are equivalent:*

1. *R is a local ring.*
2. *$1 + x \in R^\times$ whenever $x \in R \setminus R^\times$*

Proof. (1) $\implies$ (2): Let $\mathfrak{m} \in \mathrm{Max}(R)$ and let $x \in R \setminus R^\times$. Then $\langle x\rangle$ must be contained in a maximal ideal, and the only one available is $\mathfrak{m}$. Suppose $(1 + x) \neq R$. Then $1 + x \in \mathfrak{m}$ by the same argument. But then $1 = x - (1 + x) \in \mathfrak{m}$ which is a contradiction. Therefore $1 + x$ is a unit. (2) $\implies$ (1) : Suppose $\mathfrak{m}$ and $\mathfrak{m}'$ are maximal ideals such that $\mathfrak{m} \neq \mathfrak{m}'$. Then $\mathfrak{m} \subset \mathfrak{m} + \mathfrak{m}' \subset R$. Since $\mathfrak{m} \neq \mathfrak{m}'$, we must have $\mathfrak{m} + \mathfrak{m}' = R$. So $1 = a + b$ where $a \in \mathfrak{m}$ and $b \in \mathfrak{m}'$. So $a = 1 - b$ with $b \notin R^\times$, but that would make $a \in R^\times$, which is a contradiction. □

9 Basic Theorems

In this section, we go over some basic theorems in Ring Theory.

9.1 Isomorphism Theorems

The isomorphism theorems from Group Theory have an analogue in Ring Theory.

9.1.1 First Isomorphism Theorem

Theorem 9.1. *(First Isomorphism Theorem) Let R and S be rings and let $\varphi\colon R \to S$ be a ring homomorphism. Then*

1. *The kernel of φ is a two-sided ideal in R.*

2. *The image of φ is a subring of S and moreover we have the ring isomorphism $R/\ker\varphi \cong \operatorname{im}\varphi$.*

Proof. 1. First let us check $\ker\varphi$ is a two-sided ideal in R. First note that $\ker\varphi$ is an additive subgroup of R. Indeed, this follows from the first isomorphism theorem for groups. So to show that $\ker\varphi$ is a two-sided ideal in R, it suffices to show that it is closed under scalar multiplication: let $a \in R$ and let $x \in \ker\varphi$. Then

$$\begin{aligned}\varphi(ax) &= a\varphi(x)\\ &= a \cdot 0\\ &= 0\end{aligned}$$

implies $ax \in \ker\varphi$. A similar computation shows that $xa \in \ker\varphi$. Thus $\ker\varphi$ is a two-sided ideal in R.

2. First let us check $\operatorname{im}\varphi$ is a subring of S. Again, it follows from the first isomorphism theorem for groups that $\operatorname{im}\varphi$ is an additive subgroup of S. So to show that $\operatorname{im}\varphi$ is a subring of R, it suffices to show that $\operatorname{im}\varphi$ is closed under multiplication in S and shares the same identity: let $\varphi(a), \varphi(b) \in \operatorname{im}\varphi$ where $a, b \in R$. Then since φ is a ring homomorphism, we have

$$\begin{aligned}\varphi(a)\varphi(b) &= \varphi(ab)\\ &\in \operatorname{im}\varphi.\end{aligned}$$

It follows that $\operatorname{im}\varphi$ is closed under multiplication in S. It also shares the same identity as S since ring homomoprhisms by definition maps the multiplicative identity in R to the multiplicative identity in S.

Next, we define $\overline{\varphi}\colon R/\ker\varphi \to \operatorname{im}\varphi$ by

$$\overline{\varphi}(\overline{a}) = \varphi(a) \tag{32}$$

for all $\overline{a} \in R/\ker\varphi$. By the first isomorphism theorem for groups, $\overline{\varphi}$ is a well-defined group isomorphism. To see that $\overline{\varphi}$ is a *ring* isomorphism, it suffices to show that φ respects multiplication and that it maps the multiplicative identity in $R/\ker\varphi$ to the multiplicative identity in $\operatorname{im}\varphi$: let $\overline{a}, \overline{b} \in R/\ker\varphi$. Then

$$\begin{aligned}\overline{\varphi}(\overline{a}\overline{b}) &= \overline{\varphi}(\overline{ab})\\ &= \varphi(ab)\\ &= \varphi(a)\varphi(b)\\ &= \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b}).\end{aligned}$$

Also $\overline{\varphi}(\overline{1}) = \varphi(1) = 1$. It follows that $\overline{\varphi}$ gives a ring isomorphism from $R/\ker\varphi$ to $\operatorname{im}\varphi$. □

9.1.2 Second Isomorphism Theorem

Theorem 9.2. *(Second Isomorphism Theorem) Let R be a ring, A be a subring of R, and B an ideal of R. Then*

1. *$A + B = \{a + b \mid a \in A,\ b \in B\}$ is a subring of R.*

2. *$A \cap B$ is an ideal of A.*

3. *$A/A \cap B \cong (A + B)/B$.*

Proof.

1. Since A and B are normal subroups of R under additon, $A + B$ is a subgroup of R under addition too. Multiplication is given by

$$(a + b)(a' + b') = aa' + ab' + ba' + bb' \in A + B$$

where $a, a' \in A$ and $b, b' \in B$, so $A + B$ is closed under multiplication. Left and right distributive laws hold because $A + B$ is a subset of R with the same addition and multiplication operations.

2. Suppose $a \in A$ and $x \in A \cap B$. Since B is an ideal, $ax \in B$. Since A is a ring, $ax \in A$. So $ax \in A \cap B$.

3. Define a map $\varphi : A + B \to A/A \cap B$ by $\varphi(a+b) = \bar{a}$. This is well-defined since if $a' + b' = a + b$ is another representation, then

$$\begin{aligned}\varphi(a'+b') &= \overline{a'} \\ &= \overline{a+b-b'} \\ &= \bar{a},\end{aligned}$$

since $b - b' \in A \cap B$. The map φ is clearly surjective, and $\mathrm{Ker}\varphi = B$. So by the first isomorphism theorem, $A/A \cap B \cong (A+B)/B$.

$\square$

Example 9.1. Take $R = \mathbb{Z}$, $A = 12\mathbb{Z}$, and $B = 15\mathbb{Z}$. Then $A + B = 3\mathbb{Z}$ and $A \cap B = 60\mathbb{Z}$. So the second isomorphism theorem tells us $12\mathbb{Z}/60\mathbb{Z} \cong 3\mathbb{Z}/15\mathbb{Z}$.

Theorem 9.3. *(Third Isomorphism Theorem) Let R be a ring and let I, J be ideals in R such that $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.*

Proof. Let $\varphi : R/I \to R/J$ be given by $\varphi(\bar{a}) = \bar{a}$. This is well-defined since if $\overline{a+x}$ is another representative, then

$$\begin{aligned}\varphi(\overline{a+x}) &= \overline{a+x} \\ &= \bar{a}\end{aligned}$$

since $I \subseteq J$. The map φ is a surjective ring homomorphism with kernel J/I. So by the first isomorphism theorem, $(R/I)/(J/I) \cong R/J$. $\square$

Example 9.2. Show that the equation $x^2 + y^2 = 3z^2$ has no solutions in $\mathbb{Z}$. Suppose (a, b, c) is a solution. We can assume $\gcd(a, b, c) = 1$ since $x^2 + y^2 - 3z^2$ is homogeneous. Then $x^2 + y^2 \equiv 3z^2 \bmod n$ for any $n \geq 2$. However when $n = 4$, we run into a problem, since $a^2 + b^2 + c^2 \equiv 0 \bmod 4$ has no solutions where a, b, c are relatively prime.

9.2 The Chinese Remainder Theorem

Definition 9.1. Let I and J be ideals in R. We say I and J are **relatively prime** to one another if $I + J = R$.

Remark 20. In other words, there exists $x \in I$ and $y \in J$ such that $x + y = 1$.

Example 9.3. If $I = a\mathbb{Z}$ and $J = b\mathbb{Z}$, then I and J are relatively prime if and only if $\gcd(a, b) = 1$.

Lemma 9.4. *Let $I_1, \ldots, I_k$ be pairwise relatively prime*

1. *If I and J are relatively prime, then $I \cap J = IJ$.*

2. *If $I_1, \ldots, I_k$ are pairwise relatively prime (i.e. $I_i + I_j = R$ for $i \neq j$), then $I_1 \cdots I_k = I_1 \cap \cdots \cap I_k$.*

Proof.
1. The inclusion $IJ \subset I \cap J$ holds in every ring. For the reverse inclusion, note that

$$\begin{aligned}I \cap J &= (I \cap J)(I + J) \\ &= (I \cap J)I + (I \cap J)J \\ &\subseteq JI + IJ \\ &= IJ.\end{aligned}$$

2. We prove by induction on k. The base case is (1). Now suppose the statement is true for some $k - 1 \geq 1$. Since $I_1, \ldots I_{k-1}$ are relatively prime to I_k, there exists $x_i \in I_i$ and $y_i \in I_k$ such that $x_i + y_i = 1$ for all $1 \leq i < k$. Choose such $x_i \in I_i$ and $y_i \in I_k$ for all $1 \leq i < k$. Then

$$\begin{aligned}1 &= (x_1 + y_1) \cdots (x_{k-1} + y_{k-1}) \\ &\in I_1 \cdots I_{k-1} + I_k.\end{aligned}$$

Therefore $I_1 \cdots I_{k-1}$ and I_k are relatively prime. Therefore using the base case and induction step, we see that

$$\begin{aligned}I_1 \cap \cdots \cap I_k &= (I_1 \cdots I_{k-1}) \cap I_k \\ &= I_1 \cdots I_k.\end{aligned}$$

$\square$

Theorem 9.5. *(The Chinese Remainder Theorem) Let $I_1, \dots, I_k$ be pairwise relatively prime ideals in R. Then*

$$R/I_1 \cdots I_k \cong R/I_1 \times \cdots \times R/I_k.$$

Proof. Let $\varphi \colon R \to R/I_1 \times \cdots \times R/I_k$ be the ring homomorphism given by

$$\varphi(r) = (r + I_1, \dots, r + I_k)$$

for all $r \in R$. We first show that φ is surjective. Let $(r_1 + I_1, \dots, r_k + I_k) \in R/I_1 \times \cdots \times R/I_k$. Since $I_1, \dots, I_k$ are pairwise relatively prime, for each $1 \leq i < j \leq k$, there exists $x_{ij} \in I_i$ and $x_{ji} \in I_j$ such that $x_{ij} + x_{ji} = 1$. Set

$$r := \sum_{j=1}^{k} r_j x_{1j} \cdots \widehat{x}_{jj} \cdots x_{kj} \in R,$$

where the hat symbol means omit that element. Then $\varphi(r) = (r_1 + I_1, \dots, r_k + I_k)$. Indeed, since $x_{ij} \equiv 1 \bmod I_j$ with j fixed and $i \neq j$, we have $r \bmod I_j \equiv r_j$.

Next, observe that the kernel of φ is given by $I_1 \cdots I_k$. Indeed, $\varphi(r) = 0$ if and only if $r + I_j = I_j$ for all $j = 1, \dots, k$ if and only if $r \in I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$. The theorem now follows from the first isomorphism theorem for rings. □

10 Integral Domains

In this section, we discuss integral domains. Let us begin with some definitions.

Definition 10.1. Let R be a ring and let a be a nonzero element of R.

1. We say a is a **zerodivisor** if there exists a nonzero b of R such that $ab = 0$.

2. We say a is a **nonzerodivisor** (or an R**-regular element**) if a is not a zerodivisor. Equivalent, a is a nonzerodivsior if the homothety map $\mathrm{m}_a \colon R \to R$ is injective, where m_a is defined by $\mathrm{m}_a(b) = ab$ for all $b \in R$.

3. We say R is an **integral domain** (or simply **domain**) if every nonzero element of R is a nonzerodivisor.

Many rings which we are familiar with are integral domains. For instance ring of integers $\mathbb{Z}$ is an integral domain. Also every field is an integral domain. The next proposition tells us when a quotient ring is an integral domain.

Proposition 10.1. *Let I be an ideal of R. Then R/I is an integral domain if and only if I is prime.*

Proof. Suppose I is prime and suppose $\overline{x}, \overline{y} \in R/I$ with $\overline{xy} = 0$. Then $xy \in I$. Since I is prime, we either have $x \in I$ or $y \in I$. In other words, either $\overline{x} = 0$ or $\overline{y} = 0$. Thus R/I is an integral domain.

Conversely, suppose R/I is an integral domain. Let $x, y \in R$ such that $xy \in I$. Then $\overline{xy} = 0$ in R/I. Since R/I is an integral domain, we either have $\overline{x} = 0$ or $\overline{y} = 0$. In other words, either $x \in I$ or $y \in I$. Thus I is a prime ideal. □

10.1 Euclidean Domains

Definition 10.2. An integral domain R is called **Euclidean** if there is a function $\mathrm{d} \colon R \backslash \{0\} \to \mathbb{Z}_{\geq 0}$ such that R has division with remainder with respect to d: for all a and b in R with $b \neq 0$ we can find q and r in R such that

$$a = bq + r, \qquad r = 0 \text{ or } \mathrm{d}(r) < \mathrm{d}(b). \tag{33}$$

We allow $a = 0$ in this definition since in that case we can use $q = 0$ and $r = 0$. A function satisfying (33) is called a **Euclidean function**.

10.1.1 Examples of Euclidean Domains

Example 10.1. Let K be a field. Then K is a Euclidean domain with respect to the Euclidean function $\mathrm{d} \colon K \backslash \{0\} \to \mathbb{Z}_{\geq 0}$ given by

$$\mathrm{d}(x) = 0$$

for all $x \in K$. Indeed, if $a, b \in K$ with $b \neq 0$, then we set $q = ab^{-1}$ and $r = 0$.

Example 10.2. The ring of integers $\mathbb{Z}$ is a Euclidean domain with respect to the Euclidean function $\mathrm{d}\colon \mathbb{Z}\backslash\{0\} \to \mathbb{N}$ given by

$$\mathrm{d}(m) = |m|$$

for all $m \in \mathbb{Z}$. Indeed, let $a, b \in \mathbb{Z}$ with $b \neq 0$. If $|a| < |b|$, then we set $q = 0$ and $r = a$, so assume $|a| > |b|$. Without loss of generality, assume both a and b are positive. Then there is a $q \in \mathbb{Z}$ such that

$$bq \leq a < b(q+1).$$

Choose such a $q \in \mathbb{Z}$ and set $r = a - bq$. If $bq = a$, then $r = 0$, otherwise

$$\begin{aligned} |r| &= |a - bq| \\ &< |b(q+1) - bq| \\ &= |b(q+1-q)| \\ &= |b|. \end{aligned}$$

Remark 21. Let (R, d) be a Euclidean domain and let $a, b \in R$ with $b \neq 0$. Suppose that

$$a = bx + y$$

where $x, y \in R$. Then it may not be the case that either $\mathrm{d}(y) = 0$ or $\mathrm{d}(y) < \mathrm{d}(b)$. Being a Euclidean domain just means that there exists at least one such pair of elements $q, r \in R$ such that

$$a = bq + r$$

where $r = 0$ or $\mathrm{d}(r) < \mathrm{d}(b)$. For instance, in $\mathbb{Z}$, we have

$$10 = 3 \cdot 1 + 7,$$

where $|7| \neq 0$ and $|7| \not< |3|$.

Example 10.3. Let K be a field. Then $K[T]$ is a Euclidean Domain with respect to the Euclidean function $\mathrm{d}\colon K[T]\backslash\{0\} \to \mathbb{N}$ given by

$$\mathrm{d}(f) = \deg f$$

for all $f \in K[T]\backslash\{0\}$. Indeed, suppose $f, g \in K[T]$ with $g \neq 0$. We can perform long division to get $q, r \in K[T]$ such that

$$f = gq + r$$

where either $r = 0$ or $\deg r < \deg g$.

Example 10.4. The Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain with respect to the Euclidean function $\mathrm{d}\colon \mathbb{Z}[i]\backslash\{0\}$ given by

$$\mathrm{d}(m + in) = |m + in| = m^2 + n^2$$

for all $m + in \in \mathbb{Z}[i]$. To see how this works, let $z_1 = m_1 + in_1$ and $z_2 = m_2 + in_2$ be two Gaussian integers with $z_2 \neq 0$. Then z_1/z_2 may not be a Gaussian integer, but it is a complex number. Recall that the Gaussian integers forms a lattice inside the complex plane. In particular, we can choose q to be a Gaussian integer which is as closed to z_1/z_2 as possible; that is if z is any other Gaussian integer, then we have $|q - z_1/z_2| \leq |z - z_1/z_2|$. Now with q chosen, we set $r = z_1 - z_2 q$. Clearly, both r and q are Gaussian integers. We also have $z_1 = z_2 q + r$. Finally, note that $|q - z_1/z_2| \leq 1/\sqrt{2}$ (here we are using the fact that the Gaussian integers forms a lattice inside of the complex plane). In particular, if $r \neq 0$, then we see that

$$\begin{aligned} \mathrm{d}(r) &= \mathrm{d}(z_1 - z_2 q) \\ &= |z_1 - z_2 q| \\ &= |z_2||z_1/z_2 - q| \\ &\leq |z_2|/\sqrt{2} \\ &< |z_2| \\ &= \mathrm{d}(z_2). \end{aligned}$$

10.1.2 Refining the Euclidean Function

Let (R, d) be a Euclidean domain. We will introduce a new Euclidean function $\widetilde{\mathrm{d}}\colon R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$, built out of d, which satisfies the **$\widetilde{\mathrm{d}}$-inequality**

$$\widetilde{\mathrm{d}}(a) \leq \widetilde{\mathrm{d}}(ab) \tag{34}$$

for all $a, b \in R\backslash\{0\}$. We define $\widetilde{\mathrm{d}}$ as follows: for nonzero a in R, we set

$$\widetilde{\mathrm{d}}(a) = \min_{b \neq 0} \mathrm{d}(ab).$$

That is, $\widetilde{\mathrm{d}}(a)$ is the smallest d-value on the nonzero multiples of a (note that $ab \neq 0$ when $b \neq 0$ since R is an integral domain). Since $a = a \cdot 1$ is a nonzero multilpe of a, we have

$$\widetilde{\mathrm{d}}(a) \leq \mathrm{d}(a)$$

for all nonzero a in R. For each $a \neq 0$ in R, we have $\widetilde{\mathrm{d}}(a) = \mathrm{d}(ab_0)$ for some nonzero b_0 and $\mathrm{d}(ab_0) = \widetilde{\mathrm{d}}(a) \leq \mathrm{d}(ab)$ for all nonzero b. For example,

$$\widetilde{\mathrm{d}}(1) = \min_{b \neq 0} \mathrm{d}(b)$$

is the smallest d-value on $R\backslash\{0\}$.

Proposition 10.2. *$(R, \widetilde{\mathrm{d}})$ is a Euclidean domain. Furthermore, $\widetilde{\mathrm{d}}$ satisfies the inequality (34).*

Proof. We first show that R admits division with remainder with respect to $\widetilde{\mathrm{d}}$. Pick a and b in R with $b \neq 0$. Set $\widetilde{\mathrm{d}}(b) = \mathrm{d}(bc)$ for some nonzero $c \in R$. Using division of a by bc (which is nonzero) in (R, d) there are q_0 and r_0 in R such that

$$a = (bc)q_0 + r_0, \qquad r_0 = 0 \text{ or } \mathrm{d}(r_0) < \mathrm{d}(bc).$$

Set $q = cq_0$ and $r = r_0$, so $a = bq + r$. If $r_0 = 0$ we are done, so assume $r_0 \neq 0$. Then observe that

$$\begin{aligned}\widetilde{\mathrm{d}}(r) &= \widetilde{\mathrm{d}}(r_0) \\ &\leq \mathrm{d}(r_0) \\ &< \mathrm{d}(bc) \\ &= \widetilde{\mathrm{d}}(b).\end{aligned}$$

Thus we have

$$a = bq + r, \qquad r = 0 \text{ or } \widetilde{\mathrm{d}}(r) < \widetilde{\mathrm{d}}(b).$$

Hence $(R, \widetilde{\mathrm{d}})$ is a Euclidean domain.

Now we will show that $\widetilde{\mathrm{d}}$ satisfies the inequality (34). Let $a, b \in R\backslash\{0\}$. Write $\widetilde{\mathrm{d}}(ab) = \mathrm{d}(abc)$ for some nonzero c in R. Since abc is a nonzero multiple of a, we have

$$\widetilde{\mathrm{d}}(a) \leq \mathrm{d}(abc) = \widetilde{\mathrm{d}}(ab).$$

$\square$

Let us now briefly describe two other possible refinements one might want in a Euclidean function: namely uniqueness of the quotient and remainder it produces and multiplicativity.

In $\mathbb{Z}$ we write $a = bq + r$ with $0 \leq r < |b|$ and q and r are *uniqely* determined by a and b. There is also uniqueness of the quotient and remainder when we do division in $F[T]$ (relative to the degree function) and in a field (the remainder is always 0). Are there other Euclidean domains where the quotient and remainder are unique? Division in $\mathbb{Z}[i]$ does *not* have a unique quotient and remainder relative to the norm on $\mathbb{Z}[i]$. For instance, dividing $1 + 8i$ by $2 - 4i$ gives

$$1 + 8i = (2 - 4i)(-1 + i) - 1 + 2i \quad \text{and} \quad 1 + 8i = (2 - 4i)(-2 + i) + 1 - 2i,$$

where both remainders have norm 5, which is less than $\mathrm{N}(2 - 4i) = 20$.

Theorem 10.1. *If R is a Euclidean domain where the quotient and remainder are unique, then R is a field or $R = F[T]$ for a field F.*

10.1.3 Units in Euclidean Domains

In integral domains, there are three types of elements: units, irreducibles, and nonirreducibles. In this subsection, we want to characterize what

Proposition 10.3. *Let (R, d) be a Euclidean domain where* d *satisfies the* d*-inequality and let $n = \inf(\mathrm{d}(R \backslash \{0\}))$. Then $R^\times = \{a \in R \backslash \{0\} \mid \mathrm{d}(a) = n\}$.*

Proof. Let $a \in R\backslash\{0\}$ such that $\mathrm{d}(a) = n$. Then there exists $q, r \in R$ such that

$$1 = aq + r,$$

where either $r = 0$ or $\mathrm{d}(r) < n$. We can't have $\mathrm{d}(r) < n$ since n is the smallest integer value which d takes, so $r = 0$. This implies $1 = aq$, and hence a is a unit. Conversely, suppose a is a unit in R, say $ab = 1$. Choose $c \in R\backslash\{0\}$ such that $\mathrm{d}(c) = n$. Then

$$\begin{aligned} \mathrm{d}(a) &\leq \mathrm{d}(ab) \\ &= \mathrm{d}(1) \\ &\leq \mathrm{d}(c) \\ &= n. \end{aligned}$$

This implies $\mathrm{d}(a) = n$. □

10.1.4 Euclidean Algorithm

Definition 10.3. Let R be a commutative ring and let $a, b \in R$.

1. We say that a **divides** b, written $a \mid b$, if there exists $c \in R$ such that $ac = b$.
2. An element $d \in R$ is a $\gcd(a, b)$ if for all $d' \in R$ such that $d' \mid a$ and $d' \mid b$, we have $d \mid d'$.

We now describe the Euclidean algorithm. Let (R, d) be a Euclidean domain and let $a, b \in R$ with $b \neq 0$. Since R is a Euclidean domain, there exists $q_1, r_1 \in R$ such that

$$a = bq_1 + r_1$$

where either $\mathrm{d}(r_1) < \mathrm{d}(b)$ or $r_1 = 0$. If $r_1 = 0$, then the algorithm is terminated. Otherwise, we have $\mathrm{d}(r_1) < \mathrm{d}(b)$. We again use the fact that R is a Euclidean domain to conclude that there exists $q_2, r_2 \in R$ such that

$$b = r_1 q_2 + r_2$$

where either $\mathrm{d}(r_2) < \mathrm{d}(r_1)$ or $r_2 = 0$. If $r_2 = 0$, then the algorithm is terminated. Otherwise, we have $\mathrm{d}(r_2) < \mathrm{d}(r_1)$. Continuing in this manner, at the ith step, we obtain $q_{i+1}, r_{i+1} \in R$ such that

$$r_{i-1} = r_i q_{i+1} + r_{i+1},$$

where we have a stirictly decreasing sequence in $\mathbb{N}$:

$$\mathrm{d}(b) > \mathrm{d}(r_1) > \mathrm{d}(r_2) > \cdots > \mathrm{d}(r_i).$$

Since $\mathbb{N}$ is well-founded, this algorithm must terminate, say at the nth step (meaning $r_{n+1} = 0$). Thus, at the nth step, we have

$$r_{n-1} = r_n q_{n+1}.$$

In this case, we say that r_n is the last nonzero remainder in the division algorithm for a and b.

Proposition 10.4. *The last nonzero remainder in the division algorithm for a and b is the a $\gcd(a, b)$.*

10.2 Principal Ideal Domains

Definition 10.4. Let R be an integral domain. We say R is a **principal ideal domain (PID)** if every ideal in R is **principal**. In other words, every ideal in R can be generated by one element.

Remark 22. Let K be a field. Every ideal in $K[x]/\langle x^2 \rangle$ is principal. However we do not consider this ring to be a principal ideal domain since it is not a domain.

Proposition 10.5. *Let R be an integral domain. Then R is a PID if and only if every prime ideal is principal.*

Proof. If R is a PID, then every ideal in R is principal, so every prime ideal is principal. Conversely, suppose every prime ideal is principal. Let I be an ideal in R and assume for a contradiction that I is not principal. Consider the partially order set $(\Gamma, \subseteq)$ where

$$\Gamma = \{\text{ideals } \mathfrak{a} \mid I \subseteq \mathfrak{a} \subseteq R \text{ and } \mathfrak{a} \text{ not principal}\}$$

and where $\subseteq$ is set inclusion. Note that Γ is nonempty since $I \in \Gamma$. Also note that every totally ordered subset in Γ has an upper bound. Indeed, if $(\mathfrak{a}_\lambda)_{\lambda \in \Lambda}$ is a totally ordered subset, then $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ is an upper bound of $(\mathfrak{a}_\lambda)$: the set $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ is an ideal which contains I since $(\mathfrak{a}_\lambda)$ is totally ordered and each $\mathfrak{a}_\lambda$ contains I. Also, if $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ is principal, then there must exist some $\mathfrak{a}_\lambda$ which is principal (again since $(\mathfrak{a}_\lambda)$ is totally ordered), thus $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ is *not* principal. Hence

$$\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda \in \Gamma.$$

Thus using Zorn's Lemma, we see that Γ has a maximal element, say $\mathfrak{p} \in \Gamma$. We claim that $\mathfrak{p}$ is a prime ideal. To see this, assume for a contradiction that $\mathfrak{p}$ is not a prime ideal. Choose $a, b \in R$ such that $ab \in \mathfrak{p}$ and $a, b \notin \mathfrak{p}$. Then observe that $\langle \mathfrak{p}, a \rangle$ and $\langle \mathfrak{p}, b \rangle$ both properly contain $\mathfrak{p}$. By maximality of $\mathfrak{p}$, they must both be principal ideals, say $\langle \mathfrak{p}, a \rangle = \langle x \rangle$ and $\langle \mathfrak{p}, b \rangle = \langle y \rangle$. Then observe that

$$\begin{aligned} \mathfrak{p} &\subseteq \langle \mathfrak{p}, a \rangle \langle \mathfrak{p}, b \rangle \\ &= (\mathfrak{p} + \langle a \rangle)(\mathfrak{p} + \langle b \rangle) \\ &= \mathfrak{p} + \langle a \rangle \mathfrak{p} + \mathfrak{p} \langle b \rangle + \langle ab \rangle \\ &\subseteq \mathfrak{p}. \end{aligned}$$

It follows that

$$\begin{aligned} \mathfrak{p} &= \langle \mathfrak{p}, a \rangle \langle \mathfrak{p}, b \rangle \\ &= \langle x \rangle \langle y \rangle \\ &= \langle xy \rangle. \end{aligned}$$

This is a contradiction since $\mathfrak{p} \in \Gamma$. Thus $\mathfrak{p}$ is a prime ideal. However by assumption *all* prime ideals are principal, so $\mathfrak{p}$ being prime implies $\mathfrak{p}$ is principal. But this again contradicts the fact that $\mathfrak{p} \in \Gamma$. Thus every ideal in R must be principal. $\square$

10.2.1 Euclidean Domains are Principal Ideal Domains

Proposition 10.6. *Every Euclidean domain is a principal ideal domain.*

Proof. Let R be a Euclidean domain with respect to the Euclidean function $\mathrm{d}\colon R \backslash \{0\} \to \mathbb{Z}_{\geq 0}$ and let $I \subseteq R$ be an ideal. If $I = 0$, then we are done, so assume $I \neq 0$. Choose $x \in I \backslash \{0\}$ such that $\mathrm{d}(x)$ is minimal; that is, if $y \in I$, then $\mathrm{d}(x) \leq \mathrm{d}(y)$. We claim that $I = \langle x \rangle$. Indeed, let $y \in I$. Since R is a Euclidean domain, we have

$$y = qx + r \tag{35}$$

for some $q, r \in R$ where either $r = 0$ or $\mathrm{d}(r) < \mathrm{d}(x)$. Assume for a contradiction that $r \neq 0$, so $\mathrm{d}(r) < \mathrm{d}(x)$. Rewriting (35) as

$$r = y - qx$$

shows us that $r \in I$ since $x, y \in I$. However, this contradicts our choice of x with $\mathrm{d}(x)$ being minimal, since $r \in I$ and $\mathrm{d}(r) < \mathrm{d}(x)$. Therefore $r = 0$, which implies $y \in \langle x \rangle$. Thus $I \subseteq \langle x \rangle$, and since clearly $\langle x \rangle \subseteq I$, we in fact have $I = \langle x \rangle$. So every ideal in R is principal, which means R is a principal ideal domain. $\square$

Example 10.5. $\mathbb{Z}[x]$ is *not* a PID since $\langle 2, x \rangle$ is not a principal ideal, so it can't be a Euclidean Domain.

10.2.2 Principal Ideal Domains are not Necessarily Euclidean Domains

In this subsection, we will show that the ring $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a principal ideal domain which is not a Euclidean domain. To see why it's not a Euclidean domain, we will need the following propoistion:

Proposition 10.7. *Let (R, d) be a Euclidean domain that is not a field, so there is a nonzero nonunit $a \in R$ with least* d*-value among all nonunits. Then the quotient ring $R/\langle a \rangle$ is represented by* 0 *and units.*

Proof. Pick $x \in R$. By division with remainder in R we can write $x = aq + r$ where $r = 0$ or $\mathrm{d}(r) < \mathrm{d}(a)$. If $r \neq 0$, then the inequality $\mathrm{d}(r) < \mathrm{d}(a)$ forces r to be a unit. Since $x \equiv r \mod a$, we conclude that $R/\langle a \rangle$ is represented by 0 and by units. $\square$

Theorem 10.2. *Let $R = \mathbb{Z}[(1+\sqrt{-19})/2]$. Then R is a principal ideal domain which is not a Euclidean domain.*

Proof. We first show that R is not a Euclidean domain. First note that R is not a field since $\mathbb{Z} \subseteq R$ but $1/2 \notin R$. Therefore to prove R is not Euclidean, we will show that for no nonzero nonunit $a \in R$ is $R/\langle a \rangle$ represented by 0 and units. First we compute the norm of a typical element $\alpha = x + y(1+\sqrt{-19})/2$:

$$\mathrm{N}(\alpha) = x^2 + xy + 5y^2 = \left(x + \frac{y}{2}\right)^2 + \frac{19y^2}{4}. \tag{36}$$

This norm always takes values ≥ 0 (this is cleary from the second expression) and once $y \neq 0$ we have

$$\begin{aligned} \mathrm{N}(\alpha) &\geq \frac{19y^2}{4} \\ &\geq \frac{19}{4} \\ &> 4. \end{aligned}$$

In particular, the units are solutions to $\mathrm{N}(\alpha) = 1$, which are ± 1:

$$R^\times = \{\pm 1\}.$$

The first few norm values are $0, 1, 4, 5, 7$, and 9. In particular, there is no element of R with norm 2 or 3. This and the fact that $R^\times \cup \{0\}$ has size 3 are the key facts we will use.

If R were Euclidean, then there would be a nonzero nonunit a in R such that $R/\langle a \rangle$ is represented by 0 and units, so 0, 1, and -1. Perhaps $1 \equiv -1 \mod a$, but we definitely have $\pm 1 \not\equiv 0 \mod a$. Thus $R/\langle a \rangle$ has size 2 (if $1 \equiv -1 \mod a$) or has size 3 (if $1 \not\equiv= 1 \mod a$). We show this can't happen.

If R/a has size 2 then $2 \equiv 0 \mod a$, so $a \mid 2$ in R. Therefore $\mathrm{N}(a) \mid 4$ in $\mathbb{Z}$. There are no elements of R with norm 2, so the only nonunits with norm dividing 4 are elements with norm 4. A check using (36) shows the only such numbers are ± 2. However, $R/\langle 2 \rangle = R/\langle -2 \rangle$ does not have size 2. For instance, 0, 1, and $(1+\sqrt{-19})/2$ are incongruent modulo ± 2: the difference of two of these (different) numbers, divided by two, is never of the form $x + y(1+\sqrt{-19})/2$ for x and y in $\mathbb{Z}$.

Similarly, if $R/\langle a \rangle$ has size 3, then $a \mid 3$ in R, so $\mathrm{N}(a) \mid 9$ in $\mathbb{Z}$. There is no element of R with norm 3, so a must have norm 9 (it doesn't have norm 1 since it is not a unit). The only elements of R with norm 9 are ± 3, so $a = \pm 3$. The ring $R/\langle 3 \rangle = R/\langle -3 \rangle$ does not have size 3: 0, 1, 2, and $(1+\sqrt{-19})/2$ are incongruent modulo ± 3. Since $R^\times \cup \{0\}$ has size 3 and R has no element a such that $R/\langle a \rangle$ has size 2 or 3, R can't be a Euclidean domain. □

10.2.3 Prime ideals in Principal Ideal Domain are Maximal Ideals

Proposition 10.8. *Let R be a principal ideal domain and let p be a prime in R. Then $\langle p \rangle$ is a maximal ideal.*

Proof. Assume for a contradiction that $\langle p \rangle$ is not a maximal ideal. Choose a maximal ideal which contains $\langle p \rangle$, say $\langle p \rangle \subsetneq \mathfrak{m}$. Since R is a principal ideal domain, we have $\mathfrak{m} = \langle a \rangle$ for some $a \in R$. Then $\langle p \rangle \subsetneq \langle a \rangle$ implies $p = xa$ for some $x \in R$. Since p is a prime ideal, this implies $x \in \langle p \rangle$ (we cannot have $a \in \langle p \rangle$ since this would imply $\langle a \rangle = \langle p \rangle$, a contradiction). Thus $x = py$ for some $y \in R$. Therefore

$$\begin{aligned} 0 &= p - xa \\ &= p - pya \\ &= p(1 - ya). \end{aligned}$$

Since R is an integral domain and $p \neq 0$, this implies $1 = ya$, which implies a is a unit; a contradiction! Thus $\langle p \rangle$ is a maximal ideal. □

Corollary 12. *Let R be a principal ideal domain. Then $R[x]$ is a principal ideal domain if and only if R is a field.*

Proof. Assume R is a field. Then $R[x]$ is an Euclidean domain, and therefore a principal ideal domain. Conversely, assume $R[x]$ is a principal ideal domain. Recall that $R[x]/\langle x \rangle \cong R$. Since $R[x]$ is a principal ideal domain, $\langle x \rangle$ is a maximal ideal, and therefore R is a field. □

10.3 Unique Factorization Domains

Definition 10.5. Let R be an integral domain.

1. A nonzero nonunit element $a \in R$ is said to be **irreducible** if whenever $a = bc$ for some $b, c \in R$, then either $b \in R^\times$ or $c \in R^\times$. If a is not irreducible, then we say a is **reducible**.

2. A nonzero nonunit element $p \in R$ is said to be **prime** if $\langle p \rangle$ is prime.

3. Two nonzero elements $a, b \in R$ are said to be **associate** if $b = au$ for some $u \in R^\times$. We denote this by $a \sim b$.

10.3.1 Equivalent Definitions of Irreducibility

Proposition 10.9. *Let R be an integral domain and let a be a nonzero nonunit element in R. The following are equivalent*

1. *a is irreducible;*
2. *$\langle a \rangle$ is a maximal ideal among the proper principal ideals;*
3. *If $a = bc$, then a is a unit multiple of b or c;*
4. *If $a = bc$, then either $\langle a \rangle = \langle b \rangle$ or $\langle a \rangle = \langle c \rangle$;*

Proof. Let us first show 1 implies 2. Suppose $\langle a \rangle \subseteq \langle b \rangle$ for some nonzero nonunit $b \in R$. Since $\langle b \rangle$ contains $\langle a \rangle$, we have $bc = a$ for some $c \in R$. Since a is irreducible and b is a nonunit, c must be a unit. But then this implies $b = ac^{-1}$, which implies $\langle a \rangle = \langle b \rangle$. Thus $\langle a \rangle$ is a maximal ideal among the proper principal ideals.

Now we show 2 implies 3. Suppose $a = bc$ for some $b, c \in R$. Clearly b and c must be nonzero since a is nonzero. If either b or c is a unit, then we are done, so we may assume that both b and c are nonunits as well. Then $\langle a \rangle \subseteq \langle b \rangle$ and $\langle a \rangle \subseteq \langle c \rangle$. Since $\langle a \rangle$ is maximal among the proper principal ideals, we must have $\langle a \rangle = \langle b \rangle$ and $\langle a \rangle = \langle c \rangle$. This implies $a = bx$ and $a = cy$ for some $x, y \in R$. □

In general commutative rings, we have (1) $\implies$ (2) $\implies$ (3) $\implies$ (4), and none of these implications reverse. For more general commutative rings, (1) is the definition of an irreducible element, (2) is the definition of a strongly irreducible element, (3) is the definition of an m-irreducible element, and (4) is the definition of a very strongly irreducible element. Our focus however is on integral domains, so we will worry about these generalizations. Thus whenever we talk about irreducible or reducible elements, we will always assume that we are in an integral domain.

10.3.2 Primes are Irreducible

Proposition 10.10. *Let R be an integral domain. Then every prime is irreducible.*

Proof. Let p be a prime element in R. Suppose $p = ab$ for some $a, b \in R$. Since p is prime, either $p \mid a$ or $p \mid b$. Without loss of generality, assume $p \mid a$. Then $a = px$ for some $x \in R$. Then $p = (px)b$ implies $p(1 - xb) = 0$. Since R is an integral domain, and $p \neq 0$, we must have $1 - xb = 0$. In other words, b must be a unit. Therefore p is irreducible. □

10.3.3 Irreducibles are Prime in a Principal Ideal Domain

Remark 23. The converse to Proposition (10.10) is *not* always true.

Example 10.6. Take $R = \mathbb{Z}[\sqrt{-5}]$. We will show that 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, but 3 is not prime. Recall the norm $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$, given by $N(a + b\sqrt{-5}) = a^2 + 5b^2$, is multiplicative. Suppose $3 = \alpha\beta$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Then $N(3) = N(\alpha)N(\beta)$ implies $9 = N(\alpha)N(\beta)$. If $N(\alpha) = 9$, then $N(\beta) = 1$. Similarly, if $N(\beta) = 9$, then $N(\alpha) = 1$. So assume $N(\alpha) = N(\beta) = 3$. But this is impossible since there are no integers a and b such that $a^2 + 5b^2 = 3$. So 3 is irreducible. On the other hand, 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$ since $3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$ but $3 \nmid (2 + \sqrt{-5})$ and $3 \nmid (2 - \sqrt{-5})$.

Proposition 10.11. *Let R be a PID. A nonzero element is prime if and only if it is irreducible.*

Proof. From Proposition (10.10), we know that being prime implies being irreducible. So it suffices to check the converse. Let r be an irreducible element in R. Then $\langle r \rangle \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ in R. Since R is a PID, we have $\mathfrak{m} = \langle m \rangle$ for some m in R. Since $\mathfrak{m}$ contains $\langle r \rangle$, there is some $q \in R$ such that $r = mq$. Since r is irreducible and m is not a unit, q must be a unit, so $qu = 1$ for some $u \in R$. Then $m = ru$ implies $\langle r \rangle$ contains $\mathfrak{m}$. Therefore $\mathfrak{m} = \langle r \rangle$. □

10.3.4 Irreducibles are not Necessarily Prime in General

In general, irreducibles are not necessarily prime. Indeed, consider $\mathbb{Q}[X^2, X^3]$. In this ring, both X^2 and X^3 are irreducible. On the other hand, notice that

$$(X^3)(X^3) = X^6 = (X^2)(X^2)(X^2).$$

So X^2 divides the product $(X^3)(X^3)$ but it does not divide any term in that product.

For another example, consider the ring

$$\mathbb{R} + X\mathbb{C}[X] = \{a_0 + a_1X + a_2X + \cdots + a_nX^n \mid n \in \mathbb{Z}_{\geq 0}, a_0 \in \mathbb{R}, a_1, \ldots, a_n \in \mathbb{C}\}.$$

Then X is irreducible in this ring but not prime.

For a final example, consider the ring of all algebraic integers:

$$\overline{\mathbb{Z}} = \{z \in \mathbb{C} \mid z \text{ is a root of a monic polynomial in } \mathbb{Z}[X]\}.$$

This domain has *no* irreducibles. To see this, note that if $z \in \overline{\mathbb{Z}}$, then $\sqrt{z} \in \overline{\mathbb{Z}}$ and $z = \sqrt{z}\sqrt{z}$, where $\sqrt{z} \notin \overline{\mathbb{Z}}^\times$ if $z \notin \overline{\mathbb{Z}}^\times$.

10.3.5 Definition of Unique Factorization Domain

Definition 10.6. Let R be an integral domain. We say R is a **unique factorization domain (UFD)** if every nonzero nonunit element $a \in R$ satisfies the following two properties

1. an irreducible factorization exists: we can express a as a product of irreducible elements, that is,

$$a = p_1 \cdots p_m \tag{37}$$

   where $p_1, \dots, p_m$ are irreducible elements in R. In this case, we call (37) an **irreducible factorization** of a and we say m is the **length** of this irreducible factorization.

2. irreducible factorizations are unique: If we have two irreducible factorizations of a, say

$$p_1 \cdots p_m = a = q_1 \cdots q_n$$

   where $p_1, \dots, p_m$ and $q_1, \dots, q_n$ are irreducible elements in R, then $m = n$ and (perhaps after relabeling the irreducible elements), we have $p_i \sim q_i$ for all $1 \leq i \leq m$. In this case, we say a has a **unique irreducible factorization**.

10.3.6 Irreducible Factorizations Exists in Noetherian Rings

In this subsubsection, we will show that irreducible factorizations of nonzero nonunits exists in a large class of rings. These rings are called Noetherian rings. Let us recall the definition of this ring:

Definition 10.7. Let R be a ring. We say R is a **Noetherian ring** if it satisfies the ascending chain property: if (I_n) is an ascending sequence of ideal in R (where ascending means $I_n \subseteq I_{n+1}$ for all $n \in \mathbb{N}$), then it must **terminate**, that is, there exists an $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$.

Remark 24. One can show that the ascending chain property is equivalent to the property that every ideal in R is finitely generated. In particular, principal ideal domains are Noetherian rings. We will use this fact in a moment.

Proposition 10.12. *Let R be a Noetherian domain and let a be a nonzero nonunit in R. Then a has an irreducible factorization.*

Proof. If a is irreducible, then we are done, so assume that a is reducible. We assume for a contradiction that a cannot be factored into irreducible. Since a is reducible, there is a factorization of a into nonzero nonunits, say

$$a = a_1 b_1.$$

If both a_1 and b_1 can be factored into irreducibles, then so can a, so at least one of them cannot be factored into irreducible elements, say a_1. In particular, a_1 is reducible, and thus there is factorization of a_1 into nonzero nonunits, say

$$a_1 = a_2 b_2.$$

By the same reasoning above, we may assume that a_2 cannot be factored into irreducibles. Proceeding inductively, we construct sequences (a_n) and (b_n) in R where each a_n is reducible and each b_n is a nonzero nonunit, furthermore we have the factorization

$$a_n = a_{n+1} b_{n+1}$$

for all $n \in \mathbb{N}$. In particular, we have an ascending chain of ideals $(\langle a_n \rangle)$. Indeed, $\langle a_n \rangle \subseteq \langle a_{n+1} \rangle$ because $a_n = a_{n+1} b_{n+1}$. Since R is Noetherian, this ascending chain must terminate, say at $N \in \mathbb{N}$. In particular, we have $\langle a_N \rangle = \langle a_{N+1} \rangle$. This implies there exists $c_N \in R$ such that

$$a_N c_N = a_{N+1}.$$

Thus we have

$$\begin{aligned}0 &= a_N - a_{N+1}b_{N+1} \\ &= a_N - a_N c_N b_{N+1} \\ &= a_N(1 - c_N b_{N+1}).\end{aligned}$$

Since R is an integral domain, this implies $b_{N+1}c_N = 1$ (as $a_N \neq 0$), which implies b_{N+1} is a unit. This is a contradiction. □

10.3.7 Principal Ideal Domains are Unique Factorization Domains

In this subsubsection, we will show that every principal ideal domain is a unique factorization domain.

Theorem 10.3. *Let R be a principal ideal domain. Then R is a unique factorization domain.*

Proof. Let a be nonzero nonunit in R. Since R is a Noetherian, an irreducible factorization of a exists, so it suffices to check that such an irreducible factorization is unique. Let

$$p_1 \cdots p_m = a = q_1 \cdots q_n \tag{38}$$

be two irreducible factorizations of a. By relabeling if necessary, we may assume that $m \leq n$. We will prove by induction on $m \geq 1$ that $m = n$ and (perhaps after relabeling) we have $p_i \sim q_i$ for all $1 \leq i \leq m$. For base case $m = 1$, we have

$$p_1 = a = q_1 \cdots q_n.$$

The first step will be to show that $n = 1$. To prove this, we assume for a contradiction that $n > 1$. Since R is a principal ideal domain, every irreducible is a prime. In particular, p_1 is prime. Thus $p_1 \mid q_i$ for some $1 \leq i \leq n$. By relabeling necessary, we may assume that $p_1 \mid q_1$. In terms of ideals, this means $\langle q_1 \rangle \subseteq \langle p_1 \rangle$. Since both $\langle q_1 \rangle$ and $\langle p_1 \rangle$ are both maximal ideals, this implies $\langle q_1 \rangle = \langle p_1 \rangle$. Thus $q_1 = xp_1$ for some $x \in R^\times$. This implies

$$\begin{aligned}0 &= p_1 - q_1 q_2 \cdots q_n \\ &= p_1 - x p_1 q_2 \cdots q_n \\ &= p_1(1 - x q_2 \cdots q_n).\end{aligned}$$

Again $p_1 \neq 0$ and R an integral domain implies $xq_2 \cdots q_n = 1$, thus $q_2 \cdots q_n \in R^\times$. This is a contradiction as each $q_2, \dots, q_n$ are irreducible! Thus $n = 1$, and clearly in this case, we have $p_1 \sim q_1$ (as $p_1 = q_1$).

Now suppose $m > 1$ and we have shown that if a has an irreducible factorization of length k where $1 \leq k < m$, then it has a unique irreducible factorization. Again, let (38) be two irreducible factorizations of a where we may assume that $m \leq n$. Arguing as above, p_1 is prime, and since $q_1 \cdots q_n \in \langle p_1 \rangle$, we must have $q_i \in \langle p \rangle$ for some $1 \leq i \leq n$. By rebaling if necessary, we may assume that $q_1 \in \langle p \rangle$. Thus $\langle q_1 \rangle \subseteq \langle p_1 \rangle$, and since both $\langle q_1 \rangle$ and $\langle p \rangle$ are maximal ideals, we must in fact have $\langle q_1 \rangle = \langle p_1 \rangle$. In particular, $q_1 = p_1 x$ for some $x \in R^\times$. This implies

$$\begin{aligned}0 &= p_1 p_2 \cdots p_m - q_1 q_2 \cdots q_n \\ &= p_1 p_2 \cdots p_m - p_1 x q_2 \cdots q_n \\ &= p_1(p_2 \cdots p_m - x q_2 \cdots q_n).\end{aligned}$$

Since $p_1 \neq 0$ and R is an integral domain, this implies

$$p_2 \cdots p_m = x q_2 \cdots q_n.$$

Note that xq_2 is an irreducible element, and thus we may apply induction step to get $m = n$ and (perhaps after relabeling) $p_i \sim q_i$ for all $2 \leq i \leq m$. Since already we have $p_1 \sim q_1$, we are done. □

10.3.8 Irreducibles are Prime in a Unique Factorization Domain

Proposition 10.13. *Let R be a unique factorization domain and let p be an irreducible element in R. Then p is prime.*

Proof. Assume for a contradiction that p is not prime. Thus there exists $a, b \in R \backslash \langle p \rangle$ such that $ab \in \langle p \rangle$. Note that a and b are necessarily nonzero nonunits. Since $ab \in \langle p \rangle$, we have $xp = ab$ for some $x \in R$. Let

$$a = q_1 \cdots q_k \quad \text{and} \quad b = q_{k+1} \cdots q_m$$

be the unique irreducible factorizations of a and b respetively (here we have $m > k$). Then

$$xp = q_1 \cdots q_m.$$

Since R is a unique factorization domain, we must have $p \sim q_i$ for some $1 \leq i \leq m$. By relabeling if necessary, we may assume that $p \sim q_1$. Finally, since $q_1 \mid a$ and $p \sim q_1$, we see that $p \mid a$, which is a contradiction. □

10.3.9 If R is a Unique Factorization Domain, then $R[T]$ is a Unique Factorization Domain

In this subsubsection, we will show that if R is a unique factorization domain, then $R[T]$ is also a unique factorization domain (this is actually an if and only if statement, but the converse is clear, so we don't state that). We first note that if K is a field, then $K[T]$ is a unique factorization domain. Indeed, $K[T]$ is a principal ideal domain, and thus a unique factorization domain.

Proposition 10.14. *Let R be a unique factorization domain. Then $R[T]$ is a unique factorization domain.*

Proof. Let $a(T)$ be a nonzero nonunit in $R[T]$ and let K be the fraction field of R. First note that $R[T]$ is Noetherian, and thus $a(T)$ has an irreducible factorization. Suppose

$$p_1(T) \cdots p_m(T) = a(T) = q_1(T) \cdots q_n(T)$$

are two irreducible factorizations of $a(T)$ in $R[T]$. By Gauss' Lemma, each $p_i(T)$ and $q_j(T)$ is irreducible in $K[T]$. Since $K[T]$ is a unique factorization domain, we see that $m = n$ and (perhaps after relabeling) $p_i(T) \sim q_i(T)$ in $K[T]$. In particular, $p_i(T) = x_i q_i(T)$ for some $x_i \in K[T]^\times = K^\times$. Note that since $p_i(T), q_i(T) \in R[T]$, we must have $x_i \in R \backslash \{0\}$. Therefore

$$\begin{aligned} 0 &= p_1(T) \cdots p_m(T) - q_1(T) \cdots q_m(T) \\ &= p_1(T) \cdots p_m(T) - x_1 \cdots x_m p_1(T) \cdots p_m(T) \\ &= p_1(T) \cdots p_m(T)(1 - x_1 \cdots x_m) \\ &= a(T)(1 - x_1 \cdots x_m), \end{aligned}$$

and since $a(T) \neq 0$ and $R[T]$ is a domain, this implies $1 = x_1 \cdots x_n$, which implies each x_i is a unit in R. Thus $p_i(T) \sim q_i(T)$ in $R[T]$. □

11 Polynomial Rings

An important class of rings are the **polynomial rings**. If R is a ring, then we define the **polynomial ring over R in n-variables**, denoted $R[X_1, \dots, X_n]$, to be the set of all elements of the form

$$\sum_{(\alpha_1,\dots,\alpha_n)\in\mathbb{Z}^n_{\geq 0}} a_{(\alpha_1,\dots,\alpha_n)} X_1^{\alpha_1} \cdots X_n^{\alpha_n} \tag{39}$$

where $a_{(\alpha_1,\dots,\alpha_n)} \in R$ and where $a_{(\alpha_1,\dots,\alpha_n)} = 0$ for all but finitely many $(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. We call the elements in (39) **polynomials**. The elements $a_{(\alpha_1,\dots,\alpha_n)}$ in R are called **coefficients**. A **monomial** is a polynomial of the form $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. To simplify our notation, we usually denote a polynomial $R[X_1, \dots, X_n]$ by

$$\sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}} = \sum_{(\alpha_1,\dots,\alpha_n)\in\mathbb{Z}^n_{\geq 0}} a_{(\alpha_1,\dots,\alpha_n)} X_1^{\alpha_1} \cdots X_n^{\alpha_n},$$

where it is understood that bold greek letters like $\boldsymbol{\alpha}$ denote a vector in $\mathbb{Z}^n_{\geq 0}$. Addition in $R[X_1, \dots, X_n]$ is defined by

$$\sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}} + \sum_{\boldsymbol{\beta}} b_{\boldsymbol{\beta}} X^{\boldsymbol{\beta}} = \sum_{\boldsymbol{\gamma}} (a_{\boldsymbol{\gamma}} + b_{\boldsymbol{\gamma}}) X^{\boldsymbol{\gamma}}.$$

Multiplication in $R[X_1, \dots, X_n]$ is defined by

$$\sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta}} b_{\boldsymbol{\beta}} X^{\boldsymbol{\beta}} = \sum_{\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{\alpha}+\boldsymbol{\beta}=\boldsymbol{\gamma}} a_{\boldsymbol{\alpha}} b_{\boldsymbol{\beta}} \right) X^{\boldsymbol{\gamma}}.$$

One should check that addition and multiplication defined in this way really does turn $R[X_1, \dots, X_n]$ into a ring.

For instance, associativity of multiplication holds in $R[X_1, \dots, X_n]$ because it holds in R:

$$\begin{aligned}
\left(\sum_\alpha a_\alpha X^\alpha \sum_\beta b_\beta X^\beta\right) \sum_\gamma c_\gamma X^\gamma &= \sum_\delta \left(\sum_{\alpha+\beta=\delta} a_\alpha b_\beta\right) X^\delta \sum_\gamma c_\gamma X^\gamma \\
&= \sum_\kappa \left(\sum_{\delta+\gamma=\kappa} \left(\sum_{\alpha+\beta=\delta} a_\alpha b_\beta\right) c_\gamma\right) X^\kappa \\
&= \sum_\kappa \left(\sum_{\alpha+\beta+\gamma=\kappa} (a_\alpha b_\beta) c_\gamma\right) X^\kappa \\
&= \sum_\kappa \left(\sum_{\alpha+\beta+\gamma=\kappa} \sum_\gamma a_\alpha (b_\beta c_\gamma)\right) X^\kappa \\
&= \sum_\kappa \left(\sum_{\alpha+\beta+\gamma=\kappa} a_\alpha (b_\beta c_\gamma)\right) X^\kappa \\
&= \sum_\kappa \left(\sum_{\alpha+\delta=\kappa} a_\alpha \sum_{\beta+\gamma=\delta} b_\beta c_\gamma\right) X^\kappa \\
&= \sum_\alpha a_\alpha X^\alpha \sum_\delta \left(\sum_{\beta+\gamma=\delta} b_\beta c_\gamma\right) X^\delta \\
&= \sum_\alpha a_\alpha X^\alpha \left(\sum_\beta b_\beta X^\beta \sum_\gamma c_\gamma X^\gamma\right)
\end{aligned}$$

Example 11.1. Here are two polynimals in $\mathbb{Z}[X, Y]$:

$$f(X,Y) = 3X^2Y + 2Y \quad \text{and} \quad g(X,Y) = X^2Y - Y^2.$$

Let's add and multiply these two polynomials together. We get

$$\begin{aligned}
(f+g)(X,Y) &:= f(X,Y) + g(X,Y) \\
&= 3X^2Y + 2Y + X^2Y - Y^2 \\
&= 4X^2Y + 2Y - Y^2.
\end{aligned}$$

Next, let's multiply them together. We get

$$\begin{aligned}
(f \cdot g)(X,Y) &:= f(X,Y)g(X,Y) \\
&= (3X^2Y + 2Y)(X^2Y - Y^2) \\
&= 3X^4Y^2 - 3X^2Y^3 + 2X^2Y^2 - 2Y^3.
\end{aligned}$$

To get a better understanding of polynomial rings, we first study polynomials rings in one variable, namely $R[X]$.

11.0.1 Polynomial Ring over a Domain is a Domain

Proposition 11.1. *Let R be an integral domain. Then the polynomial ring $R[X]$ is an integral domain.*

Proof. Let $f, g \in R[X]$ such that $fg = 0$. Write them as $f = \sum a_k X^k$ and $g = \sum b_m X^m$ where $a_k, b_m \in R$ for all $k, m \geq 0$ and $a_k = 0 = b_m$ for $k, m \gg 0$. Then the polynomial identity $fg = 0$ gives us the equations

$$\sum_{k=0}^{n} a_k b_{n-k} = 0 \tag{40}$$

for all $n \geq 0$. If both $a_0 = 0$ and $b_0 = 0$, then we can write $f = X\widetilde{f}$ and $g = X\widetilde{g}$ where $\widetilde{f}, \widetilde{g} \in R[X]$. In this case,

$$\begin{aligned}
0 &= fg \\
&= X\widetilde{f}X\widetilde{g} \\
&= X^2\widetilde{f}\widetilde{g}
\end{aligned}$$

implies $\widetilde{f}\widetilde{g} = 0$. Thus by replacing f and g with $\widetilde{f}$ and $\widetilde{g}$ if necessary, we may assume that one of a_0 or b_0 is nonzero. Without loss of generality, assume that $b_0 \neq 0$.

We claim that $a_n = 0$ for all n (which implies $f = 0$). Indeed, we will prove this by induction on n. For the base case $n = 0$, the polynomial identity (40) in the $n = 0$ case gives us $a_0 b_0 = 0$. Since $b_0 \neq 0$ and R is an integral domain, we must have $a_0 = 0$. Now suppose we have shown $a_k = 0$ for all $0 \leq k < n$ for some $n \in \mathbb{N}$. Then the polynomial identity (40) together with the induction assumption implies

$$\begin{aligned} 0 &= \sum_{k=0}^{n} a_k b_{n-k} \\ &= a_n b_0. \end{aligned}$$

Again since $b_0 \neq 0$ and R is a domain, we must have $a_n = 0$. Thus we have $a_n = 0$ for all n by induction. Therefore $f = 0$, and hence $R[X]$ is a domain. □

11.0.2 Characterizing units in a polynomial ring in one variable with over a commutative ring

In this subsection, we wish to characterize the units in $R[X]$ where R is an abritrary commutative ring.

Proposition 11.2. *Let $f(X) \in R[X]$ and it express it as*

$$f(X) = a_m X^m + \cdots + a_1 X + a_0$$

where $a_0, a_1, \ldots, a_m \in R$. Then f is a unit in $R[X]$ if and only if a_0 is a unit in R and a_i is nilpotent for all $1 \leq i \leq m$.

Before proving this proposition, let us state and prove the following lemma:

Lemma 11.1. *Let R be a commutative ring and let $\mathrm{N}(R)$ be the set of all nilpotent elements of R. Then*

$$\mathrm{N}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}.$$

Proof. Clearly we have

$$\mathrm{N}(R) \subseteq \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}.$$

Assume for a contradiction that we do not have the reverse inclusion. Thus there exists $x \in R$ such that $x \in \mathfrak{p}$ for all primes $\mathfrak{p}$ of R and such that the set $\{x^n \mid n \in \mathbb{N}\}$ is multiplicative. Let R_x be the ring obtained by localizing R at $\{x^n \mid n \in \mathbb{N}\}$. Recall that the primes of R_x are in one-to-one correspondence with the primes of R which are disjoint from $\{x^n \mid n \in \mathbb{N}\}$. Every commutative ring has at least one prime ideal (this follows from a standard Zorn's Lemma argument). In particular,

$$\{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap \{x^n \mid n \in \mathbb{N}\} = \emptyset\} \cong \operatorname{Spec} R_x \neq \emptyset.$$

Thus there exists a prime ideal $\mathfrak{p}$ of R such that $x \notin \mathfrak{p}$ which is a contradiction. □

Proof. (proof of Proposition (11.2)). First suppose a_0 is a unit in R and a_i is nilpotent for all $1 \leq i \leq m$. Then each $a_i X^i$ is also nilpotent, and since the sum of two nilpotent elements is nilpotent, we see that $\sum_{i=1}^m a_i X^i$ is nilpotent. Also since a_0 is a unit in R, it is also a unit in $R[X]$. So f is the sum of a unit plus a nilpotent element. This implies f is a unit since the sum of a unit plus a nilpotent element is always a unit (if u is a unit with $uv = 1$, and ε is a nilpotent element with $\varepsilon^m = 0$, then $(u + \varepsilon)\sum_{i=1}^m v^i \varepsilon^{i-1} = 1$). This establishes one direction.

For the reverse direction, suppose f is a unit in $R[X]$. We consider two steps:

Step 1: Assume that R is a domain. In this case, we want to show that a_0 is a unit in R and $a_i = 0$ for all $1 \leq i \leq m$. To see this, first we assume for a contradiction that $a_i \neq 0$ for some $1 \leq i \leq m$. By relabeling if necessary, we may in fact that assume $a_m \neq 0$ where a_m is the lead coefficient of f. Now let $g(X) \in R[X]$ such that $fg = 1$ and it express it as

$$g(X) = b_n X^n + \cdots + b_1 X + b_0$$

where $b_0, b_1, \ldots, b_n \in R$ and $b_n \neq 0$. Then the lead term of fg is just $a_m b_n X^{m+n}$ since $a_m \neq 0$ and $b_n \neq 0$ and R is a domain. This is a contradiction since $fg = 1$ and $m + n \geq 1$. Thus we must have $a_i = 0$ for all $1 \leq i \leq m$. By the same proof, we must also have $b_j = 0$ for all $1 \leq j \leq n$. Thus $f(X) = a_0$ and $g(X) = b_0$, and $fg = 1$ implies $a_0 b_0 = 1$ which implies a_0 is a unit.

Step 2: Now we consider the more general case where R may not be a domain. First, to see why a_0 is a unit, note that a_0 is in the image of the unit f under the evaluation map $\mathrm{e}_0 \colon R[X] \to R$, where e_0 is defined by $\mathrm{e}_0(h) = h(0)$

for all $h \in R[X]$. Thus $a_0 = \mathrm{e}_0(f)$ is a unit since f is a unit and e_0 is a ring homomorphism (which preserves the identity element). Next, to see why a_i is nilpotent for all $1 \leq i \leq m$, first note that for any prime ideal $\mathfrak{p}$ of R, the quotient $R/\mathfrak{p}$ is a domain. Since f is a unit in $R[X]$, its image $\overline{f}$ is a unit in $(R/\mathfrak{p})[X]$. Since $\overline{f}$ is obtained from f by reducing coefficients modulo $\mathfrak{p}$, we see from step 1 above that $a_i \in \mathfrak{p}$ for all $1 \leq i \leq m$. Since $\mathfrak{p}$ was arbitrary, we see that

$$a_i \in \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p} = \mathrm{N}(R)$$

for all $1 \leq i \leq m$. $\square$

11.0.3 Characterizing units in a power series ring in one variable over a commutative ring

We now wish to characterize the units of $R((x))$ in the case where R has no non-trivial idempotents. Let $f, g \in R((x))$ such that $fg = 1$ and express them as

$$f = \sum_{i=m}^{\infty} a_i x^i \quad \text{and} \quad g = \sum_{j=n}^{\infty} b_j x^j$$

where $m, n \in \mathbb{Z}$ and $a_i, b_j \in R$. Since

$$1 = \sum_{i+j=0} a_i b_j,$$

we see that at least some a_i must not be a nilpotent (otherwise 1 would be a nilpotent which is a contradiction). By replacing g with $x^k g$ for an appropriate k if necessary, we may assume that $m = 0$ and a_0 is not a nilpotent. Setting $a = a_0$ and $b = b_n$ to simplify notation, we can show that $a^{(n+1)} b = a^n$ for all large n. This implies b and ab aren't nilpotent either (take powers on both sides) and that $(ab)^k$ is idempotent for some large k. Since 1 is the only non-trivial idempotent, this implies $(ab)^k = 1$ which implies a is a unit.

11.1 Gauss' Lemma

Theorem 11.2. *(Gauss' Lemma) Let R be a UFD with fraction field K. If $f \in R[X]$ has positive degree and f is reducible in $K[X]$, then $f = gh$ with $g, h \in R[X]$ having positive degree.*

Proof. If $f = c \cdot \widetilde{f}$ for some nonzero $c \in R$ and some $\widetilde{f} \in R[X]$, it suffices to treat $\widetilde{f}$ instead of f. Thus, by factoring out the greatest common divisor of the coefficients of f (which makes sense since the coefficient ring R is a UFD), we may assume that the coefficients of f have gcd equal to 1. We call such polynomials **primitive**.

The key fact that we need is that a product of primitives is a primitive. To prove it, let $g, h \in R[X]$ be such that $gh \in R[X]$ is not primitive. We wish to prove that one of g or h is not primitive. The non-primitivity of gh implies that some nonzero non-unit $c \in R$ divides all coefficients of gh. If π is an irreducible factor of c then π divides all coefficients of gh.

Let $\overline{R} = R/(\pi)$, a domain since π is irreducible and R is a UFD. Working in $\overline{R}[X]$, we have $\overline{g}\overline{h} = \overline{gh} = 0$. But a polynomial ring over a domain is again a domain, so one of $\overline{g}$ or $\overline{h}$ vanishes. This says that π divides all coefficients of g or h, so one of these is non-primitive, as desired.

Say our given non-trivial factorization is $f = gh$ with $g, h \in K[X]$ having positive degree. If we write the coefficients of g as reduced form fractions with a "least common denominator" and then consider the gcd of the numerators, we can write $g = qg_0$ where $q \in K^\times$ and $g_0 \in R[X]$ is primitive. Likewise, $h = q'h_0$ where $q' \in K^\times$ and $h_0 \in R[X]$ is primitive. Hence, $f = (qq')g_0h_0$ with f and g_0h_0 both primitive. Writing $qq' = a/b$ as a reduced-form fraction with a, b in the UFD R, we have $bf = ag_0h_0$ in $R[X]$. Comparing gcd's of coefficients on both sides, it follows that $a = bu$ with $u \in R^\times$, so $qq' = u \in R^\times$. Hence, $f = (ug_0)(h_0)$ is a factorization of f in $R[X]$ with ug_0 and h_0 having positive degree. $\square$

Lemma 11.3. *(Gauss Lemma) Let R be a UFD and let F be its field of fractions. Let $f(x) \in R[x]$. If $f(x)$ is reducible in $F[x]$, then $f(x)$ is reducible in $R[x]$.*

Proof. Write $f(x) = A(x)B(x)$ with $A(x), B(x) \in F[x]$ such that $\deg(A(x)), \deg(B(x)) \geq 1$. There is some $d \in R$ such that $df(x) = a'(x)b'(x)$ with $a'(x), b'(x) \in R[x]$. Since R is a UFD, we have $d = p_1p_2 \cdots p_n$ with p_i being irreducible. Now since p_1 is prime in R, p_1 is prime in $R[x]$ too. Then

$$p_1p_2 \cdots p_m f(x) = a'(x)b'(x) \qquad \text{in } R[x]$$

and $p_1 \mid a'(x)b'(x)$ together with p_1 being a prime implies p_1 divides one of $a'(x)$ or $b'(x)$. Say p_1 divides $a'(x)$. So $a'(x) = p_1a''(x)$ with $a''(x) \in R[x]$. So

$$p_1p_2 \cdots p_n f(x) = p_1 a''(x)b'(x).$$

And since we are in an integral domain, we can cancel p_1 on both sides. The proceeding inductively, we find that $f(x)$ is reducible in $R[x]$.

$\square$

11.2 Polynomial Rings that are UFDs

Recall that $f(x) \in F[x]$ is irreducible when $f(x) = g(x)h(x)$ implies either $g(x)$ is a unit or $h(x)$ is a unit. Another way to think of this is that $f(x)$ is reducible if it factors as $f(x) = g(x)h(x)$ where $1 \leq \deg(g(x)) < \deg(f(x))$ and $1 \leq \deg(h(x)) < \deg(f(x))$.

Let R be a ring. We want to show that $R[x]$ is a UFD if and only if R is a UFD. To show this, we need Gauss' Lemma:

Lemma 11.4. *(Gauss Lemma) Let R be a UFD and let F be its field of fractions. Let $f(x) \in R[x]$. If $f(x)$ is reducible in $F[x]$, then $f(x)$ is reducible in $R[x]$.*

Proof. Write $f(x) = A(x)B(x)$ with $A(x), B(x) \in F[x]$ such that $\deg(A(x)), \deg(B(x)) \geq 1$. There is some $d \in R$ such that $df(x) = a'(x)b'(x)$ with $a'(x), b'(x) \in R[x]$. Since R is a UFD, we have $d = p_1p_2\cdots p_n$ with p_i being irreducible. Now since p_1 is prime in R, p_1 is prime in $R[x]$ too. Then

$$p_1p_2\cdots p_m f(x) = a'(x)b'(x) \qquad \text{in } R[x]$$

and $p_1 \mid a'(x)b'(x)$ together with p_1 being a prime implies p_1 divides one of $a'(x)$ or $b'(x)$. Say p_1 divides $a'(x)$. So $a'(x) = p_1a''(x)$ with $a''(x) \in R[x]$. So

$$p_1p_2\cdots p_n f(x) = p_1a''(x)b'(x).$$

And since we are in an integral domain, we can cancel p_1 on both sides. The proceeding inductively, we find that $f(x)$ is reducible in $R[x]$.

□

Corollary 13. *Let R be a UFD and let F be its field of fractions. Let $f(x) \in R[x]$ be such that the gcd of the coefficients of $f(x)$ is 1. Then $f(x)$ is irreducible in $R[x]$ if and only if $f(x)$ is irreducible in $F[x]$.*

Proof. ($\Longrightarrow$) Assume that $f(x)$ is reducible in $F[x]$. Then by Gauss' Lemma, $f(x)$ is reducible in $R[x]$, which is a contradiction. ($\Longleftarrow$) Assume that $f(x)$ is reducible in $R[x]$. Then $f(x) = a(x)b(x)$ with $a(x), b(x) \in R[x] \subset F[x]$. Since $f(x)$ is irreducible in $F[x]$, one of the factors, say $a(x)$, has to a constant; $a(x) = r \in R$. So $f(x) = rb(x)$ with $r \in R$. This implies r divides all of the coefficients of $f(x)$, which implies r is a unit. □

Theorem 11.5. *$R[x]$ is a UFD if and only if R is a UFD.*

Proof. ($\Longleftarrow$) Let $f(x)$ be a nonzero nonunit element in $f(x)$. Let d be the gcd of the coefficients of $f(x)$. Then $f(x) = dp(x)$ with $p(x) \in R[x]$ and such that the gcd of the coefficients of $p(x)$ is 1. Since R is a UFD, $d = q_1q_2\cdots q_t$ with q_i prime in R, so they are also prime in $R[x]$. So it suffices to show that $p(x)$ is a finite product of irreducibles in $R[x]$. Since $p(x) \in F[x]$ and $F[x]$ is a UFD, we have $p(x) = p_1'(x)\cdots p_n'(x)$ with $p_i'(x)$ irreducible in $F[x]$. By Gauss' Lemma, we obtain $p(x) = p_1(x)\cdots p_n(x)$ where $p_i(x) = a_ip_i'(x)$. Since $p_i'(x)$ is irreducible in $F[x]$ and a_i is a unit in $F[x]$, we have $p_i(x)$ is irreducible in $F[x]$. Since $p_i(x) \mid p(x)$, the gcd of the coefficients of $p_i(x)$ is 1, so $p_i(x)$ is irreducible in $R[x]$.

We need to show uniqueness. Assume $p(x)$ in $R[x]$ be such that the gcd of all coefficients of $f(x)$ is 1. If $p(x) = p_1(x)\cdots p_n(x) = \ell_1(x)\cdots\ell_s(x)$ are two factorizations into irreducibles in $R[x] \subseteq F[x]$. Then $n = s$ and $p_i(x) \sim \ell_i(x)$ since $F[x]$ is a UFD. So $b_ip_i(x) = a_i\ell_i(x)$ where $a_i, b_i \in R$ with $b_i \neq 0$. So gcd of LHS is the same as the gcd of the RHS which implies $a_i = b_i$. Thus $p_i(x) \sim \ell_i(x)$ in $R[x]$.

($\Longrightarrow$) Let r be a nonzero nonunit element in R. Then $r \in R[x]$ implies $r = p_1(x)\cdots p_n(x)$ with $p_i(x)$ be irreducible in $R[x]$. But the the degree on the left side must be equal to the degree of the right hand side. This implies $\deg(p_i(x)) = 0$, so $p_i(x) = p_i \in R$, and p_i is irreducible in R. Uniqueness holds because $R[x]$ is a UFD and R is a subring of $R[x]$.

□

11.3 Irreducibility Criteria

Proposition 11.3. *Let F be a field and let $f(x) \in F[x]$. Then $f(x)$ has a factor of degree 1 if and only if $f(x)$ has a root in F, i.e. there is some $\alpha \in F$ such that $f(\alpha) = 0$.*

Proof. ($\Longrightarrow$) $f(x) = (ax+b)g(x)$ with $a, b \in F$, $a \neq 0$, and $g(x) \in F[x]$. Let $\alpha = -ab^{-1} \in F$. Then $f(\alpha) = 0$. ($\Longleftarrow$) Let $\alpha \in F$ such that $f(\alpha) = 0$. Then we have

$$f(x) = (x-\alpha)g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < 1$. Suppose $r(x) \neq 0$. Then $r(x) = r \in F$ is a constant. And this is a contradiciton since

$$\begin{aligned} f(\alpha) &= (\alpha - \alpha)g(\alpha) + r(\alpha) \\ &= r, \end{aligned}$$

so $f(x) = (x-\alpha)g(x)$. □

Proposition 11.4. *Let F be a field and let $f(x) \in F[x]$ be a polynomial of degree 2 or 3. Then $f(x)$ is reducible if and only if $f(x)$ has a root in F.*

Proof. ($\Longleftarrow$) If $f(x)$ has a root $\alpha \in F$, then $f(x) = (x-\alpha)g(x)$ where $g(x) \in F[x]$. ($\Longrightarrow$) If $f(x)$ is reducible, then $f(x) = g(x)h(x)$ where $g(x), h(x) \in F[x]$. Then

$$\deg g(x) + \deg h(x) = \deg f(x) \leq 3$$

implies either $g(x)$ or $h(x)$ has degree 1. By Proposition (11.3), $f(x)$ must have a root in F. $\square$

Proposition 11.5. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If $r/s \in \mathbb{Q}$ is a root of $f(x)$, and $\gcd(r,s) = 1$, then $r \mid a_0$ and $s \mid a_n$.*

Proof. Since r/s is a root of $f(x)$, we have

$$\begin{aligned} 0 &= f\left(\frac{r}{s}\right) \\ &= a_n \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 \\ &= \frac{a_n r^n + a_{n-1}sr^{n-1} + \cdots + a_1 s^{n-1} r + a_0 s^n}{s^n}. \end{aligned}$$

This implies

$$r(a_n r^{n-1} + a_{n-1}sr^{n-2} + \cdots + a_1 s^{n-1}) = -a_0 s^n.$$

Therefore $r \mid a_0 s^n$, and since r and s are relatively prime, $r \mid a_0$. Similarly,

$$s(a_{n-1}r^{n-1} + \cdots + a_1 s^{n-2} r + a_0 s^{n-1}) = -a_n r^n.$$

So $s \mid a_n$ by the same reasoning as above. $\square$

Example 11.2. Let $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}[x]$. Show that $f(x)$ is irreducible in $\mathbb{Z}[x]$. By Gauss' Lemma, $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if $f(x)$ is irreducible in $\mathbb{Q}[x]$. Suppose $f(x)$ is reducible in $\mathbb{Q}[x]$. By Proposition (11.4), $f(x)$ has a root $r/s \in \mathbb{Q}$. By Proposition (11.5), $s \mid 1$ and $r \mid 1$. This implies $r/s = \pm 1$. However $f(\pm 1) \neq 0$, which is a contradiction.

Example 11.3. Let p be a prime. We show $x^3 - p \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$. Using the same reasoning as in the Example (11.2), the only possible roots of $x^3 - p$ are $\pm p$ and ± 1, however none of these are roots.

11.4 Eisenstein's Criterion

Let R be an integral domain with fraction field K and let $\mathfrak{p}$ be a prime ideal of R. Let $f(T)$ be a monic polynomial in $\mathbb{Z}[T]$ expressed as

$$f = T^n + c_{n-1}T^{n-1} + \cdots + c_1 T + c_0.$$

where $c_0, \dots, c_{n-1} \in R$. We say f is **$\mathfrak{p}$-Eisenstein** if $c_i \in \mathfrak{p}$ for all $0 \leq i \leq n-1$ and $c_i \notin \mathfrak{p}^2$.

Theorem 11.6. *f is irreducible in $R[T]$.*

Proof. Assume for a contradiction that f is reducible, say $f = gh$, where

$$g = \sum_{k \geq 0} a_k T^k \quad \text{and} \quad h = \sum_{l \geq 0} b_l T^l$$

where $a_k, b_l \in R$ and $a_k = 0$ for $k \gg 0$ and $b_l = 0$ for $l \gg 0$. The polynomial identity $f = gh$ gives us the system of $n+1$ equations

$$\sum_{k=0}^{m} a_k b_{m-k} = c_m \tag{41}$$

for all $0 \leq m \leq n$. In the case where $m = 0$, we have $a_0 b_0 = c_0$. Since $c_0 \in \mathfrak{p}\backslash\mathfrak{p}^2$, we must have either $a_0 \in \mathfrak{p}$ or $b_0 \in \mathfrak{p}$, but not both! Without loss of generality, say $a_0 \in \mathfrak{p}$ and $b_0 \notin \mathfrak{p}$. We claim that $a_k \in \mathfrak{p}$ for all k. Indeed, we will prove this by induction on m where $0 \leq m < n$. The base case $m = 0$ is by assumption. Suppose that we have shown $a_k \in \mathfrak{p}$ for all $k \leq m$ for some $0 \leq m < n$. Then the identity (41) in the $m+1$ case implies

$$\begin{aligned} 0 &\equiv c_{m+1} \bmod \mathfrak{p} \\ &\equiv \sum_{k=0}^{m+1} a_k b_{m-k} \bmod \mathfrak{p} \\ &\equiv a_{m+1} b_0 \bmod \mathfrak{p}. \end{aligned}$$

Thus $a_{m+1}b_0 \in \mathfrak{p}$. Since $b_0 \notin \mathfrak{p}$, we must have $a_{m+1} \in \mathfrak{p}$. Thus by induction, we have $a_k \in \mathfrak{p}$ for all k. But this contradicts the fact that f is monic! Indeed, the identity (41) in the n case together with the fact that $a_k \in \mathfrak{p}$ for all k implies $c_n \in \mathfrak{p}$. However $c_n = 1$, and $1 \notin \mathfrak{p}$. Contradiction. □

Example 11.4. Let $f(x) = x^5 - 30x^4 + 9x^3 - 6x + 3$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein's Criterion for $p = 3$.

Example 11.5. Let $f(x) = x^4 + 1$. Then $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible. Since $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ is Eisenstein at 2, $f(x+1)$ is irreducible, and so $f(x)$ is irreducible.

11.4.1 Goldbach Conjecture for $\mathbb{Z}[X]$

It turns out that we can use Eisenstein's Criterion to prove Goldbach's conjecture for $\mathbb{Z}[X]$. The following proposition and proof were

Proposition 11.6. *Every polynomial in $\mathbb{Z}[X]$ is the sum of two irreducible polynomials in $\mathbb{Z}[X]$.*

Proof. Let $f(X)$ be any polynomial in $\mathbb{Z}[X]$ and write it as

$$f(X) = \sum_{k=0}^{n} a_k X^k$$

where $a_k \in \mathbb{Z}$ for all $0 \leq k \leq n$. Choose any two distinct odd primes, say p and q. Since $\gcd(p,q) = 1$, there exists $u_k, v_k \in \mathbb{Z}$ such that

$$a_k = u_k p + v_k q$$

for all $0 \leq k \leq n$. Now let $r \in \mathbb{Z}$ and let

$$g(X) = (u_0 + rq)p + \sum_{k=1}^{n} u_k p X^k + X^{n+1} \quad \text{and} \quad h(X) = (v_0 - rp)q + \sum_{k=1}^{n} v_k q X^k - X^{n+1}.$$

Clearly we have $f = g + h$. Also g and h almost satisfy Eisenstein's irreducibility criterion: all coefficients except the leading term are divisible by p (resp. q). However, we want to ensure that the constant term is not divisible by p^2 (resp. q^2). In other words, we need

$$p \nmid u_0 + rq \quad \text{and} \quad q \nmid v_0 - rp. \tag{42}$$

This can easily be acheived: as most one of the numbers $u_0 - q, u_0, u_0 + q$ is a multiple of p because the gcd of two of them divides $2q$ and at most one of $v_0 + p, v_0, v_0 - p$ is a multiple of q. Hence at least one of the choices $r \in \{-1, 0, 1\}$ leads to (42). With this choice, g and h are irreducible per Einstein. □

12 Noetherian Rings

Proposition 12.1. *Let R be a commutative ring. The following conditions are equivalent:*

1. *Every ascending chain of ideals in R stabilizes: if (I_n) is ascending chain of ideals in R, meaning $I_n \subseteq I_{n+1}$ for all $n \in \mathbb{N}$, then there exists $N \in \mathbb{N}$ such that $I_N = I_n$ for all $n \geq N$.*
2. *Every ideal of R is finitely generated.*

Proof. Suppose every chain of ideal in R stabilizes and let I be an ideal in R. Assume for a contradiction that I is not finitely generated. Choose any $x_1 \in I$. Since I is not finitely generated, we have

$$\langle x_1 \rangle \subset I$$

where the inclusion is proper. Next we choose $x_2 \in I \backslash \langle x_1 \rangle$. Again, since I is not finitely generated, we have

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset I$$

where each inclusion is proper. Proceeding inductively on $n \geq 3$, we choose $x_n \in I \backslash \langle x_1, \ldots, x_{n-1} \rangle$. Then since I is not finitely generated, we have

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots \subset \langle x_1, x_2, \ldots, x_n \rangle \subset I$$

where each inclusion is proper. Continuing in this manner, we construct an ascending chain of ideals

$$(\langle x_1, x_2 \ldots, x_n \rangle)_{n \in \mathbb{N}}$$

which never stabilizes since $\langle x_1, x_2, \dots, x_n \rangle$ is properly contained in $\langle x_1, x_2, \dots, x_n, x_{n+1} \rangle$ for all $n \in \mathbb{N}$. This contradicts the hypothesis that every chain of ideal in R stabilizes. Thus every ideal in R is finitely generated.

Now let us show the converse. Suppose every ideal in R is finitely generated. Let (I_n) be an ascending chain of ideals. Then $\bigcup_{n=1}^{\infty} I_n$ is an ideal in R since (I_n) is totally ordered, thus it must be finitely generated, say

$$\bigcup_{n=1}^{\infty} I_n = \langle x_1, \dots, x_m \rangle.$$

Observe that $x_i \in I_{n_i}$ for some $n_i \in \mathbb{N}$ for each $1 \leq i \leq m$. Set $N = \max_{1 \leq i \leq m}\{n_i\}$. Then $x_i \in I_N$ for each $1 \leq i \leq m$ since (I_n) is totally ordered. It follows that for any $n \geq N$, we have

$$\begin{aligned} I_N &\subseteq I_n \\ &\subseteq \bigcup_{n=1}^{\infty} I_n \\ &= \langle x_1, \dots, x_m \rangle \\ &\subseteq I_N. \end{aligned}$$

In particular we have $I_N = I_n$ for all $n \geq N$. Thus every chain of ideals in R stabilizes. □

Definition 12.1. If R satisfies any of the equivalent definitions in (12.1), then we say R is **Noetherian**.

12.0.1 Hilbert Basis Theorem

Theorem 12.1. *Let R be a Noetherian ring. Then $R[X]$ is a Noetherian ring.*

Proof. Let I be an ideal in $R[X]$. For each $n \in \mathbb{N}$, we denote $I_n = \{f \in I \mid \deg f = n\}$ and we define

$$\mathfrak{a}_n = \{a_n \in R \mid a_n = \mathrm{LT}(f) \text{ for some } f \in I_n\} \cup \{0\}.$$

Thus $a_n \in \mathfrak{a}_n \backslash \{0\}$ if there exists a polynomial $f \in I$ of degree n whose lead term in a_n. Observe that $\mathfrak{a}_n$ is an ideal. Indeed, if $a_n, b_n \in \mathfrak{a}_n$ and $a, b \in R$, then if we choose $f, g \in I_n$ such that $a_n = \mathrm{LT}(f)$ and $b_n = \mathrm{LT}(g)$, then we see that either $aa_n + bb_n = 0$ or

$$aa_n + bb_n = \mathrm{LT}(af + bg),$$

which implies $aa_n + bb_n \in \mathfrak{a}_n$. Also note that the sequence of ideals $(\mathfrak{a}_n)$ is ascending. This is because if $a_n \in \mathfrak{a}_n$ with $a_n = \mathrm{LT}(f)$ for some $f \in I_n$, then $a_n = \mathrm{LT}(xf)$ where $xf \in I_{n+1}$, so $a_n \in \mathfrak{a}_{n+1}$. Since R is Noetherian, the ascending chain $(\mathfrak{a}_n)$ of ideals must stabilize, say $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geq N$ for some $N \in \mathbb{N}$. Also since R is Noetherian, $\mathfrak{a}_N$ must be finitely generated, say

$$\mathfrak{a}_N = \langle a_{N,1}, a_{N,2}, \dots, a_{N,s} \rangle.$$

Choose $f_1, \dots, f_s \in I_N$ such that $\mathrm{LT}(f_r) = a_{N,r}$ for all $1 \leq r \leq s$. We claim that

$$I = \langle 1, x, , \dots, x^N, f_1, \dots, f_s \rangle.$$

To see this, let $g \in I$. We will prove that g can be expressed as an R-linear combination of $1, x, \dots, x^N, f_1, \dots, f_s$ using induction on $\deg g$. Clearly if $\deg g \leq N$, then g can be expressed as an R-linear combination of $1, x, \dots, x^N$. This establishes the base case. Now denote $n = \deg g$ and assume that $n > N$ and that we can express polynomials $h \in I$ of degree $< n$ as an R-linear combination of $1, x, \dots, x^N, f_1, \dots, f_s$. Write

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0.$$

Since $a_n \in \mathfrak{a}_n = \mathfrak{a}_N$, we can express it as

$$a_n = c_1 a_{N,1} + c_2 a_{N,2} + \cdots + c_s a_{N,s}$$

for some $c_1, c_2, \dots, c_s \in R$. Now we set

$$h = g - c_1 f_1 - c_2 f_2 - \cdots - c_s f_s.$$

Then note that $h \in I$ and $\deg h < n$. By the induction hypothesis, it follows that $h \in \langle 1, x, , \dots, x^N, f_1, \dots, f_s \rangle$. However this also implies $g \in \langle 1, x, , \dots, x^N, f_1, \dots, f_s \rangle$. □

12.1 Krull's principal ideal theorem

This subsection is based on and inspired by Melvon Hochster's notes from [Hoc3]. We now wish to study dimension theory in Noetherian rings.

Definition 12.2. Let $\mathfrak{q}$ be a prime ideal of R. The n**th symbolic power of** $\mathfrak{q}$, denoted $\mathfrak{q}^{(n)}$, is defined to be the ideal

$$\mathfrak{q}^{(n)} = \mathfrak{q}^n R_{\mathfrak{q}} \cap R = \{a \in R \mid as \in \mathfrak{q}^n \text{ for some } s \in R \backslash \mathfrak{q}\}.$$

Lemma 12.2. *Let $\mathfrak{q}$ be a prime ideal of R. Then $\mathfrak{q}^{(n)}$ is the smallest $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$.*

Proof. It is clear that $\mathfrak{q}^n \subseteq \mathfrak{q}^{(n)}$. Let us show that $\mathfrak{q}^{(n)}$ is a $\mathfrak{q}$-primary ideal. Suppose $ab \in \mathfrak{q}^{(n)}$ and $a \notin \mathfrak{q}^{(n)}$. We want to show that some power of b belongs to $\mathfrak{q}^{(n)}$. Choose $s \in R\backslash\mathfrak{q}$ such that $abs \in \mathfrak{q}^n$. Since $a \notin \mathfrak{q}^{(n)}$, we must have $bs \notin R\backslash\mathfrak{q}$, so $bs \in \mathfrak{q}$, and since $s \notin \mathfrak{q}$, this implies $b \in \mathfrak{q}$ since $\mathfrak{q}$ is a prime ideal. But then this implies $b^n \in \mathfrak{q}^n \subseteq \mathfrak{q}^{(n)}$. It follows that $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary.

Now we will show that $\mathfrak{q}^{(n)}$ is the smallest $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$. Let Q be any $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$ and let $a \in \mathfrak{q}^{(n)}$. Choose $s \in R\backslash\mathfrak{q}$ such that $as \in \mathfrak{q}^n \subseteq Q$. Since $s \notin \mathfrak{q}$ and $Q = \sqrt{\mathfrak{q}}$, we see that $s^n \notin Q$ for all $n \in \mathbb{N}$. This implies $a \in Q$ since Q is primary. It follows that $\mathfrak{q}^{(n)} \subseteq Q$. □

Example 12.1. Let $R = \Bbbk[x,y,z]$ and let $\mathfrak{p} = \langle x^3 - yz, y^2 - xz, z^2 - x^2 y\rangle$. Then $\mathfrak{p}^2$ is not $\mathfrak{p}$-primary! Indeed, we have $\operatorname{Ass}(R/\mathfrak{p}^2) = \{\mathfrak{p}, \mathfrak{m}\}$ where $\mathfrak{m} = \langle x,y,z\rangle$. In fact, there are even principal prime ideals with powers not primary. For instance, consider $R = \Bbbk[x,y]/\langle x^2 y\rangle$ and $\mathfrak{p} = \langle \overline{x}\rangle$. Then $\mathfrak{p}$ is a prime ideal, but $\mathfrak{p}^3 = \langle \overline{x}^3\rangle$ is not $\mathfrak{p}$-primary since $\langle \overline{y}\rangle = 0 : \overline{x}^2$ is an associated prime of $R/\mathfrak{p}^3$.

Theorem 12.3. *Let R be a Noetherian ring, let $x \in R$, and let $\mathfrak{p}$ be a minimal prime of $\langle x\rangle$. Then* $\operatorname{height}\mathfrak{p} \leq 1$.

Proof. Assume for a contradiction that there is a chain of primes of length two or more in R, say

$$\mathfrak{p} \supset \mathfrak{p}' \supset \mathfrak{p}''.$$

If we localize R at $\mathfrak{p}$, then we still have a chain of length two or more in $R_{\mathfrak{p}}$, so we may as well assume that $(R,\mathfrak{p})$ is local. If we pass to the quotient $R/\mathfrak{p}''$, we still get a chain of length two in $R/\mathfrak{p}''$, so we may assume that $(R,\mathfrak{p})$ is a local domain, that $\mathfrak{p}$ is a minimal prime of $\langle x\rangle$, and that there is a prime $\mathfrak{q}$ of R such that

$$\mathfrak{p} \supset \mathfrak{q} \supset \langle 0\rangle.$$

From this, we will obtain a contradiction.

The ring R/x has only one prime ideal, namely $\mathfrak{p}/x$. Indeed, this follows from the fact that is $\mathfrak{p}$ is minimal over $\langle x\rangle$ and that $\mathfrak{p}$ is a maximal ideal of R. Therefore R/x is a zero-dimensional local ring, and has DCC. In consequence, the chain of ideals $\langle \mathfrak{q}^{(n)}, x\rangle/x$ is eventually stable. Taking inverse images in R, we find that there exists N such that

$$\mathfrak{q}^{(n)} + \langle x\rangle = \mathfrak{q}^{(n+1)} + \langle x\rangle \tag{43}$$

for all $n \geq N$. In fact, we claim that for $n \geq N$ we must have

$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)} \tag{44}$$

since $\mathfrak{q}^{(n)}$ is primary and since $\mathfrak{p}$ is the only minimal prime of $\langle x\rangle$. To see why this is the case, first note that

$$\mathfrak{q}^{(n)} \supseteq \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)}$$

follows from the fact that $\mathfrak{q}^{(n)} \supseteq \mathfrak{q}^{(n+1)}$ and $\mathfrak{q}^{(n)} \supseteq x\mathfrak{q}^{(n)}$. To show the reverse inclusion, let $a \in \mathfrak{q}^{(n)}$. Then by (43), there exists $b \in R$ and $a' \in \mathfrak{q}^{(n+1)}$ such that $xb = a + a' \in \mathfrak{q}^{(n)}$. But $x^n \notin \mathfrak{q}$ for any $n \in \mathbb{N}$ since $\mathfrak{p}$ is the only minimal prime of $\langle x\rangle$ in R. Since $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary, we must have $b \in \mathfrak{q}^{(n)}$. Since $a = a' + xb$, this leads us to the conclusion that

$$\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)}.$$

Thus we have the equality (44). In particular this implies $M = xM$ where $M = \mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)}$. It follows from Nakayama's lemma that $M = 0$, that is, that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. Thus in $R_{\mathfrak{q}}$ we have

$$\mathfrak{q}_{\mathfrak{q}}^n = (\mathfrak{q}^{(n)})_{\mathfrak{q}} = (\mathfrak{q}^{(n+1)})_{\mathfrak{q}} = \mathfrak{q}_{\mathfrak{q}}^{n+1} = \mathfrak{q}_{\mathfrak{q}}\mathfrak{q}_{\mathfrak{q}}^n,$$

and so by Nakayama's lemma again (this time in $R_{\mathfrak{q}}$) we obtain $\mathfrak{q}_{\mathfrak{q}}^n = 0$, and thus $\mathfrak{q}^n = 0$ (as R is a domain). However this is a contradiction since $\mathfrak{q} \neq 0$ implies $\mathfrak{q}^n \neq 0$. □

Theorem 12.4. *(Prime Avoidance) Let A be a ring. Let $V \subseteq W$ be vector spaces over an infinite field K.*

1. *Let $\mathfrak{U}$ be an ideal of A. Given finitely many ideals of A, all but two of which are prime, if $\mathfrak{U}$ is not contained in any of these ideals, then it is not contained in their union.*

2. *Given finitely many subspaces of W, if V is not contained in any of these subspaces, then V is not contained in their union.*

3. *(Ed Davis) Let $x \in A$ and $I, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be ideals of A, such that $\mathfrak{p}_i$ are prime. If $\langle I, x\rangle$ is not contained in any of the $\mathfrak{p}_i$, then for some $b \in I$, $b + x \notin \bigcup_i \mathfrak{p}_i$.*

Proof.

1. We may assume that no term may be omitted from the union, or work with a smaller family of ideals. Call the ideals $I, J, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ with $\mathfrak{p}_i$ prime. Choose elements $x \in I \cap \mathfrak{U}$, $y \in J \cap \mathfrak{U}$, and $z_i \in \mathfrak{p}_i \cap \mathfrak{U}$, such that each belongs to only one of the ideals $I, J, \mathfrak{p}_1, \ldots \mathfrak{p}_n$, i.e., to the one it is specified in. This must be possible, or not all of the ideals would be needed to cover $\mathfrak{U}$. For instance, if every element $x \in I \cap \mathfrak{U}$ belonged to $J \cap \mathfrak{U}$, then $I \cap \mathfrak{U} \subset J \cap \mathfrak{U}$, and thus
$$(I \cap \mathfrak{U}) \cup (J \cap \mathfrak{U}) \cup (\mathfrak{p}_1 \cap \mathfrak{U}) \cup \cdots \cup (\mathfrak{p}_n \cap \mathfrak{U}) = (J \cap \mathfrak{U}) \cup (\mathfrak{p}_1 \cap \mathfrak{U}) \cup \cdots \cup (\mathfrak{p}_n \cap \mathfrak{U}),$$
and we would simply proceed with the ideals $J, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Let $a = (x + y) + xyb$, where
$$b = \prod_{i \text{ such that } x+y \notin \mathfrak{p}_i} z_i,$$
where a product over the empty set is defined to be 1. Then $x + y$ is not in I nor in J, while xyb is in both, so that $a \notin I$ and $a \notin J$. Now choose i, $1 \leq i \leq n$. If $x + y \in \mathfrak{p}_i$, the factors of xyb are not in $\mathfrak{p}_i$, and so $xyb \notin \mathfrak{p}_i$, and therefore $a \notin \mathfrak{p}_i$. If $x + y \notin \mathfrak{p}_i$ there is a factor of b in $\mathfrak{p}_i$, and so $a \notin \mathfrak{p}_i$ again.

2. If V is not contained in any one of the finitely many vector spaces V_t covering V, for every t choose a vector $v_t \in V \backslash V_t$. Let V_0 be the span of the v_t. Then V_0 is a finite-dimensional counterexample. We replace V by V_0 and V_t by its intersection with V_0. Thus, we need only show that a finite-dimensional vector space K^n is not a finite union of proper subspaces V_t. (When the field is algebraically closed we have a contradiction because K^n is irreducible. Essentially the same idea works over any infinite field). For each t we can choose a linear form $L_t \neq 0$ that vanishes on V_t. The product $f = L_1 \cdots L_t$ is a nonzero polynomial that vanishes identically on K^n. This is a contradiction, since K is infinite.

3. We may assume that no $\mathfrak{p}_t$ may be omitted from the union. For every t, choose an element p_t in $\mathfrak{p}_t$ and not in any of the other $\mathfrak{p}_k$. Suppose, after renumbering, that $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ all contain x while the other $\mathfrak{p}_t$ do not (the values 0 and n for k are allowed). If $I \subseteq \bigcup_{j=1}^k \mathfrak{p}_j$ then it is easy to see that $\langle I, x\rangle \subseteq \bigcup_{j=1}^k \mathfrak{p}_j$, and hence in one of the $\mathfrak{p}_j$ by part (1), a contradiction. Choose $a \in I$ not in any of the $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. Let q be the product of the p_t for $t > k$ (or 1 if $k = n$). Then $x + aq$ is not in any $\mathfrak{p}_t$, and so we may take $b = aq$.

□

Example 12.2. Consider the ring $\mathbb{F}_2[x, y]/\langle x^2, xy, y^2\rangle$. Then $\langle x, y\rangle = \langle x\rangle \cup \langle y\rangle \cup \langle x + y\rangle$, but $\langle x, y\rangle \not\subset \langle x\rangle$, $\langle x, y\rangle \not\subset \langle y\rangle$, and $\langle x, y\rangle \not\subset \langle x + y\rangle$. This shows that we cannot replace "all but two are prime" by "all but three are prime" in part (1) of Theorem (12.4). Also note that $\mathbb{F}_2[x, y]/\langle x^2, xy, y^2\rangle$ is a finite-dimensional $\mathbb{F}_2$-vector space which is the union of the proper subspaces $\langle 1\rangle$ and $\langle x, y\rangle$.

Theorem 12.5. *(Krull's principal ideal theorem, strong version, alias Krulls height theorem) Let A be a Noetherian ring and $\mathfrak{p}$ a minimal prime ideal of an ideal generated by n elements. Then the height of $\mathfrak{p}$ is at most n. Conversely, if $\mathfrak{p}$ has height n, then it is a minimal prime of an ideal generated by n elements. That is, the height of a prime $\mathfrak{p}$ is the same as the least number of generators of an ideal $I \subset \mathfrak{p}$ of which $\mathfrak{p}$ is a minimal prime. In particular, the height of every prime ideal $\mathfrak{p}$ is at most the number of generators of $\mathfrak{p}$, and is therefore finite. For every local ring A, the Krull dimension of A is finite.*

Proof. We begin by proving by induction on n that the first statement holds. If $n = 0$, then $\mathfrak{p}$ is a minimal prime of $\langle 0\rangle$ and this does mean that $\mathfrak{p}$ has height 0. Note that the zero ideal is the ideal generated by the empty set, and so constitutes a 0 generator ideal. The case $n = 1$ has already been proved. Now suppose that $n \geq 2$ and that we know the result for integers $< n$. Suppose that $\mathfrak{p}$ is a minimal prime of $\langle x_1, \ldots, x_n\rangle$ and that we want to show that the height of $\mathfrak{p}$ is at most n. Suppose not, and that there is a chain of primes
$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{n+1} = \mathfrak{p}$$

with strict inclusions. If $x_1 \in \mathfrak{p}_1$, then $\mathfrak{p}$ is evidently also a minimal prime of $\mathfrak{p}_1 + \langle x_2, \ldots, x_n \rangle$ and this implies that $\mathfrak{p}/\mathfrak{p}_1$ is a minimal prime of the ideal generated by the images of $x_2, \ldots, x_n$ in $A/\mathfrak{p}_1$. Then the chain

$$\mathfrak{p}_1/\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{n+1}/\mathfrak{p}_1$$

contradicts the induction hypothesis. Therefore it will suffice to show that the chain

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{n+1} = \mathfrak{p}$$

can be modified so that $x = x_1$ is in $\mathfrak{p}_1$. Suppose that $x \in \mathfrak{p}_k$ but not in $\mathfrak{p}_{k-1}$ for $k \geq 2$. (To get started, note that $x \in \mathfrak{p} = \mathfrak{p}_{n+1}$.) It will suffice to show that there is a prime strictly between $\mathfrak{p}_k$ and $\mathfrak{p}_{k-2}$ that contains x, for then we use this prime instead of $\mathfrak{p}_{k-1}$, and we have increased the number of primes in the chain that contains x. Thus, we eventually reach a chain such that $x \in \mathfrak{p}_1$.

To find such a prime, we may work in the local domain

$$D = A_{\mathfrak{p}_k}/\mathfrak{p}_{k-2}A_{\mathfrak{p}_k}.$$

The element x has nonzero image in the maximal ideal of this ring. A minimal prime $\mathfrak{p}'$ of $\langle x \rangle$ in this ring cannot be $\mathfrak{p}_k A_{\mathfrak{p}_k}$, for that ideal has height at least two, and $\mathfrak{p}'$ has height at most one by the case of the principal ideal theorem already proved. Of course, $\mathfrak{p}' \neq 0$ since it contains $x \neq 0$. The inverse image of $\mathfrak{p}'$ in A gives the required prime.

Thus we can modify the chain

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{n+1} = \mathfrak{p}$$

repeatedly until $x_1 \in \mathfrak{p}_1$. This completes the proof that the height of $\mathfrak{p}$ is at most n.

We now prove the converse. Suppose that $\mathfrak{p}$ is a prime ideal of A of height n. We want to show that we can choose $x_1, \ldots, x_n$ in $\mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime of $\langle x_1, \ldots, x_n \rangle$. If $n = 0$ we take the empty set of x_i. The fact that $\mathfrak{p}$ has height 0 means precisely that it is a minimal prime of $\langle 0 \rangle$. It remains to consider the case where $n > 0$. We use induction on n. Let $\mathfrak{q}_1, \ldots \mathfrak{q}_k$ be the minimal primes of A that are contained in $\mathfrak{p}$. Then $\mathfrak{p}$ cannot be contained in the union of these, or else it will be contained in one of them, and hence be equal to one of them and of height 0. Choose $x_1 \in \mathfrak{p}$ not in any minimal prime contained in $\mathfrak{p}$. Then the height of $\mathfrak{p}/x_1$ in A/x_1 is at most $n-1$: the chains in A descending from $\mathfrak{p}$ that had maximum length n must have ended with a minimal prime of A contained in $\mathfrak{p}$, and these are no longer available. By the induction hypothesis, $\mathfrak{p}/x_1$ is a minimal prime of an ideal generated by at most $n-1$ elements. Consider x_1 together with pre-images of these elements chosen in A. Then $\mathfrak{p}$ is a minimal prime of the ideal they generate, and so $\mathfrak{p}$ is a minimal prime of an ideal generated by at most n elements. The number cannot be smaller than n, or else by the first part, $\mathfrak{p}$ could not have height n. ☐

13 Systems of paramaters for a local ring

Definition 13.1. Let $(A, \mathfrak{m})$ be a local Noetherian ring of Krull dimension n. A **system of parameters** for A is a sequence of elements $x_1, \ldots, x_n \in \mathfrak{m}$ such that, equivalently:

1. $\mathfrak{m}$ is a minimal prime of $\langle x_1, \ldots, x_n \rangle$.

2. $\sqrt{\langle x_1, \ldots, x_n \rangle}$ is $\mathfrak{m}$.

3. $\mathfrak{m}$ has a power in $\langle x_1, \ldots, x_n \rangle$.

4. $\langle x_1, \ldots, x_n \rangle$ is $\mathfrak{m}$-primary.

The theorem we have just proved shows that every local ring of Krull dimension n has a system of parameters.

One cannot have fewer than n elements generating an ideal whose radical is $\mathfrak{m}$, for then $\dim A$ would be $< n$. Note that $x_1, \ldots, x_k \in \mathfrak{m}$ can be extended to a system of paramaters for A if and only if

$$\dim(A/\langle x_1, \ldots, x_k \rangle) \leq n - k$$

in which case

$$\dim(A/\langle x_1, \ldots, x_k \rangle) = n - k.$$

In particular, $x = x_1$ is a part of a system of parameters if and only if x is not in any minimal prime $\mathfrak{p}$ of A such that $\dim(A/\mathfrak{p}) = n$. In this situation, elements $y_1, \ldots, y_{n-k}$ extend $x_1, \ldots, x_k$ to a system of parameters for A if and only if their images in $A/\langle x_1, \ldots, x_k \rangle$ are a system of parameters for $A/\langle x_1, \ldots, x_k \rangle$.

Corollary 14. *Let $(A, \mathfrak{m})$ be local and let $x_1, \ldots, x_k$ be k elements of $\mathfrak{m}$. Then the dimension of $A/\langle x_1, \ldots, x_k \rangle$ is at least* $\dim A - k$.

14 Polynomial and Power Series Extensions

We next want to address the issue of how dimension behaves for Noetherian rings when one adjoins either polynomial or formal power series indeterminates.

We first note the following fact:

Lemma 14.1. *Let x be an indeterminate over A. Then x is in every maximal ideal of $A[[x]]$.*

Proof. If x is not in the maximal ideal $\mathfrak{m}$ it has an inverse mod $\mathfrak{m}$, so that we have $xf \equiv 1 \bmod \mathfrak{m}$, i.e. $1 - xf \in \mathfrak{m}$. Thus, it will suffice to show that $1 - xf$ is a unit. The idea of the proof is to show that

$$u = 1 + xf + x^2f^2 + x^3f^3 + \cdots$$

is an inverse: the infinite sum makes sense because only finitely many terms involve any given power of x. Note that

$$u = (1 + xf + \cdots + x^n f^n) + x^{n+1}w_n$$

with

$$w_n = f^{n+1} + xf^{n+2} + x^2f^{n+3} + \cdots,$$

which again makes sense since any given power of x occurs in only finitely many terms. Thus:

$$u(1 - xf) - 1 = (1 + xf + \cdots + x^n f^n)(1 - xf) + x^{n+1}w_n(1 - xf) - 1.$$

The first of the summands on the right is $1 - x^{n+1}f^{n+1}$, and so this becomes

$$1 - x^{n+1}f^{n+1} + x^{n+1}w_n(1 - xf) - 1 = x^{n+1}(-f^{n+1} + w_n(1 - xf)) \in x^{n+1}A[[x]],$$

and since the intersection of the ideals $x^t A[[x]]$ is clearly 0, we have that $u(1 - xf) - 1 = 0$ as required. $\square$

15 Integral Extensions

Integral extension of a ring means adjoining roots of monic polynomials over the ring. This is an important tool for studying affine rings, and it is used in many places, for example, in dimension theory, ring normalization and primary decomposition. Integral extensions are closely related to finite maps which, geometrically, can be though of as projections with finite fibres plus some algebraic conditions. Let us record the following definitions.

Definition 15.1. Let $A \subseteq B$ be an extension of rings.

1. An element $b \in B$ is called **integral over** A if there is a monic polynomial $f(T) \in A[T]$ satisfying $f(b) = 0$. In this case, we say b is a **root** of the monic $f(T)$.

2. B is called **integral over** A or an **integral extension of** A if every $b \in B$ is integral over A.

3. B is called a **finite extension** of A if B is a finitely generated A-module.

4. If $\varphi\colon A \to B$ is a ring map then φ is called an **integral** (respectively **finite**) **extension** if this holds for the subring $\varphi(A) \subset B$. Similarly, an element $b \in B$ is called **integral over** A if it is integral over $\varphi(A)$.

15.1 Examples and Nonexamples of Integral Extensions

Example 15.1. Let A be a ring. Then for any ideal $\mathfrak{a}$ in A, the quotient map $\pi\colon A \to A/\mathfrak{a}$ is an integral extension. More generally, any surjective ring map $\varphi\colon A \to B$ is an integral extension.

Example 15.2. $K[x, y] \subset K[x, y, z]/\langle x - yz\rangle$ is not an integral extension. Indeed, there is no monic polynomial $f \in K[x, y][t]$ such that $f(z) = 0$. To see why, suppose that

$$z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 0, \tag{45}$$

where $a_0, \ldots, a_{n-1} \in K[x, y]$. Since $z \equiv x/y$ in $K[x, y, z]/\langle x - yz\rangle$, we can rewrite (45) as

$$\frac{x^n}{y^n} + a_{n-1}\frac{x^{n-1}}{y^{n-1}} + \cdots + a_0 = 0.$$

After clearing the denominators and rearranging terms, we obtain

$$x^n = -y(a_{n-1}x^{n-1} + \cdots + a_0y^{n-1}).$$

This is clearly false since $K[x,y]$ is a UFD.

On the other hand, $K[y,z] \subset K[x,y,z]/\langle x-yz\rangle$ is an integral extension. Indeed, clearly y and z are integral over $K[y,z]$. Also, since x satisfies the monic polynomial

$$f(t) = t - yz \in K[y,z][t],$$

x is integral of $K[y,z]$ as well. We will see shortly that the product and sum of integral elements is integral, and thus every element in $K[x,y,z]/\langle x-yz\rangle$ is integral over $K[y,z]$. In fact, $K[x,y,z]/\langle x-yz\rangle \cong K[y,z]$.

Example 15.3. Let A be a ring and let $x \in A$ be a nonzerodivisor. Then $A \to A[x^{-1}]$ is an integral extension if and only if x is a unit. Indeed, if x is a unit in A, then $A[x^{-1}] = A$, and so obviously $A \to A[x^{-1}]$ is an integral extension. Conversely, suppose x^{-1} is integral over A. Then there exists $a_0, \dots, a_{n-1} \in A$ such that

$$x^{-n} + a_{n-1}x^{-(n-1)} + \cdots + a_0 = 0. \tag{46}$$

Multiplying both sides of (46) by x^{n-1} and rearranging terms, we obtain

$$x^{-1} = -a_{n-1} + a_{n-2}x + \cdots + a_0x^{n-1} \in A.$$

Thus x is a unit.

Example 15.4. Let K be a field and let $\overline{K}$ be an algebraic closure of K. Then $K \subseteq \overline{K}$ is an integral extension. Indeed, let $x \in \overline{K}$. Then x is algebraic over K, which means there exists $n \geq 0$ and $a_0, \dots, a_{n-1}, a_n \in K$ such that

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0. \tag{47}$$

Multiplying by a_n^{-1} on both sides of (47) gives us

$$x^n + a_{n-1}a_n^{-1}x^{n-1} + \cdots + a_0a_n^{-1} = 0.$$

Thus x is a root of the monic $f(T) = T^n + a_{n-1}a_n^{-1}T^{n-1} + \cdots + a_0a_n^{-1}$. This implies x is integral over K. Thus $K \subseteq \overline{K}$ is an integral extension.

15.2 Properties of Integral Extensions

Integrality is a local property in the following sense:

Proposition 15.1. *Let $A \subseteq B$ be an extension of rings and let $b \in B$. Then b is integral over A if and only if $\rho_{\mathfrak{p}}(b) = b/1$ is integral over $A_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ in A.*

Proof. First suppose b in integral over A and let $\mathfrak{p}$ be a prime ideal in A. Since b is integral over A, there exists $a_0, \dots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0. \tag{48}$$

Applying the localization map $\rho_{\mathfrak{p}}$ to (48) gives us

$$(b/1)^n + (a_{n-1}/1)(b/1)^{n-1} + \cdots + (a_0/1) = 0$$

where each $a_i/1 \in A_{\mathfrak{p}}$. Thus $b/1$ is integral over $A_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ in A.

Conversely, suppose $\rho_{\mathfrak{p}}(b) = b/1$ is integral over $A_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ in A. Note that $b/1$ being integral over $A_{\mathfrak{p}}$ means that there exists $n_{\mathfrak{p}} \in \mathbb{N}$, $s_{\mathfrak{p}} \in A\backslash\mathfrak{p}$, and $a_{\mathfrak{p},n_{\mathfrak{p}}-1}, \dots, a_{\mathfrak{p},0} \in A$ such that

$$s_{\mathfrak{p}}b^{n_{\mathfrak{p}}} + a_{\mathfrak{p},n_{\mathfrak{p}}-1}b^{n_{\mathfrak{p}}-1} + \cdots + a_{\mathfrak{p},0} = 0.$$

Now let $\langle\{s_{\mathfrak{p}} \mid \mathfrak{p} \text{ prime ideal}\}\rangle$ be the ideal generated by all $s_{\mathfrak{p}}$'s. Then we must have $\langle\{s_{\mathfrak{p}}\}\rangle = A$. Indeed, otherwise $\langle\{s_{\mathfrak{p}}\}\rangle$ would be contained in a maximal ideal, say $\mathfrak{m}$, which would be a contradiction as this would imply $s_{\mathfrak{m}} \in \mathfrak{m}$. Thus since $\langle\{s_{\mathfrak{p}}\}\rangle = A$, there exists finitely many primes $\mathfrak{p}_1, \dots \mathfrak{p}_k$ and elements $a_1, \dots, a_k \in A$ such that

$$a_1s_{\mathfrak{p}_1} + \cdots + a_ks_{\mathfrak{p}_k} = 1.$$

By reordering if necessary, we may assume that $n_{\mathfrak{p}_1} \geq n_{\mathfrak{p}_i}$ for all $1 \leq i \leq k$. Then note that

$$\begin{aligned} 0 &= \sum_{i=1}^k a_ib^{n_{\mathfrak{p}_1}-n_{\mathfrak{p}_i}}\left(s_{\mathfrak{p}_i}b^{n_{\mathfrak{p}_i}} + a_{\mathfrak{p}_i,n_{\mathfrak{p}_i}-1}b^{n_{\mathfrak{p}_i}-1} + \cdots + a_{\mathfrak{p}_i,0}\right) \\ &= \left(\sum_{i=1}^k a_is_{\mathfrak{p}_i}\right)b^{n_{\mathfrak{p}_1}} + \text{lower terms in } b \\ &= b^{n_{\mathfrak{p}_1}} + \text{lower terms in } b. \end{aligned}$$

It follows that b is integral over A. □

Remark 25. Essentially the same proof shows that b being integral is a Zariski-local property. In other words, b is integral over A if and only if there exists $s_1, \dots, s_n \in A$ such that $\langle s_1, \dots, s_n\rangle = 1$ and such that $\rho_{s_i}(b) = b/1$ is integral over A_{s_i} for all $1 \leq i \leq n$ (equivalently this says there exists an open covering $\{U_i\}$ of $X = \operatorname{Spec} A$ such that b is integral over U_i for all i).

15.2.1 Finite Extensions are Integral Extensions

Proposition 15.2. *Let $A \subseteq B$ be a finite extension of rings. Then $A \subseteq B$ is an integral extension. More generally, if $\mathfrak{a}$ is an ideal in A and N is a finitely generated B-module, then any $b \in B$ with $bN \subseteq \mathfrak{a}N$ satisfies a relation*

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0,$$

where $a_i \in \mathfrak{a}^{n-i}$ for all $0 \leq i < n$.

Proof. Let $b \in B$ and let $\mathrm{m}_b \colon B \to B$ be the multiplication by b map, given by $\mathrm{m}_b(x) = bx$ for all $x \in B$. Then m_b is an A-linear endomorphism of B. Choose a finite generating set of B over A, say $\{b_1, \dots, b_n\}$, and let $[\mathrm{m}_b]$ be a matrix representation of this endomorphism with respect to this generating set: for each $1 \leq i \leq n$, we have

$$bb_i = \sum_{j=1}^{n} a_{ji} b_j$$

for some $a_{ji} \in A$. Then we set $[\mathrm{m}_b] = (a_{ij})$. By the Cayley-Hamiltonian Theorem, $[\mathrm{m}_b]$ satisfies it's own characteristic polynomial, which is a monic polynomial with coefficients in A. Therefore b must satisfy this monic polynomial too. For the moreover part, note that one can show that the characteristic polynomial of $[\mathrm{m}_b]$ has the form

$$\chi_{[\mathrm{m}_b]}(T) = T^n - \mathrm{tr}[\mathrm{m}_b]T^{n-1} + \cdots + (-1)^n \mathrm{tr}(\Lambda^n[\mathrm{m}_b]).$$

Thus if $a_{ji} \in \mathfrak{a}$ for all i and j, then the coefficients in $\Lambda^k[\mathrm{m}_b]$ have entries in $\mathfrak{a}^k$, and hence $\mathrm{tr}(\Lambda^k[\mathrm{m}_b]) \in \mathfrak{a}^k$. □

15.2.2 A-Algebra Generated by Integral Elements is Finite

Proposition 15.3. *Let $A \subseteq B$ be an extension of rings. Suppose B is a finitely generated A-algebra of the form $B = A[b_1, \dots, b_k]$ with $b_i \in B$ integral over A for all $1 \leq i \leq k$. Then B is finite over A.*

Proof. We prove this by induction on the number of generators n. First consider the base case $n = 1$, so $B = A[b_1]$ where b_1 is integral over A. Thus there exists a First observe that $A[b_1]$ is finite over A. If b_1 satisfies a monic polynomial of degree n with coefficients in A, then $\{1, b_1, \dots, b_1^{n-1}\}$ form a system of generators of $A[b_1]$ as an A-module. By the same reasoning, $A[b_1, b_2] = A[b_1][b_2]$ is finite over $A[b_1]$, and hence finite over A. An inductive argument completes the proof. □

Corollary 15. *Let $A \subseteq B$ be a ring extension. Then an element $b \in B$ is integral over A if and only if $A[b]$ is a finitely generated A-module. In particular, if $b' \in B$ is also integral over A, then bb' and $b + b'$ are integral over A.*

Proof. If b is integral over A, then there is a monic polynomial $f(T) \in A[T]$ satisfying $f(b) = 0$. Then $A[b] \cong A[T]/\langle f(T) \rangle$ as A-modules. In particular, $A[b]$ is a finitely-generated A-module. The converse direction follows from Proposition (83.3). Finally, to see that bb' and $b + b'$ are integral over A, note that $A \subseteq A[b, b']$ is an integral extension since both b and b' are integral over A. It follows that $b + b'$ and bb' are integral over A since $b + b', bb' \in A[b, b']$. □

15.2.3 Transitivity of Integral Extensions

Proposition 15.4. *Let $A \subseteq B$ and $B \subseteq C$ be integral extensions. Then $A \subseteq C$ is an integral extension.*

Proof. Let $c \in C$. Since c is integral over B, there are $b_0, \dots, b_{n-1} \in B$ such that

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0.$$

Then $A \subseteq A[b_0, \dots, b_{n-1}] \subseteq A[b_0, \dots, b_{n-1}][c]$ is a composition of finite extensions. Thus, $A \subseteq A[b_0, \dots, b_{n-1}, c]$ is a finite extension, hence an integral extension. It follows that c is integral over A. □

15.2.4 Integral Extension $A \subseteq B$ with B an Integral Domain

Lemma 15.1. *Let $A \subset B$ be an integral extension and suppose B is an integral domain. Then B is a field if and only if A is a field.*

Proof. Suppose that B is a field and let a be a nonzero element in A. We will show that a is a unit in A. Since a belongs to B, we know that it is a unit in B, say $ab = 1$ for some b in B. Since B is integral over A, there exists $n \in \mathbb{N}$ and $a_0, \dots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0. \tag{49}$$

Multiplying a^{n-1} on both sides of (49) gives us

$$b + a_{n-1} + \cdots + a^{n-1}a_0 = 0.$$

In particular, $b \in A$. Thus a is a unit in A.

Conversely, suppose A is a field and let b be a nonzero element in B. Since b is integral over A, there exists $n \in \mathbb{N}$ and $a_0, \dots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0,$$

where we may assume that n is minimal. Then since n is minimal and B is an integral domain, we must have $a_0 \neq 0$. Thus

$$\begin{aligned} 1 &= (-a_0)^{-1}(b^n + a_{n-1}b^{n-1} + \cdots + a_1 b) \\ &= (-a_0)^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)b \end{aligned}$$

implies

$$(-a_0)^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)$$

is the inverse of b. □

Corollary 16. *Let L/K be an algebraic extension of fields and let A be an integral domain such that*

$$K \subseteq A \subseteq L.$$

Then A is a field.

Proof. First note that $K \subseteq A$ is an integral extension since L/K is an algebraic extension. Indeed, let $x \in A$. Then $x \in L$, and since L/K is algebraic, there exists $n \in \mathbb{N}$ and $a_0, a_1, \dots, a_n \in K$ such that

$$a_n x^n + \cdots + a_1 x + a_0 = 0. \tag{50}$$

where $a_n \neq 0$. Since K is a field, we can multiply both sides of (50) by a_n^{-1} and obtain

$$x^n + \cdots + a_n^{-1}a_1 x + a_n^{-1}a_0 = 0. \tag{51}$$

Then (51) implies x is integral over K. Since x was arbitrary, we see that $K \subseteq A$ is an integral extension. Now it follows from Lemma (80.3) that since K is a field, A must be a field too. □

15.2.5 Inverse Image of Maximal Ideal under Integral Extension is Maximal Ideal

Lemma 15.2. *Let $A \subseteq B$ is an integral extension and let $\mathfrak{n}$ be a maximal ideal in B. Then $\mathfrak{n} \cap A$ is a maximal ideal in A.*

Proof. The inverse image of any ideal in B is an ideal in A, so it suffices to show that $A \cap \mathfrak{n}$ is maximal in A. Observe that $A/(A \cap \mathfrak{n}) \subseteq B/\mathfrak{n}$ is an integral extension. Thus, since $B/\mathfrak{n}$ is a field, it follows from Lemma (80.3) that $A/(A \cap \mathfrak{n})$ is a field. Thus $A \cap \mathfrak{n}$ is a maximal ideal. □

15.3 More Integral Extension Properties

Proposition 15.5. *Let $A \subseteq B$ be an integral extension.*

1. *Let S be a multiplicatively closed subset of A. Then $A_S \subset B_S$ is an integral extension.*
2. *Let $\mathfrak{b} \subset B$ be an ideal. Then $A/A \cap \mathfrak{b} \to B/\mathfrak{b}$ is an integral extension.*
3. *Let $\mathfrak{m} \subset A$ be a maximal ideal. If $\mathfrak{m}B \neq B$, then $A/\mathfrak{m} \to B/\mathfrak{m}B$ is an integral extension.*

Proof.

1. Let $b/s \in B_S$. Since b is integral over A, there exists $a_0, \dots a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0. \tag{52}$$

Multiplying both sides of (52) by s^{-n}, we obtain

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_0}{s^n}\right) = 0.$$

Since $a_i/s^{n-i} \in A_S$ for all $0 \leq i < n$, we conclude that b/s is integral over A_S. Thus $A_S \subset B_S$ is an integral extension since b/s was arbitrary.

2. The map $\pi \colon A \to B/\mathfrak{b}$ is a composition of integral extensions, and hence must be an integral extension. Therefore

$$\begin{aligned} A/A \cap \mathfrak{b} &= A/\ker \pi \\ &\cong \operatorname{im} \pi \\ &\subset B/\mathfrak{b} \end{aligned}$$

is an integral extension.

3. The map $\pi \colon A \to B/\mathfrak{m}B$ is a composition of integral extensions, and hence must be an integral extension. Therefore

$$\begin{aligned} A/(A \cap \mathfrak{m}B) &= A/\ker \pi \\ &\cong \operatorname{im} \pi \\ &\subseteq B/\mathfrak{m}B \end{aligned}$$

is an integral extension. Now we claim that $A \cap \mathfrak{m}B = \mathfrak{m}$. Indeed, $A \cap \mathfrak{m}B$ is an ideal of A, and since

$$\mathfrak{m} \subseteq A \cap \mathfrak{m}B \subseteq A,$$

we must either have $\mathfrak{m} = A \cap \mathfrak{m}B$ or $A \cap \mathfrak{m}B = A$. If $A \cap \mathfrak{m}B = A$, then there exists $a_1, \ldots, a_n \in \mathfrak{m}$ and $b_1, \ldots, b_n \in B$ such that

$$1 = a_1 b_1 + \cdots + a_n b_n.$$

But this also implies that $B = \mathfrak{m}B$. Contradiction. □

Example 15.5. Let us give another reason why $K[x, y] \subset K[x, y, z]/\langle x - yz \rangle$ is not an integral extension. Assuming it was, then

$$\begin{aligned} K &\cong K[x, y]/\langle x, y \rangle \\ &\subset K[x, y, z]/\langle x - yz, x, y \rangle \\ &\cong K[z] \end{aligned}$$

would also be an integral extension. Contradiction.

15.3.1 Lying Over and Going Up Properties for Integral Extensions

Proposition 15.6. *Let $\iota \colon A \hookrightarrow B$ be an integral extension and let $\pi \colon Y \to X$ be the corresponding map of affine schemes where $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, and $\pi \colon Y \to X$ is defined by $\pi(\mathfrak{q}) = A \cap \mathfrak{q}$ for all primes $\mathfrak{q}$ of B.*

1. *(Lying over property) Let $\mathfrak{p}$ be a prime ideal in A. Then there exists a prime ideal $\mathfrak{q}$ of B that lies over $\mathfrak{p}$, that is, $A \cap \mathfrak{q} = \mathfrak{p}$. Equivalently, the map $\pi \colon Y \to X$ is surjective.*

2. *(Incomparability) Suppose $\mathfrak{q} \subseteq \mathfrak{q}'$ are two prime ideals of B which lie over the same prime ideal $\mathfrak{p}$ of A. Then we must have $\mathfrak{q} = \mathfrak{q}'$.*

3. *(Going up property) Let $\mathfrak{p} \subset \mathfrak{p}'$ be prime ideals of A and let $\mathfrak{q}$ be a prime ideal of B that $A \cap \mathfrak{q} = \mathfrak{p}$. Then there exists a prime ideal $\mathfrak{q}'$ of B such that $\mathfrak{q} \subset \mathfrak{q}'$ and $A \cap \mathfrak{q}' = \mathfrak{p}'$.*

Proof.
1. Since $A \subseteq B$ is an integral extension, we see that $A_\mathfrak{p} \subseteq B_\mathfrak{p}$ is an integral extension. Let $\mathfrak{n}$ be a maximal ideal in $B_\mathfrak{p}$. Then $\mathfrak{n} \cap A_\mathfrak{p}$ is a maximal ideal in $A_\mathfrak{p}$ by Lemma (15.2). Since $A_\mathfrak{p}$ is a local ring, it must be the unique maximal ideal, so $\mathfrak{n} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. Now we set $\mathfrak{q} = \mathfrak{m} \cap B$. Then $\mathfrak{q}$ is a prime ideal in B which lies over $\mathfrak{p}$.

2. Since $A \subseteq B$ is an integral extension, we see that $A_\mathfrak{p} \subseteq B_\mathfrak{p}$ is an integral extension. Then since $\mathfrak{p}_\mathfrak{p}$ is maximal in $A_\mathfrak{p}$ and both $\mathfrak{q}_\mathfrak{p}$ and $\mathfrak{q}'_\mathfrak{p}$ lie over $\mathfrak{p}_\mathfrak{p}$, it follows that $\mathfrak{q}_\mathfrak{p}$ and $\mathfrak{q}'_\mathfrak{p}$ are maximal ideals in $B_\mathfrak{p}$. Thus $\mathfrak{q}_\mathfrak{p} = \mathfrak{q}'_\mathfrak{p}$, which implies $\mathfrak{q} = \mathfrak{q}'$.

3. Since $A \subseteq B$ is an integral extension, we see that $A/A \cap \mathfrak{q} \subseteq B/\mathfrak{q}$ is an integral extension. In other words, since $A \cap \mathfrak{q} = \mathfrak{p}$, we see that $A/\mathfrak{p} \subseteq A/\mathfrak{q}$ is an integral extension. By part 1 of this proposition, there exists a prime ideal $\mathfrak{q}'/\mathfrak{q}$ in $B/\mathfrak{q}$ such that $(A/\mathfrak{p}) \cap (\mathfrak{q}'/\mathfrak{q}) = \mathfrak{p}'/\mathfrak{p}$. In particular, $\mathfrak{q}'$ is a prime ideal in B such that $\mathfrak{q} \subset \mathfrak{q}'$ and $A \cap \mathfrak{q}' = \mathfrak{p}'$. □

Corollary 17. *Let $A \subseteq B$ be an integral extension.*

1. *Let $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_r$ be a chain of prime ideals of B. Then $A \cap \mathfrak{q}_0 \subset \cdots \subset A \cap \mathfrak{q}_r$ forms a chain of prime ideals of A.*

2. *(Going up property) Conversely, let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r$ be a chain of prime ideals of A and suppose $\mathfrak{q}_0$ is a prime ideal of B which lies over $\mathfrak{p}_0$. Then there exists a chain $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_r$ of prime ideals of B with origin $\mathfrak{q}_0$ such that $\mathfrak{q}_i$ lies over $\mathfrak{p}_i$ for all $0 \leq i \leq r$.*

3. *We have $\dim A = \dim B$. If $\mathfrak{b}$ is an ideal of B which lies over an ideal $\mathfrak{a}$ of A, then $\operatorname{ht} \mathfrak{b} \leq \operatorname{ht} \mathfrak{a}$.*

Example 15.6. Let $A = \Bbbk[x]$, let $B = \Bbbk[x,y]/\langle xy \rangle$ and let $\iota \colon A \to B$ be the inclusion map. Note that the primes $\mathfrak{q}_1 = \langle \overline{x} \rangle$ and $\mathfrak{q}_2 = \langle \overline{x}, \overline{y} \rangle$ of B both lie over the prime $\mathfrak{p} = \langle x \rangle$ of A, and yet $\mathfrak{q}_1 \subset \mathfrak{q}_2$ where the inclusion is strict. In particular, $\dim(B/\mathfrak{p}B) = 1$ and $\dim(A/\mathfrak{p}) = 0$. Thus we know that $\iota \colon A \to B$ cannot be an integral extension, and indeed, it's easy to see that $\overline{y} \in B$ is not integral over A.

15.4 Geometric Interpretation

Corollary 18. *Let $\varphi \colon A \to B$ be an integral extension and let $f \colon Y \to X$ be the corresponding map of affine schemes, where $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, and $f(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q})$ for all $\mathfrak{q} \in Y$. Then f is a closed map.*

Proof. We want to show that f takes closed sets to closed sets. An arbitrary closed subset of Y has the form $\mathrm{V}(\mathfrak{b})$ where $\mathfrak{b}$ is an ideal of B. Thus we want to show $f(\mathrm{V}(\mathfrak{b}))$ is closed in X. In fact, we claim that $f(\mathrm{V}(\mathfrak{b})) = \mathrm{V}(\varphi^{-1}(\mathfrak{b}))$ Indeed, first note that the inclusion $f(\mathrm{V}(\mathfrak{b})) \subseteq \mathrm{V}(\varphi^{-1}(\mathfrak{b}))$ is always true (regardless of whether φ is an integral extension or not). Let us show why φ being an integral extension gives us the reverse inclusion. Let $\mathfrak{p} \in \mathrm{V}(\varphi^{-1}(\mathfrak{b}))$. Thus $\mathfrak{p}$ is a prime of A such that $\mathfrak{p} \supseteq \varphi^{-1}(\mathfrak{b})$. We want to show that $\mathfrak{p} \in f(\mathrm{V}(\mathfrak{b}))$. In other words, we want to find a prime $\mathfrak{q}$ of B such that $\mathfrak{q} \supseteq \mathfrak{b}$ and $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. Can this be done? Well, we know that since φ is an integral extension, we can certainly find a prime $\mathfrak{q}$ of B that lies over $\mathfrak{p}$ (i.e. such that $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$). However, the question is: can we find a prime $\mathfrak{q}$ of B that lies over $\mathfrak{p}$ *and* such that $\mathfrak{q} \supseteq \mathfrak{b}$. The answer is: yes. Indeed, consider the induced ring homomorphism $\overline{\varphi} \colon \overline{A} \to \overline{B}$ where $\overline{A} = A/\varphi^{-1}(\mathfrak{b})$ and $\overline{B} = B/\mathfrak{b}$. Then since $\overline{\varphi}$ is an integral extension, we can find a prime $\overline{\mathfrak{q}}$ of $\overline{B}$ which lies over the prime $\overline{\mathfrak{p}}$. This is equivalent to finding a prime $\mathfrak{q}$ of B which contains $\mathfrak{b}$ and which lies over $\mathfrak{p}$. $\square$

Example 15.7. Let $A = \mathbb{Q}[x,y]$, $\mathfrak{p} = \langle x \rangle$, and $B = \mathbb{Q}[x,y,z]/\langle z^2 - xz - 1 \rangle$. We want to find a prime ideal $\mathfrak{q} \subset \mathfrak{p}B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. We compute a primary decomposition of $\mathfrak{p}B$:

$$\mathfrak{p}B = \langle x, z^2 - xz - 1 \rangle = \langle x, z-1 \rangle \cap \langle x, z+1 \rangle.$$

Both prime ideals $\langle x, z-1 \rangle$ and $\langle x, z+1 \rangle$ in B give as intersection with A the ideal $\mathfrak{p}$.

Proposition 15.7. *Let A and C be rings, B be an integral domain, $\varphi : A \to B$ an integral extension. and $\psi : B \to C$ a ring homomorphism such that the restriction of ψ to A is injective. Then $\psi : B \to C$ is injective.*

Proof. Suppose $b \in \operatorname{Ker}(\psi)$. Since b is integral over A, we have

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \tag{53}$$

for some $a_i \in A$, and where n is minimal. Assume $b \neq 0$. Then $a_0 \neq 0$, since B is an integral domain. Applying ψ to (53) gives us $\psi(a_0) = 0$. Since the restriction of ψ to A is injective, $a_0 = 0$, which is a contradiction. Therefore $b = 0$, which implies ψ is injective. $\square$

Remark 26. For a finite map $\varphi : A \to B$ and $\mathfrak{m} \subset A$ a maximal ideal, $B/\mathfrak{m}B$ is a finite dimensional $(A/\mathfrak{m})$-vector space. This implies that the fibres of closed points of the induced map $\phi : \operatorname{Max}(B) \to \operatorname{Max}(A)$ are finite sets. To be specific, let $A = K[x_1, \ldots, x_n]/I$, $B = K[y_1, \ldots, y_k]/J$, and let

$$\mathbb{A}^m \supset \mathbf{V}(J) \xrightarrow{\phi} \mathbf{V}(I) \subset \mathbb{A}^m$$

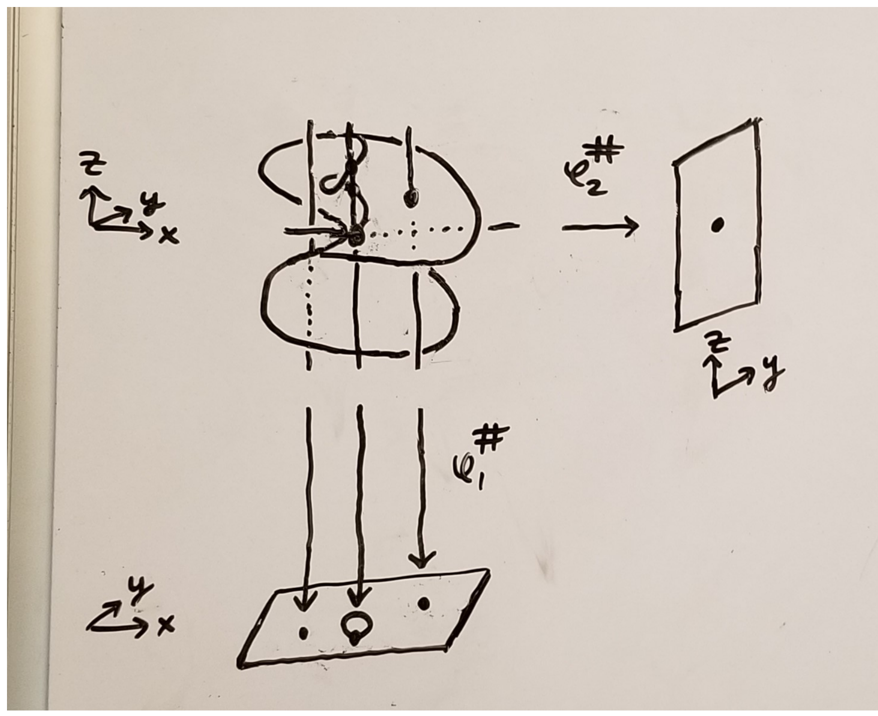
be the induced map. If $\mathfrak{m} = \langle x_1 - p_1, \ldots, x_n - p_n \rangle \subset K[x_1, \ldots, x_n]$ is the maximal ideal of the point $p = (p_1, \ldots, p_n) \in \mathbf{V}(I)$, then $\mathfrak{m}B = (J + \mathfrak{n})/J$ with $\mathfrak{n} := \langle \varphi(x_1) - p_1, \ldots, \varphi(x_n) - p_n \rangle \subset K[y_1, \ldots, y_k]$. Then $\mathbf{V}(J + N) = \phi^{-1}(p)$ is the fibre of ϕ over p, which is a finite set, since $\dim_K(K[y_1, \ldots, y_k]/(J + N)) < \infty$.

The converse, however, is not true, not even for local rings. But, if $\varphi : A \to B$ is a map between local analytic K-algebras, then φ is finite if and only if $\dim_K(B/\varphi(\mathfrak{m}_A)B) < \infty$.

Example 15.8. Let $A = K[x,y]$, $B = K[x,y,z]/\langle x - yz \rangle$, and $\varphi : A \to B$ be the ring homomorphism induced by $\varphi(x) = x$ and $\varphi(y) = y$. Then $\operatorname{Spec}(A)$ corresponds tof the (x,y)-plane, and $\operatorname{Spec}(B)$ corresponds to the "blown up" (x,y)-plane. The map $\varphi : A \to B$, induces a map $\varphi^{\#} : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$. We calculate the inverse images of some points $p_{i,j} = \langle x-i, x-j\rangle$ in $\mathrm{Max}(A) \subset \mathrm{Spec}(A)$: Let $s,t \in K\backslash\{0\}$. Then

$$\begin{aligned}
\left(\varphi^{\#}\right)^{-1}(p_{0,0}) &= \langle x-yz, x, y\rangle = \langle x,y\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{s,0}) &= \langle x-yz, x-s, y\rangle = \langle 1\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{0,t}) &= \langle x-yz, x, y-t\rangle = \langle x, y-t, z\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{s,t}) &= \langle x-yz, x-s, y-t\rangle = \langle x-1, y-1, s-tz\rangle
\end{aligned}$$

So there is one point which maps to $p_{s,t}$ and $p_{0,t}$, no points which maps $p_{s,0}$, and a whole line of points which maps to $p_{0,0}$.



On the other hand, if we let $A = K[y,z]$ and $\varphi : A \to B$ be the map given by $\varphi(y) = y$ and $\varphi(z) = z$, then it's easy to see φ is a ring isomorphism, and hence, the induced map $\varphi^{\#}$ is a bijection.

Now let us considered the projective version of this map. Let $\widetilde{A} = K[x,y,w]$, $\widetilde{B} = K[x,y,z,w]/\langle xw-yz\rangle$, and $\widetilde{\varphi} : \widetilde{A} \to \widetilde{B}$ be the ring homomorphism induced by $\widetilde{\varphi}(x) = x$, $\widetilde{\varphi}(y) = y$, and $\widetilde{\varphi}(w) = w$. Then in the $w=1$ plane, we recover $\varphi : A \to B$. We calculate the inverse images of some points $p_{i,j,k} = \langle x-i, x-j, x-k\rangle$ in $\mathrm{Max}(\widetilde{A}) \subset \mathrm{Spec}(\widetilde{A})$: Let $s,t,u \in K\backslash\{0\}$. Then

$$\begin{aligned}
\left(\varphi^{\#}\right)^{-1}(p_{0,0,0}) &= \langle x,y,w\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{s,0,0}) &= \langle x-s,y,w\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{0,t,0}) &= \langle x,y-t,w\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{0,0,u}) &= \langle x,y,w-u\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{0,t,u}) &= \langle x,y-t,w-u\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{s,t,0}) &= \langle x-s,y-t,w\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{s,0,u}) &= \langle 1\rangle \\
\left(\varphi^{\#}\right)^{-1}(p_{s,t,u}) &= \langle su-tz, x-s, y-t, w-u\rangle
\end{aligned}$$

Remark 27. Note that $\langle x-yz, x-s, y-t\rangle$ can be considered as an ideal in $K(s,t)[x,y,z]$.

15.5 Integral Closure

Definition 15.2. Let $A \subseteq B$ be an extension of rings. The **integral closure** of A in B, denoted $\overline{A_B}$, is defined to be set of all elements in B which are integral over A:

$$\overline{A_B} = \{b \in B \mid b \text{ is integral over } A\}.$$

It follows from Corollary (15) that $\overline{A_B}$ is closed under addition and multiplication. In particular, $\overline{A_B}$ is a ring. We say A is **integrally closed** in B if $A = \overline{A_B}$. In the situation where A is an integral domain and $B = K$ is its fraction field, then we write $\overline{A}$ instead of $\overline{A_K}$. We also say "$\overline{A}$ is the integral closure of A" and "A is integrally closed" instead of "$\overline{A}$ is the integral closure of A in K" and "A is integrally closed in K".

15.5.1 Integral Closure is Integrally Closed

Proposition 15.8. *Let $A \subseteq B$ be an extension of rings. Then $\overline{A_B}$ is integrally closed in B. In other words, $\overline{A_B} = \overline{(\overline{A_B})_B}$.*

Proof. This follows from transitivity of integral extensions. Indeed, let $b \in B$ be integral over $\overline{A_B}$. Then since $\overline{A_B}[b]$ is integral over $\overline{A_B}$ and since $\overline{A_B}$ is integral over A, we see that $\overline{A_B}[b]$ is integral over A. In particular, b is integral over A. This implies $b \in \overline{A_B}$ (by definition of integral closure). Thus $\overline{A_B}$ is integrally closed in B. □

15.5.2 Every Valuation Ring is Integrally Closed

Proposition 15.9. *Every Valuation Ring is Integrally Closed.*

Proof. Let A be a valuation ring with fraction field K and let $x \in K$ be integral over A. Then there exists $n \geq 1$ and $a_{n-1}, \dots, a_0 \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

If $x \in A$ we are done, so assume $x \notin A$. Then $x^{-1} \in A$, since A is a valuation ring. Multiplying the equation above by $x^{-(n-1)} \in A$ and moving all but the first term on the lefthand side to the righthand side yields

$$x = -a_{n-1} - \cdots - a_0 x^{-(n-1)} \in A,$$

contradicting our assumption that $x \notin A$. It follows that $x \in A$, and hence A is integrally closed. □

15.6 Integral Closure Properties

15.6.1 Localization Commutes With Integral Closure

Proposition 15.10. *Let $A \subseteq B$ be an extension of rings and let $S \subseteq A$ be a multiplicatively closed set. Then the integral closure of A in B localized at S is "the same as" the integral closure of the A_S in B_S. In symbols, this says $(\overline{A_B})_S = \overline{(A_S)_{B_S}}$.*

Proof. Recall that $A_S \subseteq B_S$ is an extension of rings (localization preserves injective maps). Let $b/s \in (\overline{A_B})_S$, where $b \in \overline{A_B}$. Thus there exists $n \geq 1$ and $a_0, \dots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Then $b/s \in \overline{(A_S)_{B_S}}$ since

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_0}{s^n}\right) = 0.$$

Convsersely, let $b/s \in \overline{(A_S)_{B_S}}$. Then there exists $n \geq 1$ and $a_0/s_0, \dots, a_{n-1}/s_{n-1} \in A_S$ such that

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s_{n-1}}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_0}{s_0}\right) = 0. \tag{54}$$

Multiplying both sides of (54) by $s^n s_0^n \cdots s_{n-1}^n$ gives us

$$(s_0 \cdots s_{n-1}b)^n + ss_0 \cdots s_{n-2}a_{n-1}(s_0 \cdots s_{n-1}b)^{n-1} + \cdots + s^n s_0^{n-1} \cdots s_{n-1}^n a_0 = 0.$$

Thus $s_0 \cdots s_{n-1}b$ is integral over A, and since $b/s = (s_0 \cdots s_{n-1}b)/(s_0 \cdots s_{n-1}s)$, we see that $b/s \in (\overline{A_B})_S$. □

Remark 28. The notation here is admittedly a bit clumsy. However when $B = K$ is a field, the notation becomes a little more readable. In this case, our notation says $\overline{A}_S = \overline{A_S}$.

15.6.2 Integral Closure Is Intersection of all Valuation Overrings

Proposition 15.11. *Let A be an integral domain, let K be its quotient field, and let $\overline{A}$ be the integral closure of A in K. Then*

$$\overline{A} = \bigcap_{A \subseteq B \subseteq K} B$$

where the intersection runs over all valuation overrings B of A.

Proof. Let B be a valuation overring of A. Then since B is integrally closed and $A \subseteq B$, it follows that $\overline{A} \subseteq B$. Since B was arbitrary, we see that $\overline{A} \subseteq \bigcap_{A \subseteq B \subseteq K} B$ where the intersection runs over all valuation overrings B of A.

Conversely, let $x \in \bigcap_{A \subseteq B \subseteq K} B$ and assume for a contradiction that x is not integral over A. Observe that $x^{-1}A[x^{-1}]$ is a proper ideal in $A[x]$. Indeed, if $x^{-1}A[x^{-1}] = A[x^{-1}]$, then there exists $n \geq 0$ and $a_1, \ldots, a_{n-1}, a_n \in A$ such that

$$a_n x^{-n} + a_{n-1} x^{-n+1} + \cdots + a_1 x^{-1} = 1. \tag{55}$$

Multiplying both sides of (55) by x^n and rearranging terms gives us

$$x^n - a_1 x^{n-1} - \cdots - a_{n-1} x - a_n = 0,$$

which contradicts the fact that x is not integral over A. Thus $x^{-1}A[x^{-1}]$ is a proper ideal in $A[x^{-1}]$. In particular, it is contained some maximal ideal, say $\mathfrak{m}$. Then there is a valuation ring $(B, \mathfrak{n})$ that dominates $(A[x^{-1}]_{\mathfrak{m}}, \mathfrak{m}A[x^{-1}]_{\mathfrak{m}})$. Since $x^{-1} \in \mathfrak{m} \subseteq \mathfrak{n}$, we see that $x \notin B$ (we can't have $x \in B$ *and* $x^{-1} \in \mathfrak{n}$ since $\mathfrak{n}$ does not contain any units). This contradicts our assumption that $x \in \bigcap_{A \subseteq B \subseteq K} B$. □

15.6.3 Applications

Theorem 15.3. *(Hilbert's Nullstellensatz). Assume that $K = \bar{K}$ is an algebraically closed field. Let $I \subset K[x] := K[x_1, \ldots, x_n]$ be an ideal. Suppose $g \in K[x]$ such that $g(x) = 0$ for all $x \in \mathbf{V}(I)$. Then $g \in \sqrt{I}$.*

Proof. We consider the ideal $J := IK[x,t] + \langle 1 - tg \rangle$ in the polynomial ring $K[x,t] := K[x_1, \ldots, x_n, t]$. If $J = K[x,t]$, then there exists $g_1, \ldots, g_s \in I$ and $h, h_1, \ldots, h_s \in K[x,t]$ such that $1 = \sum_{i=1}^{s} g_i h_i + h(1 - tg)$. Setting $t := \frac{1}{g} \in K[x]_g$, this implies

$$1 = \sum_{i=1}^{s} g_i \cdot h_i \left(x, \frac{1}{g} \right) \in K[x]_g.$$

Clearing denominators, we obtain $g^{\rho} = \sum_i g_i h_i'$ for some $\rho > 0$, $h_i' \in K[x]$. Therefore $g \in \sqrt{I}$.

Now assume that $J \subset K[x,t]$. We choose a maximal ideal $\mathfrak{m} \subset K[x,t]$ such that $J \subset \mathfrak{m}$. Using Theorem 3.5.1 (5), we know that $K[x,t]/\mathfrak{m} \cong K$, and, hence, $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n, t - a \rangle$ for some $a_i, a \in K$. Now $J \subset \mathfrak{m}$ implies $(a_1, \ldots, a_n, a) \in \mathbf{V}(J)$. If $(a_1, \ldots, a_n) \in \mathbf{V}(I)$, then $g(a_1, \ldots, a_n) = 0$. Hence, $1 - tg \in J$ does not vanish at $(a_1, \ldots, a_n)$, contradicting the assumption $(a_1, \ldots, a_n, a) \in \mathbf{V}(J)$. If $(a_1, \ldots, a_n) \notin \mathbf{V}(I)$, then there is some $h \in I$ such that $h(a_1, \ldots, a_n) \neq 0$, in particular $h(a_1, \ldots, a_n, a) \neq 0$ and therefore $(a_1, \ldots, a_n, a) \notin \mathbf{V}(J)$, again contradicting our assumption. □

Proposition 15.12. *Let A be an integral domain which is integrally closed in its field of fractions K, let L be a normal extension of K, let B be the integral closure of A in L, let G be the group of automorphisms of L over K, and let $\mathfrak{p}$ be a prime ideal of A. Then G acts transitively on the set of all primes of B which lie over $\mathfrak{p}$.*

Proof. We first consider the case where G is finite. Let $\mathfrak{q}$ and $\mathfrak{q}'$ be two prime ideals of B which lie over $\mathfrak{p}$. Then the $\sigma\mathfrak{q}$ (where $\sigma \in G$) is an ideal of B which lies over $\mathfrak{p}$ since B is integrally closed in L, and it suffices to show that $\mathfrak{q}'$ is contained in one of them, or equivalently, in their union by prime avoidance. Let $y \in \mathfrak{q}'$ and let $x = \prod \sigma y$ where the product runs over $\sigma \in G$. Note that x is fixed by G, thus since L/K is normal, it follows that there exists a power q of the characteristic of K such that $x^q \in K$. In particular, $x^q \in K \cap B = A$ since A is integrally closed. Thus $x^q \in \mathfrak{q}' \cap A = \mathfrak{p}$, which shows that x^q is contained in $\mathfrak{q}$. It follows that there exists a $\sigma \in G$ such that $\sigma y \in \mathfrak{q}$, whence $y \in \sigma^{-1}\mathfrak{q}$.

For the general case, assume $\mathfrak{q}$ and $\mathfrak{q}'$ lie over $\mathfrak{p}$. For every subfield E of L which is a finite normal extension over K, let G_E be the subset of G which consists of all $\sigma \in G$ which transform $\mathfrak{q} \cap E$ to $\mathfrak{q}' \cap E$. This is a closed subspace of G, hence compact since G is compact. Furthermore, each G_E is non-empty by what was shown above. As the G_E form a decreasing filtered family, their intersection is non-empty. □

Proposition 15.13. *Let A be an integral domain which is integrally closed in its field of fractions K, let B be an integral domain which is an integral extension of A, let $\mathcal{P} = (\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r)$ be a chain of prime ideals of A, and let $\mathfrak{q}_r$ be a prime ideal of B which lies of $\mathfrak{p}_r$. Then there exists a chain $\mathcal{Q} = (\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_r)$ of prime ideals of B which lies over $\mathcal{P}$ and with extremity $\mathfrak{q}_r$.*

Proof. The field of fractions of B is algebraic over K. Embed it in a normal extension L/K, let C be the integral closure of A in L, and let G be the group of automorphism of L over K. Let $\mathfrak{r}_r$ be a prime ideal of C which lies over $\mathfrak{q}_r$, and let $\mathcal{R}' = (\mathfrak{r}'_0 \subset \cdots \subset \mathfrak{r}'_r)$ be a chain of prime ideals which lies over $\mathcal{P}$. By Proposition (15.12), there exists a $\sigma \in G$ such that $\sigma\mathfrak{r}'_r = \mathfrak{r}_r$. Thus if we set $\mathfrak{q}_i = B \cap \sigma\mathfrak{q}_i$ for all i, then the chain $\mathcal{Q} = (\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_r)$ satisfies our requirements. □

Corollary 19. *Let A be an integral domain which is integrally closed in its field of fractions K, let B be an integral domain which is an integral extension of A, let $\mathfrak{b}$ be an ideal of B, and set $\mathfrak{a} = A \cap \mathfrak{b}$. Then we have*

$$\operatorname{ht}\mathfrak{a} = \operatorname{ht}\mathfrak{b}.$$

16 Noether Normalization and Hilbert's Nullstellensatz

This section is based on and inspired by Melvon Hochster's notes from [Hoc2]. We will prove the Noether normalization theorem over a field and, more generally, over an integral domain. We then deduce Hilbert's Nullstellensatz. The key to our proofs of the Noether normalization theorem and Hilbert's Nullstellensatz is the following idea:

Consider the polynomial x_1x_2 in $K[x_1, x_2]$. It is not monic in either variable. However if we let $\phi \colon K[x_1, x_2] \to K[x_1, x_2]$ be the unique automorphism such that $\phi(x_1) = x_1 + x_2$ and $\phi(x_2) = x_2$, then we see that $\phi(x_1x_2) = (x_1 + x_2)x_2 = x_2^2 + x_1x_2$ becomes monic as a polynomial of x_2 over $K[x_1]$. We think of the effect of applying an automorphism as a change of variables. Thus by a change of variables, we can turn the non-monic x_1x_2 into a monic $x_2^2 + x_1x_2$. This trick works more generally:

Lemma 16.1. *Let D be a domain and let $f \in D[x_1, \dots, x_n]$. Let $N \geq 1$ be an integer that bounds all the exponents of the variables occuring in the terms of f. Let ϕ be the D-automorphism of $D[x_1, \dots, x_n]$ such that $x_i \mapsto x_i + x_n^{N^i}$ for $i < n$ and such that x_n maps to itself. Then the image of f under ϕ is a polynomial whose highest degree term involving x_n has the form cx_n^m where c is a nonzero element in D. In particular, if $D = K$ is a field, then the image of f is a nonzero scalar of the field times a polynomial that is monic in x_n when considered as a polynomial over $K[x_1, \dots, x_{n-1}]$.*

Proof. Consider any nonzero term of f, which will have the form $c_\alpha x_1^{a_1} \cdots x_n^{a_n}$, where $\alpha = (a_1, \dots, a_n)$ and c_α is a nonzero element in D. The image of this term under ϕ is

$$\begin{aligned}\phi(c_\alpha x_1^{a_1} \cdots x_n^{a_n}) &= c_\alpha (x_1 + x_n^N)^{a_1}(x_2 + x_n^{N^2})^{a} \cdots (x_{n-1} + x_n^{N^{n-1}})^{a_{n-1}} x_n^{a_n} \\ &= c_\alpha x_n^{a_n + a_1N + a_2N^2 + \cdots + a_{n-1}N^{n-1}} + \text{terms lower in } x_n\end{aligned}$$

The exponents that one gets on x_n in these largest degree terms coming from distinct terms of f are all distinct, because of uniqueness of representation of integers in base N. Thus, no two exponents are the same, and no two of these terms can cancel. Therefore if we set

$$m = \sup\{a_n + a_1N + \cdots + a_{n-1}N^{n-1} \mid c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n} \text{ is a term of } f\},$$

then we see that

$$\phi(f) = cx_n^m + \text{terms lower in } x_n.$$

When $D = K$ is a field, it follows that $c^{-1}\phi(f)$ is monic of degree m in x_n when viewed as a polynomial over $K[x_1, \dots, x_{n-1}]$. □

16.0.1 Noether Normalization Theorem

Let R be an A-algebra and let $z_1, \dots, z_d \in R$. We shall say that the elements $z_1, \dots, z_d$ are **algebraically independent** over A if the unique A-algebra homomorphism from the polynomial ring $A[x_1, \dots, x_d]$ to R that sends x_i to z_i for $1 \leq i \leq n$ is an isomorphism. Equivalently, the monimals $z_1^{a_1} \cdots z_d^{a_d}$ as $(a_1, \dots, a_d)$ varies in $\mathbb{N}^d$ are all distinct and span a free A-submodule of R. The failure of the z_j to be algebraically independent means precisely that there is some nonzero polynomial $f(x_1, \dots, x_d)$ in $A[x_1, \dots, x_d]$ such that $f(z_1, \dots, z_d) = 0$.

Theorem 16.2. *Let D be an integral domain and let R be any finitely-generated D-algebra extension of D. Then there is a nonzero element $c \in D$ and elements $z_1, \dots, z_d$ in R_c algebraically independent over D_c such that R_c is module-finite over its subring $D_c[z_1, \dots, z_d]$, which is isomorphic to a polynomial ring (d may be zero) over D_c. In particular, if $D = K$ is a field, then it is not necessary to invert an element: every finitely-generated K-algebra is isomorphic with a module-finite extension of a polynomial ring.*

Proof. We use induction on the number n of generators of R over D. If $n = 0$, then $R = D$. In this case, we may take $d = 0$ and $c = 1$. Now suppose that $n \geq 1$ and that we know the result for algebras generated by $n - 1$ or fewer elements. Suppose that $R = D[\theta_1, \dots, \theta_n]$ has n generators. If the θ_i are algebraically independent over D, then we are done: we may take $d = n$, $z_i = \theta_i$ for all $1 \le i \le n$, and $c = 1$. Therefore we may assume that we have a nonzero polynomial $f(x_1, \ldots, x_n) \in D[x_1, \ldots, x_n]$ such that $f(\theta_1, \ldots, \theta_n) = 0$. Instead of using the original θ_j as generators of our D-algebra, note that we may use instead the elements

$$\begin{aligned}
\theta_1' &= \theta_1 - \theta_n^N \\
\theta_2' &= \theta_2 - \theta_n^{N^2} \\
&\vdots \\
\theta_{n-1}' &= \theta_{n-1} - \theta_n^{N^{n-1}} \\
\theta_n' &= \theta_n
\end{aligned}$$

where N is chosen for f as in Lemma (16.1). With ϕ as in Lemma (16.1), we have that these new algebra generators satisfy

$$\phi(f) = f(x_1 + x_n^N, \ldots, x_{n-1} + x_n^{N^{n-1}}, x_n)$$

which we shall write as g. We replace D and R by their localizations D_c and R_c, where c is the coefficient of the highest power of x_n occuring, so that the polynomial may be replaced by a multiple that is monic in x_n. After multiplying by a unit of D_c, we have that g is monic in x_n with coefficients in $D_c[x_1, \ldots, x_{n-1}]$. This means that θ_n' is integral over $D_c[\theta_1', \ldots, \theta_{n-1}'] = R_0$, and so R_c is module-finite over R_0. Since R_0 has $n-1$ generators over R_c, we have by the induction hypothesis that R_0 is module-finite over a polynomial subring $R_{cc'}[z_1, \ldots, z_d] \subseteq R_0$, and then $R_{cc'}$ is module-finite over $D_{cc'}[z_1, \ldots, z_d]$ as well. □

Lemma 16.3. *Let K be a field and let L be a field extension of K that is finitely generated as a K-algebra. Then L is a finite extension of K.*

Proof. We apply to L Noether's normalization theorem and obtain a finite injective homomorphism $K[T_1, \ldots, T_n] \to L$ of K-algebras. In particular $K[T_1, \ldots, T_n] \to L$ is an integral extension. By Lemma (80.3), we must have $n = 0$ which shows that $K \to L$ is a finite extension. □

16.0.2 Hilbert's Nullstellensatz

The connection between affine algebraic sets and commutative algebra is established by Hilbert's Nullstellensatz.

Theorem 16.4. *(Hilbert's Nullstellensatz) Let R be a finitely generated K-algebra. Then R is **Jacobson**, that is, for every prime ideal $\mathfrak{p}$ of R, we have*

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \supseteq \mathfrak{p} \\ \mathfrak{m} \text{ is maximal}}} \mathfrak{m}.$$

Moreover, suppose $\mathfrak{m}$ is a maximal ideal of R. Then the field extension $K \subseteq R/\mathfrak{m}$ is finite.

Proof. (Hilbert's Nullstellensatz) Lemma (16.3) implies at once the second assertion. Indeed, $R/\mathfrak{m}$ is a field extension of K which is finitely generated as a K-algebra. For the proof of the first assertion we start with a remark. If L is a finite field extension of K and $\varphi \colon R \to L$ is a K-algebra homomorphism, then the image of φ is an integral domain that is finite over K. Thus $\operatorname{im}\varphi$ is a field and therefore $\ker\varphi$ is a maximal ideal of R. We now show that R is Jacobson. Let $\mathfrak{p}$ be a prime ideal of R. By replacing R with $R/\mathfrak{p}$ if necessary, we may assume that R is a domain. In this case, we are trying to show that given a finitely generated K-algebra R which happens to also be an integral domain, the intersection of all maximal ideals of R is the zero ideal. Assume for a contradiction that there existed $x \neq 0$ that is contained in all maximal ideals of R. Since x is a nonzerodivisor, $R[x^{-1}]$ is a nonzero finitely generated K-algebra. Let $\mathfrak{n}$ be a maximal ideal of $R[x^{-1}]$. Then $L := R[x^{-1}]/\mathfrak{n}$ is a finite extension of K by the second assertion of the Nullstellensatz. The kernel of the composition $\varphi : R \to R[x^{-1}] \to L$ is a maximal ideal by the above remark, but it does not contain x. Contradiction. □

17 The structure theory of complete local rings

This section is based on and inspired by Melvin Hochster's notes from **[?]**. Let $(R, \mathfrak{m}, \Bbbk)$ be a complete local ring. Suppose R contains a field. Then there exists a field $\Bbbk_0$ contained in R such that the composite map $\Bbbk_0 \subseteq R \twoheadrightarrow \Bbbk$ is an isomorphism. In this case, we have

$$R = \Bbbk_0 \oplus \mathfrak{m}$$

as $\Bbbk_0$-vector spaces, and we may identify $\Bbbk$ with $\Bbbk_0$. Such a field $\Bbbk_0$ is called a **coefficient field** for R. The choice of a coefficient field $\Bbbk_0$ is *not unique* in general, although in positive prime characteristic p it is unique if $\Bbbk$ is perfect, which is a bit surprising. A local ring $R = (R, \mathfrak{m}, \Bbbk)$ that contains a field is called **equicharacteristic**, because R contains a field if and only if R and $\Bbbk$ have the same characteristic. Indeed, it is clear that if $\Bbbk \subseteq R$, then they must have the same characteristic. Conversely, assume that R and $\Bbbk$ have the same characteristic. If $\operatorname{char} R = p$ where p is a prime, then it is clear that R contains $\mathbb{F}_p$, so suppose that $\operatorname{char} R = 0 = \operatorname{char} \Bbbk$. Then R contains a copy of $\mathbb{Z}$. In fact, we claim that R contains a copy of $\mathbb{Q}$. To see this, we just need to show that every nonzero integer in R is a unit in R. Let n be a nonzero integer in R. Then $\overline{n}$ is nonzero in $\Bbbk$ since $\operatorname{char} \kappa = 0$, thus $\overline{n}$ is a unit, say $\overline{nr} = 1$ where $r \in R$. This implies $nr = 1 + x$ where $x \in \mathfrak{m}$. Since R is a local ring, $1 + x$ is a unit in R, but this implies n is a unit in R. Local rings that are not equicharacteristic are called **mixed characteristic**. The characteristic of the residue class field of such a ring is always a positive prime integer p (indeed, if $\operatorname{char} \Bbbk = 0$, then $\overline{n} \neq 0$ for all $n \in \mathbb{N}$ certainly implies $n \neq 0$ for all $n \in \mathbb{N}$ which would imply $\operatorname{char} R = 0$). The characteristic of the ring is either 0, which is what it will be in the domain case, or else a power of a prime p.

Definition 17.1. A **discrete valuation ring**, abbreviated DVR, is a local domain V, not a field, whose maximal ideal is principal.

Remark 29. It is easily shown that in a DVR, every nonzero element of V is uniquely expressible in the form ut^n, where u is a unit, and every ideal is consequently principal.

Example 17.1. Let $V = \mathbb{R}[t]_{\langle t^2+1 \rangle}$ and let $\mathfrak{m} = \langle t^2 + 1 \rangle \mathbb{R}[t]_{\langle t^2+1 \rangle}$. Then V is a DVR. Indeed, V is a local domain which is not a field and $\mathfrak{m}$ is principal. In fact, V is an example of a local ring that contains a field but does not contain a coefficient field. Observe that $V/\mathfrak{m} \cong \mathbb{C}$, but $V \subseteq \mathbb{R}(t)$ does not contain any element whose square is -1: the square of a non-constant rational function is non-constant, and the square of a real scalar cannot be -1.

17.1 Hensel's Lemma and coefficient fields in equal characteristic 0

17.1.1 Hensel's Lemma

Theorem 17.1. *Let $(R, \mathfrak{m}, \Bbbk)$ be a complete local ring and let f be a monic polynomial of degree d in $R[X]$. We denote by $\overline{f} = F$ to be the image of f under the canonical ring homomorphism $R[X] \to \Bbbk[X]$. If $F = GH$ where $G, H \in \Bbbk[X]$ are monic of degrees s and t, respectively, and G and H are relatively prime in $\Bbbk[X]$, then there are unique monic polynomials $g, h \in R[X]$ such that $f = gh$ and $\overline{g} = G$ while $\overline{h} = H$.*

Remark 30. Suppose that $c \in \Bbbk$ is a simple root of F (i.e. $F(c) = 0$ and $F'(c) \neq 0$). Then $F = GH$ where $G = X - c$ and $H(c) \neq 0$ (i.e. G and H are relatively prime). Then the theorem tells us that there exists unique monic polynomials $g, h \in R[X]$ such that $f = gh$ and $\overline{g} = G$ while $\overline{h} = H$. In particular, g has the form $g = X - r$ for some $r \in R$ such that $\overline{r} = c$ (i.e. $r \in R$ is a lift of $c \in \Bbbk$ under the canonical ring homomorphism $R \to \Bbbk$).

Proof. Let F_n denote the image of f in $(R/\mathfrak{m}^n)[X]$. We recursively construct monic polynomials $G_n \in (R/\mathfrak{m}^n)[X]$ and $H_n \in (R/\mathfrak{m}^n)[X]$ such that $F_n = G_n H_n$ for all $n \geq 1$, where G_n and H_n reduce to G and H, respectively, mod $\mathfrak{m}$, and show that F_n and G_n are unique. Note that it will follow that for all n that G_n has the same degree as G, namely s, and that H_n has the same degree as H, namely t, where $s + t = d$. The uniqueness implies that mod $\mathfrak{m}^{n-1}$, G_n, H_n become G_{n-1}, H_{n-1}, respectively. This yields that the sequence of coefficients of X^i in G_n is an element of

$$\varprojlim (R/\mathfrak{m}^n) = R,$$

since R is complete. Using the coefficient determined in this way, we get a polynomial g in $R[X]$, monic of degree s. Similarly, we get a polynomial h in $R[X]$, monic of degree t. It is clear that $\overline{g} = G$ and $\overline{h} = H$, and that $f = gh$, since this holds mod $\mathfrak{m}^n$ for all n: thus, every coefficient of $f - gh$ is in $\bigcap_n \mathfrak{m}^n = 0$.

It remains to carry through the recursion, we have $G_1 = G$ and $H_1 = H$ from the hypothesis of the theorem. Now assume that G_n and H_n have been constructed and shown unique for a certain $n \geq 1$. We must construct G_{n+1} and H_{n+1} and show that they are unique as well. It will be convenient to work mod $\mathfrak{m}^{n+1}$ in the rest of the argument: replace R by $R/\mathfrak{m}^{n+1}$. Construct g^*, h^* in $R[X]$ by lifting each coefficient of G_n and H_n respectively, but such that the two leading coefficients occur in degrees s and t respectively and are both 1. Thus we have

$$f \equiv g^* h^* \bmod \mathfrak{m}^n$$

Set $\Delta = f - g^* h^* \in \mathfrak{m}^n R[X]$. We want to show that there are unique choices of $\delta \in \mathfrak{m}^n R[X]$ of degree at most $s - 1$ and $\varepsilon \in \mathfrak{m}^n R[X]$ of degree at most $t - 1$ such that $f - (g^* + \delta)(h^* + \varepsilon) = 0$, or in other words, such that

$$\begin{aligned} \Delta &= \varepsilon g^* + \delta h^* + \varepsilon\delta \\ &= \varepsilon g^* + \delta h^*, \end{aligned}$$

where we used the fact that $\varepsilon, \delta \in \mathfrak{m}^n R[X]$, hence $\varepsilon\delta \in \mathfrak{m}^{2n} R[X] = 0$. Now, G and H generate the unit ideal in $\Bbbk[X]$. Then since $R[X]_{\text{red}} = \Bbbk[X]$, it follows that g^* and h^* generate the unit ideal in $R[X]$, and so we can write $1 = \alpha g^* + \beta h^*$ for some $\alpha, \beta \in R[X]$. Multiplying by Δ, we get

$$\Delta = \Delta\alpha g^* + \Delta\beta h^*.$$

Then $\Delta\alpha$ and $\Delta\beta$ are in $\mathfrak{m}^n R[X]$, but do not yet satisfy our degree requirements. Since h^* is monic, we can divide $\Delta\alpha$ by h^* to get a quotient γ with remainder ε, that is, $\Delta\alpha = \gamma h^* + \varepsilon$. Let Γ_n be the image of γ in $(R/\mathfrak{m}^n)[X]$ and let $\mathcal{E}_n$ be the image of ε in $(R/\mathfrak{m}^n)[X]$. Then we have

$$0 = \Gamma_n H_n + \mathcal{E}_n. \tag{56}$$

Since H_n is monic, the lead coefficient of $\Gamma_n H_n$ is just the lead coefficient of Γ_n. Combining this with the fact that $\deg \mathcal{E}_n < \deg H_n$, we see that we must have $\Gamma_n = 0 = \mathcal{E}_n$ in order for the equation (56) to make sense. It follows that $\gamma, \varepsilon \in \mathfrak{m}^n R[X]$, hence

$$\begin{aligned} \Delta &= (\gamma h^* + \varepsilon) g^* + \Delta\beta h^* \\ &= \varepsilon g^* + (\gamma g^* + \Delta\beta) h^* \\ &= \varepsilon g^* + \delta h^* \end{aligned}$$

where we set $\delta = \gamma g^* + \Delta\beta \in \mathfrak{m}^n R[X]$. Since Δ and εg^* both have degree $< d$, so does δh^*, which implies that the degree of δ is $\leq s-1$. This establishes existence of ε and δ.

To show uniqueness of ε and δ, suppose that

$$\varepsilon g^* + \delta h^* = \Delta = \varepsilon' g^* + \delta' h^*,$$

where $\delta', \varepsilon' \in \mathfrak{m}^n R[X]$ such that $\deg \delta' \leq s-1$ and $\deg \varepsilon' \leq t-1$. Subtracting, we get an equation

$$0 = \mu g^* + \nu h^*$$

where the degree $\mu = \varepsilon - \varepsilon'$ is $\leq t-1$ and the degree $\nu = \delta - \delta'$ is $\leq s-1$. Then observe that

$$\begin{aligned} 0 &= \mu\alpha g^* + \nu\alpha h^* \\ &= \mu(1 - \beta h^*) + \nu\alpha h^* \\ &= \mu - (\mu\beta - \nu\alpha) h^*. \end{aligned}$$

In particular, h^* divides μ. But h^* is monic and $\deg \mu < \deg h^*$, so we must have $\mu = 0$. A similar argument shows $\nu = 0$ as well. □

Remark 31. Suppose f factors in $(R/\mathfrak{m}^k)[x]$ as $f \equiv GH$ where G and H are monic such that $\langle G, H \rangle$ generates the unit ideal in $(R/\mathfrak{m}^k)[x]$. Then we can replicate the proof above to conclude that there exists unique monic polynomials $g, h \in R[x]$ such that $f = gh$ and $\overline{g} = G$ and $\overline{h} = H$.

Example 17.2. Consider $R = \mathbb{Z}_3$ and $f = X^2 - 7$. Then

$$X^2 - 7 \equiv (X-1)(X-2) \bmod 3.$$

Note that $X - 1$ and $X - 2$ are relatively prime in $\mathbb{F}_3[X]$. Thus Hensel's Lemma implies there exists unique $a, b \in \mathbb{Z}_3$ such that $\overline{a} = 1$, $\overline{b} = 2$, and

$$X^2 - 7 = (X-a)(X-b)$$

in $\mathbb{Z}_3[X]$. In particular, $\mathbb{Z}_3$ contains two distinct square roots of 7. One can check that these start out as

$$a = 1 + 1 \cdot 3 + 1 \cdot 3^2 + \cdots \quad \text{and} \quad b = 2 + 1 \cdot 3 + 1 \cdot 3^2 + \cdots$$

Example 17.3. Consider $R = \mathbb{Z}_3$ and $f = x^3 - x + 1$. Then f is irreducible mod 3. It follows that f is irreducible in $\mathbb{Z}_3[x]$. In particular, we have a degree 3 extension $\mathbb{Q}_3[x]/f \cong \mathbb{Q}_3(\alpha)$ where α is a choice of a root of f. On the other hand, consider $g = x^3 + 6x + 3$. Then in $\mathbb{F}_3[x]$ we have $g \equiv x^3$. However we cannot use Hensel's Lemma to deduce anything in this case. On the other hand, note that g is irreducible in $(\mathbb{Z}/9)[x]$. It follows that g is irreducible in $\mathbb{Z}_3[x]$.

Example 17.4. Consider $R = \mathbb{Z}_3$ and $f = X^4 - 7X^3 + 2X^2 + 2X + 1 \in \mathbb{Z}_3[X]$. Then

$$\begin{aligned} X^4 - 7X^3 + 2X^2 + 2X + 1 &\equiv (X-2)^2(X^2+1) \bmod 3 \\ &\equiv (X^2 - X + 1)(X^2 + 1) \bmod 3 \end{aligned}$$

Note that $X^2 - X + 1$ and $X^2 + 1$ are relatively prime in $\mathbb{F}_3[X]$. Thus Hensel's Lemma implies there exists unique $a, b, c \in \mathbb{Z}_3$ such that $\overline{a} = 1$, $\overline{b} = 1$, $\overline{c} = 1$ and

$$X^4 - 7X^3 + 2X^2 + 2X + 1 = (X^2 - aX + b)(X^2 + c)$$

in $\mathbb{Z}_3[X]$.

Example 17.5. Consider $R = \mathbb{C}[[T]]$ and let $f = X^2 - (1+T)$. Then

$$X^2 - (1+T) \equiv (X-1)(X+1) \bmod T.$$

Note that $X-1$ and $X+1$ are relatively prime in $\mathbb{C}[X]$. Thus Hensel's Lemma implies there exists unique $\alpha, \beta \in \mathbb{C}[[T]]$ such that $\alpha(0) = 1$, $\beta(0) = -1$, and

$$X^2 - (1+T) = (X-\alpha)(X-\beta)$$

in $\mathbb{C}[[T]][X]$. In particular, $\mathbb{C}[[T]]$ contains two distinct square roots of $1+T$. One can check that these start out as

$$\alpha(T) = 1 + \frac{1}{2}T - \frac{1}{8}T^2 + \cdots \quad \text{and} \quad \beta(T) = -1 - \frac{1}{2}T + \frac{1}{8}T^2 + \cdots$$

Theorem 17.2. *Let R be a ring that is complete with respect to the ideal I and let $f \in R[x]$ be a polynomial. If $a \in R$ is an approximate root of f in the sense that $f(a) \equiv 0$ modulo $f'(a)^2 I$, then there exists a root b of f near a in the sense that $f(b) = 0$ and $b \equiv a$ modulo $f'(a)I$. If $f'(a)$ is a nonzerodivisor, then b is unique.*

17.1.2 Coefficient fields in equal characteristic 0

Theorem 17.3. *Let $(R, \mathfrak{m}, \Bbbk)$ be a complete local ring that contains a field of characteristic 0. Then R has a coefficient field. In fact, R will contain a maximal subfield, and any such subfield is a coefficient field.*

Proof. Let $\mathcal{S}$ be the set of all subrings of R which happen to be fields. By hypothesis, $\mathcal{S}$ is nonempty. Given a chain of elements of $\mathcal{S}$, the union is again a subring of R that is a field. By Zorn's Lemma, $\mathcal{S}$ will have a maximal element, say $\Bbbk_0$. The composition $\Bbbk_0 \subseteq R \to \Bbbk$ induces a field extension $\Bbbk/\overline{\Bbbk}_0$ where we write $\overline{\Bbbk}_0$ to be the image of $\Bbbk_0$ under $R \to \Bbbk$. We claim that already we have $\Bbbk_0 = \Bbbk$. Indeed, assume for a contradiction that $\theta \in \Bbbk$ but $\theta \notin \overline{\Bbbk}_0$. We consider two cases. In both cases, we will find a field contained in R which is strictly larger than $\Bbbk_0$ which leads to a contradiction:

Case 1: Suppose θ is transcendental over $\overline{\Bbbk}_0$. Let t denote an element in R which maps to θ, that is, t is a lift of θ. Then t must be transcendental over $\Bbbk_0$, thus $\Bbbk_0[t]$ is a polynomial subring of R. Furthermore, every nonzero element in $\Bbbk_0[t]$ is a unit. Indeed, if $c_n t^n + \cdots + c_1 t + c_0 \in \mathfrak{m}$ with $c_n \neq 0$, then $\overline{c}_n \neq 0$ (since the map $\Bbbk_0 \to \Bbbk$ is injective) and $\overline{c}_n \theta^n + \cdots + \overline{c}_1 \theta + \overline{c}_0 = 0$ which contradicts the assumption that θ is transcendental over $\overline{\Bbbk}_0$. By the universal mapping property of localization, the inclusion $\Bbbk_0[t] \subseteq R$ extends to a map $\Bbbk_0(t) \subseteq R$, which is necessarily an inclusion. This yields a subfield of R larger than $\Bbbk_0$, a contradiction.

Case 2: Suppose θ is algebraic over $\overline{\Bbbk}_0$. Let f_θ be the minimal polynomial of θ over $\overline{\Bbbk}_0$ and let f be a monic irreducible polynomial over $\Bbbk_0$ which lifts f_θ. Since $\theta \in \Bbbk$, we have $f_\theta(x) = (x-\theta)H(x)$ where $H \in \Bbbk[x]$ is monic and where $x - \theta$ and H are relatively prime in $\Bbbk[x]$ because θ is separable over $\overline{\Bbbk}_0$ (this is the only place in the argument where we use that the field has characteristic 0). Thus Hensel's Lemma implies there exists a unique $t \in R$ where $t \equiv \theta \bmod \mathfrak{m}$ and a unique $h \in R[x]$ where h is monic and $\overline{h} = H$ such that $f = (x-t)h$. In particular, f is the minimal polynomial of t over $\Bbbk_0$. Finally, the isomorphisms

$$\Bbbk_0[t] \cong \Bbbk_0[x]/f \cong \overline{\Bbbk}_0[x]/f_\theta \cong \Bbbk_0[\theta]$$

implies that $\Bbbk_0[t]$ is a field contained in R that is strictly larger than $\Bbbk_0$, a contradiction. □

17.1.3 Coefficient fields in characteristic p when the residue class field is perfect

Theorem 17.4. *Let $(R, \mathfrak{m}, \Bbbk)$ be a complete local ring of positive prime characteristic p. Suppose that $\Bbbk$ is perfect. Let $R^{p^n} = \{r^{p^n} \mid r \in R\}$ for every $n \in \mathbb{N}$. Then $\Bbbk_0 = \bigcap_{n=0}^{\infty} R^{p^n}$ is a coefficient field for R, and it is the only coefficient field for R.*

Proof. First we show $\Bbbk_0$ is a subfield of R. First note that $\Bbbk_0 \cap \mathfrak{m} = 0$. Indeed, suppose $u \in \Bbbk_0 \cap \mathfrak{m}$. Thus for every for every $n \in \mathbb{N}$, there exists $v_n \in R$ such that $u = v_n^{p^n}$. Since $u \in \mathfrak{m}$, this implies $v_n \in \mathfrak{m}$ too, so $u \in \bigcap_{n=0}^{\infty} \mathfrak{m}^{p^n} = 0$. Thus, $\Bbbk_0 \backslash \{0\}$ consists of units in R. Now if $u = v_n^{p^n}$, then $1/u = (1/v_n)^{p^n}$. Therefore, the inverse of every nonzero element of $\Bbbk_0$ is also in $\Bbbk_0$. Since $\Bbbk_0$ is clearly a ring (as R has characteristic p), it is a subfield of R.

Next, we want to show that given $\theta \in \Bbbk$ some element of $\Bbbk_0$ maps to θ. Let t_n denote an element of R that maps to $\theta^{1/p^n} \in \Bbbk$ (since $\Bbbk$ is perfect). Then $t_n^{p^n}$ maps to θ. We claim that $(t_n^{p^n})$ is a Cauchy sequence in R, and so has a limit R. To see this, note that t_n and t_{n+1}^p both map to θ^{1/p^n} in $\Bbbk$, and so $t_n - t_{n+1}^p$ is in $\mathfrak{m}$. Taking p^n powers, we find that

$$t_n^{p^n} - t_{n+1}^{p^{n+1}} \in \mathfrak{m}^{p^n}.$$

for all $n \in \mathbb{N}$. Therefore, the sequence is Cauchy, and has a limit $t \in R$. It is clear that t maps to θ (The quotient map $R \twoheadrightarrow \Bbbk$ is continuous, where $\Bbbk$ has the discrete topology and R has the $\mathfrak{m}$-adic topology). Therefore, it suffices to show that $t \in R^{p^k}$ for every k. But

$$t_k, t_{k+1}^p, \ldots, t_{k+h}^{p^h}, \ldots$$

is a sequence of the same sort for the element θ^{1/p^k}, and so is Cauchy and has a limit s_k in A. But $s_k^{p^k} = t$ and so $t \in R^{p^k}$ for all $k \in \mathbb{N}$.

Finally we prove uniqueness. Suppose $\widetilde{\Bbbk}_0$ is another coefficient field for R. Then for all n we have

$$\widetilde{\Bbbk}_0 = \widetilde{\Bbbk}_0^{p^n} \subseteq R^{p^n}.$$

It follows that $\widetilde{\Bbbk}_0 \subseteq \Bbbk_0$. Then $\widetilde{\Bbbk}_0 \cong \Bbbk \cong \Bbbk_0$ implies $\widetilde{\Bbbk}_0 = \Bbbk_0$.

□

17.1.4 Coefficient fields in characteristic p when the residue field need not be perfect

Definition 17.2. Let $\Bbbk$ be a field of characteristic $p > 0$. Finitely many elements $\boldsymbol{\theta} = \theta_1, \ldots, \theta_n$ in $\Bbbk - \Bbbk^p$ are called ***p*-independent** if $[\Bbbk[\boldsymbol{\theta}] : \Bbbk^p] = p^n$. This is equivalent to the assertion that

$$\Bbbk^p \subseteq \Bbbk^p[\theta_1] \subseteq \Bbbk^p[\theta_1, \theta_2] \subseteq \cdots \subseteq \Bbbk^p[\theta_1, \theta_2, \cdots, \theta_n] = \Bbbk^p[\boldsymbol{\theta}]$$

is a strictly increasing tower of fields. At each stage there are two possibilities: either θ_{i+1} is already in $\Bbbk^p[\theta_1, \ldots, \theta_i]$ or it has degree p over it, since θ_{i+1} is purely inseparable of degree p over $\Bbbk^p$. Every subset of a p -independent set is p-independent. An infinite subset of $\Bbbk - \Bbbk^p$ is called ***p*-independent** if every finite subset is p-independent. A maximal p-independent subset of $\Bbbk - \Bbbk^p$ is called a ***p*-base** for $\Bbbk$. Zorn's Lemma guarantees the existsence of a p-base since the union of a chain of p-independent sets is p-independent If Θ is a p-base, then $\Bbbk = \Bbbk^p[\Theta]$ (for an element of $\Bbbk - \Bbbk^p[\Theta]$ could be used to enlarge the p-base. The empty set if a p-base for $\Bbbk$ if and only if $\Bbbk$ is perfect. The monomials in the elements of Θ of degree at most $p-1$ in each element are a basis for $\Bbbk$ over $\Bbbk^p$.

Theorem 17.5. *Let $(R, \mathfrak{m}, \Bbbk)$ be a complete local ring of positive prime characteristic p and let Θ be a p-base for $\Bbbk$. Let T be a subset of R which maps bijectively onto Θ. Then there is a unique coefficient field that contains T, namely*

$$\Bbbk_0 = \bigcap_{n \geq 0} R^{p^n}[T].$$

Thus there is a bijection between liftings of the p-base Θ and the coefficient fields of R.

Proof. Note that any coefficient field must contain some lifting of Θ. Observe also that $\Bbbk_0$ is clearly a subring of R that contains T. It will suffice to show that $\Bbbk_0$ is a coefficient field and that any coefficient field $\widetilde{\Bbbk}_0$ containing T is already contained in $\Bbbk_0$.

□

17.2 Coefficient fields and structure theorems

Before pursuing the issue of the existence of coefficient fields and coefficient rings further, we show that the existence of a coefficient field implies that the ring is a homomorphic image of a power series ring in finitely many variables over a field, and is also a module-finite extension of such a ring.

Recall that for any A-module M, we can put a topology on M called the I-adic topology. The basic open sets in this topology are of the form $U_{x,k} = x + I^k M$, where $x \in M$ and $k \in \mathbb{Z}_{\geq 0}$. Suppose $k, \ell \in \mathbb{Z}_{\geq 0}$ with $\ell \geq k$ and $x, y \in M$. Then it's easy to show that

$$U_{x,k} \cap U_{y,\ell} = \begin{cases} U_{x,k} & \text{if } x \equiv y \bmod I^k M \\ \varnothing & \text{else.} \end{cases}$$

It is also easy to show that this topological space is separated (also known as Hausdorff) if and only if

$$\bigcap_{n=0}^{\infty} I^n M = 0.$$

Proposition 17.1. *Let A be separated and complete in the I-adic topology, where I is a finitely generated ideal of A, and let M be an I-adically separated A-module. Let $u_1, \ldots, u_h \in M$ have images that span M/IM over A/I. Then $u_1, \ldots, u_h$ spans M over A.*

Proof. Since $M = Au_1 + \cdots Au_h + IM$, we find that for all n,

$$I^n M = I^n u_1 + \cdots + I^n u_n + I^{n+1} M. \tag{57}$$

Let $u \in M$ be given. Then u can be written in the form $a_{01}u_1 + \cdots + a_{0h}u_h + v_1$ where $v_1 \in IM$. Therefore $v_1 = a_{11}u_1 + \cdots + a_{1h}u_h + v_2$ where $a_{1j} \in IM$ and $v_2 \in I^2 M$. Then

$$u = (a_{01} + a_{11})u_1 + \cdots + (a_{0h} + a_{1h})u_h + v_2.$$

By a straightforward induction on n we obtain, for every n, that

$$u = (a_{01} + a_{11} + \cdots + a_{n1})u_1 + \cdots + (a_{0h} + a_{1h} + \cdots + a_{nh})u_h + v_{n+1},$$

where every $a_{jk} \in I^j$ and $v_{n+1} \in I^{n+1}M$. In the recursive step, the formula (57) is applied to the element $v_{n+1} \in I^{n+1}M$. For every k, $\sum_{j=0}^{\infty} a_{jk}$ represents an element s_k of the complete ring A. We claim that

$$u = s_1 u_1 + \cdots + s_h u_h.$$

The point is that if we subtract

$$(a_{01} + a_{11} + \cdots + a_{n1})u_1 + \cdots + (a_{0h} + a_{1h} + \cdots + a_{nh})u_n$$

from u, we get $v_{n+1} \in I^{n+1}M$, and if we subtract it from

$$s_1 u_1 + \cdots + s_h u_h,$$

we also get an element of $I^{n+1}M$. Therefore,

$$u - (s_1 u_1 + \cdots + s_h u_h) \in \bigcap_n I^{n+1} M = 0,$$

since M is I-adically separated. □

Remark 32. We tacitly used in the argument above that if $a_{jk} \in I^j$ for $j \geq n+1$, then

$$a_{n+1,k} + a_{n+2,k} + \cdots + a_{n+t,k} + \cdots \in I^{n+1}.$$

This actually requires an argument. If I is finitely generated, then I^{n+1} is finitely generated by the monomials of degree $n+1$ in the generators of I, say $g_1, \dots, g_d$. Then

$$a_{n+1+t,k} = \sum_{\nu=1}^{d} q_{t\nu} g_\nu,$$

with every $q_{t\nu} \in I^t$, and

$$\sum_{t=0}^{\infty} a_{n+1+t,k} = \sum_{\nu=1}^{d} \left(\sum_{t=0}^{\infty} q_{t\nu} \right) g_\nu.$$

Proposition 17.2. *Let $\varphi : A \to B$ be a ring homomorphism, and suppose that B is J-adically complete and separated for an ideal $J \subseteq B$ and that $I \subseteq A$ maps into J. Then there is a unique induced homomorphism $\widehat{A}^I \to B$ that is continuous (i.e. preserves limits of Cauchy sequences in the appropriate ideal-adic topology).*

Proof. $\widehat{A}^I$ is the ring of I-adic Cauchy sequences mod the ideal of sequences that converge to 0. The continuity condition forces the element represented by $\{a_n\}_n$ to map to

$$\lim_{n \to \infty} \varphi(a_n).$$

(Cauchy sequences map to Cauchy sequences: if $a_m - a_n \in I^N$, then $\varphi(a_m) - \varphi(a_n) \in J^N$, since $\varphi(I) \subseteq J$). It is trivial to check that this is a ring homomorphism that kills the ideal of Cauchy sequences that converge to 0, which gives the required map $\widehat{A}^I \to B$. □

17.3 The Mixed Characteristic Case

Definition 17.3. We say V is a **coefficient ring** if it is a field or if it is a complete local ring of the form $(V, pV, \Bbbk)$ where $\Bbbk$ has characteristic $p > 0$. If R is a complete local ring, then we say V is a coefficient ring for R if V is a coefficient ring, $V \subseteq R$ is local, and the induced map of residue fields is an isomorphism.

We will prove that coefficient rings always exist. For simplicity we will assume all rings are noetherian. In the case where the characteristic of $\Bbbk$ is $p > 0$, there are three possibilities:

1. If $p = 0$ in V, then V is a field. We've handled this case already.
2. If p is not nilpotent in V, then it will turn out that V is a noetherian discrete valuation domain.
3. If $p \neq 0$ but is nilpotent in V, then we will show that if V is a field of characteristic $p > 0$, then V has the form $W/p^n W$ where $n \geq 1$ and W is a discrete valuation domain with maximal ideal pW.

18 Characterization of the Dimension of Local Rings

Throughout this section, let $(R, \mathfrak{m})$ be a Noetherian local ring and assume $K = R/\mathfrak{m} \subseteq R$. We shall prove that the dimension of a local ring is equal to the degree of the Hilbert-Samuel polynomial and equal to the least number of generators of an $\mathfrak{m}$-primary ideal. We introduce the following non-negative integers:

- $\delta(R) :=$ the minimal number of generators of an $\mathfrak{m}$-primary ideal of R,
- $\mathrm{d}(R) := \deg(\mathrm{HSP}_{R,\mathfrak{m}})$,
- $\operatorname{edim} R :=$ the **embedding dimension** of R, defined as the minimal number of generators for $\mathfrak{m}$. Hence,

  $$\operatorname{edim} R = \dim_K(\mathfrak{m}/\mathfrak{m}^2)$$

  by Nakayama's Lemma.

Proposition 18.1. *Let M be a finitely generated R-module, let $x \in R$ be M-regular, and let Q be an $\mathfrak{m}$-primary ideal. Then*

1. $\deg(\mathrm{HSP}_{M,Q}) = \deg(\mathrm{HSP}_{M,\mathfrak{m}})$
2. $\deg(\mathrm{HSP}_{M/xM,Q}) \leq \deg(\mathrm{HSP}_{M,Q}) - 1$

Proof.

1. Suppose $\mathfrak{m} = \langle x_1, \dots, x_r \rangle$. Choose s such that $\mathfrak{m} \supset Q \supset \mathfrak{m}^s$. Then $\mathfrak{m}^k \supset Q^k \supset \mathfrak{m}^{sk}$ for all k implies $\mathrm{HSP}_{M,\mathfrak{m}}(k) \leq \mathrm{HSP}_{M,Q}(k) \leq \mathrm{HSP}_{M,\mathfrak{m}}(sk)$ for sufficiently large k. But this is only possible if $\deg(\mathrm{HSP}_{M,Q}) = \deg(\mathrm{HSP}_{M,\mathfrak{m}})$.
2. Apply Remark 5.5.3 to the exact sequence

   $$0 \longrightarrow M \xrightarrow{\cdot x} M \longrightarrow M/xM \longrightarrow 0$$

   and conclude that $\deg(\mathrm{HSP}_{M/xM,Q}) \leq \deg(\mathrm{HSP}_{M,Q}) - 1$.

□

Theorem 18.1. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then, with the above notation, $\delta(A) = d(A) = dim(A)$.*

Proof. We shall prove that

1. $\delta(A) \geq d(A)$;
2. $d(A) \geq \dim(A)$;
3. $\dim(A) \geq \delta(A)$.

(1): If Q is an $\mathfrak{m}$-primary ideal, then $\deg(\mathrm{HSP}_{A,Q}) = d(A)$. Also, if Q is generated by r elements, then $\deg(\mathrm{HSP}_{M,Q})$ is at most r.

(2): We prove this by induction on $d = d(A)$. If $d = 0$, then $\dim_K(A/\mathfrak{m}^n)$ is constant for sufficiently large n. This implies $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for sufficiently large n, and therefore, by Nakayama's lemma, $\mathfrak{m}^n = \langle 0 \rangle$. But then $\dim(A) = 0$ because $\mathfrak{m}$ is the only prime ideal in A.

Now assume $d > 0$, and let

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_s = \mathfrak{m}$$

be a maximal chain of prime ideals in A, so $s = \dim(A)$. Let $\overline{A} = A/\mathfrak{p}_0$. Then $\dim(\overline{A}) = s$. On the other hand, the obvious map $A/\mathfrak{m}^n \to \overline{A}/\overline{\mathfrak{m}}^n$ is surjective and, therefore, $\dim_K(A/\mathfrak{m}^n) \geq \dim_K(\overline{A}/\overline{\mathfrak{m}}^n)$. This implies $d(A) \geq d(\overline{A})$, and we may assume that $A = \overline{A}$ is an integral domain. If $s = 0$, then (2) is proved. If $s > 0$, then we choose a nonzerodivisor $x \in \mathfrak{p}_1$. Then $d(A/x) \leq d(A) - 1$.

□

Definition 18.1. Let $(A, \mathfrak{m})$ be a Noetherian local ring and let $d = \dim(A)$, $\{x_1, \dots, x_d\}$ is called a **system of parameters** of A, if $\langle x_1, \dots, x_d \rangle$ is $\mathfrak{m}$-primary. If moreover, $\langle x_1, \dots, x_d \rangle = \mathfrak{m}$, then it is called a **regular system of parameters**.

Theorem 18.2. *Let $R = \Bbbk[x_1, \dots, x_n] = \Bbbk[\boldsymbol{x}]$, let $\mathfrak{m} = \langle x_1, \dots, x_n \rangle$, let $\boldsymbol{f} = f_1, \dots, f_m$ be a sequence of polynomials in R, and let $A = R_\mathfrak{m}/\boldsymbol{f}$. Set $\mathrm{J}_{\boldsymbol{f}} = (\partial_{x_i} f_j)$ to be the Jacobian matrix of $\boldsymbol{f}$:*

$$\mathrm{J}_{\boldsymbol{f}} = \mathrm{J}_{\boldsymbol{f}}(\boldsymbol{x}) = \begin{pmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_n} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_m & \cdots & \partial_{x_n} f_m \end{pmatrix}.$$

Then

$$\operatorname{edim} A = n - \operatorname{rank} \mathrm{J}_{\boldsymbol{f}}(0).$$

Proof. Let $\mathfrak{n}$ be the maximal ideal of A. We have

$$\begin{aligned} \operatorname{edim} A &= \dim_\Bbbk(\mathfrak{n}/\mathfrak{n}^2) \\ &= \dim_\Bbbk((\mathfrak{m}/\boldsymbol{f})/(\mathfrak{m}^2 + \boldsymbol{f})/\boldsymbol{f})) \\ &= \dim_\Bbbk(\mathfrak{m}/(\mathfrak{m}^2 + \boldsymbol{f})) \\ &= \dim_\Bbbk((\mathfrak{m}/\mathfrak{m}^2)/((\mathfrak{m}^2 + \boldsymbol{f})/\mathfrak{m}^2)) \\ &= \dim_\Bbbk(\mathfrak{m}/\mathfrak{m}^2) - \dim_\Bbbk((\mathfrak{m}^2 + \boldsymbol{f})/\mathfrak{m}^2) \\ &= n - \dim_\Bbbk((\mathfrak{m}^2 + \boldsymbol{f})/\mathfrak{m}^2). \end{aligned}$$

The last dimension is equal to the number of linearly independent linear forms among the f_i mod $\mathfrak{m}^2$. This is equal to rank $\mathrm{J}_{\boldsymbol{f}}(0)$. Indeed, for each $1 \leq i \leq m$, we break up f_i into a sum of its homogeneous pieces:

$$f_i = f_{i,0} + f_{i,1} + \cdots + f_{i,d_i},$$

where $f_{i,j}$ is the degree j part of f_i (in particular note that $f_{i,0} = f_i(0) = 0$ since $f_i \in \mathfrak{m}$). The $f_{i,1}$ are the linear forms of the f_i (i.e. the components of degree 1). Write

$$f_{i,1} = c_{i,1}x_1 + c_{i,2}x_2 + \cdots + c_{i,n}x_n$$

where $c_{i,j} \in \Bbbk$. Then note that

$$\mathrm{J}_{\boldsymbol{f}}(0) = \begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{m,1} & \cdots & c_{m,n} \end{pmatrix}.$$

Then the rank of $\mathrm{J}_{\boldsymbol{f}}(\boldsymbol{0})$ is precisely equal ot the number of linearly independent forms among the f_i mod $\mathfrak{m}^2$. □

Definition 18.2. A Noetherian local ring A is called a **regular local ring** if $\dim(A) = \operatorname{edim}(A)$.

Example 18.1. Let $R = \mathbb{Q}[x, y, z]_{\langle x,y,z \rangle}$ and let $\boldsymbol{f} = f_1, f_2, f_3$ where

$$\begin{aligned} f_1 &= x + y^3 \\ f_2 &= y + xyz \\ f_3 &= y + z + x^2. \end{aligned}$$

We want to find out whether $A = R/f$ is regular. First we calculate the Jacobian matrix of the ideal f:

$$\mathrm{J}_f = \mathrm{J}_f(x,y,z) = \begin{pmatrix} 1 & 3y^2 & 0 \\ 0 & 1 & xy \\ 2x & 1 & 1 \end{pmatrix}.$$

The rank of this matrix evaluated at the point $(0,0,0)$ is 3. This implies that $\operatorname{edim} A = 0$. Next, observe that

$$\begin{aligned} \langle f \rangle &= \langle x + y^3, y + xyz, y + z + x^2 \rangle \\ &= \langle x + y^3, y(1 + xz), y + z + x^2 \rangle \\ &= \langle x + y^3, y, y + z + x^2 \rangle \\ &= \langle x, y, z \rangle \end{aligned}$$

since $1 + xz$ is a unit in R. Therefore,

$$\begin{aligned} A &= \mathbb{Q}[x,y,z]_{\langle x,y,z\rangle} / \langle x + y^3, y + xyz, y + z + x^2 \rangle \\ &= \mathbb{Q}[x,y,z]_{\langle x,y,z\rangle} / \langle x, y, z \rangle \\ &\cong \mathbb{Q}. \end{aligned}$$

Thus $\dim A = 0 = \operatorname{edim} A$. Hence A is a regular local ring.

Example 18.2. Let $A = \mathbb{Q}[x,y,z]_{\langle x,y,z\rangle}$ and let $I = \langle xz, yz, z^2 \rangle$.The Jacobian matrix of the ideal I is

$$\operatorname{Jacob}(I) = \begin{pmatrix} z & 0 & 0 \\ 0 & z & 0 \\ x & y & 2z \end{pmatrix}.$$

The rank of this matrix evaluated at the point $(0,0,0)$ is 0. This implies that $\operatorname{edim}(A/I) = 3 \neq 2 = \dim(A/I)$. Therefore A/I is not a regular local ring. Indeed, let $\mathfrak{m}$ denote the maximal ideal in A/I. Then

$$\begin{aligned} \mathfrak{m} &= \langle x, y, z \rangle \\ \mathfrak{m}^2 &= \langle x^2, xy, y^2 \rangle \\ \mathfrak{m}^3 &= \langle x^3, x^2y, xy^2, y^3 \rangle \\ \mathfrak{m}^4 &= \langle x^4, x^3y, x^2y^2, xy^3, y^4 \rangle \end{aligned}$$

and

$$\begin{aligned} A/\mathfrak{m} &= \mathbb{Q} \\ \mathfrak{m}/\mathfrak{m}^2 &= \mathbb{Q}\overline{x} + \mathbb{Q}\overline{y} + \mathbb{Q}\overline{z} \\ \mathfrak{m}^2/\mathfrak{m}^3 &= \mathbb{Q}\overline{x}^2 + \mathbb{Q}\overline{xy} + \mathbb{Q}\overline{y}^2 \\ \mathfrak{m}^3/\mathfrak{m}^4 &= \mathbb{Q}\overline{x}^3 + \mathbb{Q}\overline{x}^2\overline{y} + \mathbb{Q}\overline{xy}^2 + \mathbb{Q}\overline{y}^3. \end{aligned}$$

The idea here is that z is a nilpotent element, and this is what makes $\dim_{\mathbb{Q}}(\mathfrak{m}/\mathfrak{m}^2) = 3$ instead of $\dim_{\mathbb{Q}}(\mathfrak{m}/\mathfrak{m}^2) = 2$.

Example 18.3. Here's an example of a local ring which is not regular. Let $A = \mathbb{Q}[x,y]_{\langle x,y\rangle}$ and let $I = \langle y^2 - x^3 \rangle$. The Jacobian matrix of the ideal I is

$$\operatorname{Jacob}(I) = \begin{pmatrix} -3x^2 & 2y \end{pmatrix}.$$

The rank of this matrix evaluated at the point $(0,0,0)$ is 0. This implies that $\operatorname{edim}(A) = 2$. On the other hand, we have $\dim_{\mathbb{Q}}(A/\langle y^2 - x^3 \rangle) = 1$ since $y^2 - x^3$ is a nonzerodivisor of A. Therefore A/I is not a regular ring. For instance, we have

$$\begin{aligned} \mathfrak{m} &= \langle x, y \rangle \\ \mathfrak{m}^2 &= \langle x^2, xy, y^2 \rangle \\ \mathfrak{m}^3 &= \langle x^3, x^2y, y^2 \rangle \\ \mathfrak{m}^4 &= \langle y^2 - x^3, x^4, x^3y \rangle \\ \mathfrak{m}^5 &= \langle y^2 - x^3, x^5, x^4y \rangle \end{aligned}$$

and

$$\begin{aligned}
A/\mathfrak{m} &= \mathbb{Q} \\
\mathfrak{m}/\mathfrak{m}^2 &= \mathbb{Q}\overline{x} + \mathbb{Q}\overline{y} \\
\mathfrak{m}^2/\mathfrak{m}^3 &= \mathbb{Q}\overline{x}^2 + \mathbb{Q}\overline{xy} \\
\mathfrak{m}^3/\mathfrak{m}^4 &= \mathbb{Q}\overline{x}^3 + \mathbb{Q}\overline{x}^2 y \\
\mathfrak{m}^4/\mathfrak{m}^5 &= \mathbb{Q}\overline{x}^4 + \mathbb{Q}\overline{x}^3 y
\end{aligned}$$

Note that $Q = \langle x \rangle$ is $\mathfrak{m}$-primary.

Example 18.4. Let $A = K[x,y,z]$, $\mathfrak{m} = \langle x,y,z \rangle$, and $I = \langle x^2+y^3+z^4, xy+xz+z^3 \rangle$. We want to find out whether $A_\mathfrak{m}/I$ is regular. The rank Jacobian matrix of the ideal I evaluated at the point $(0,0,0)$ is 0. Thus, $\mathrm{edim}(A_\mathfrak{m}/I) = 3$. To find the dimension of $A_\mathfrak{m}/I$, we calculate the Hilbert series of $\mathrm{Gr}_\mathfrak{m}(A_\mathfrak{m}/I)$. A standard basis for $\langle x^2+y^3+z^4, xy+xz+z^3 \rangle$ with respect to ds order is given by

$$\begin{aligned}
f_1 &= x^2+y^3+z^4 \\
f_2 &= xy+xz+z^3 \\
f_3 &= y^4+y^3z-xz^3+yz^4+z^5
\end{aligned}$$

Therefore,

$$\mathrm{Gr}_\mathfrak{m}(A_\mathfrak{m}/I) \cong A/\langle x^2, xy+xz, y^4+y^3z-xz^3 \rangle.$$

A minimal A-resolution of $\mathrm{Gr}_\mathfrak{m}(A_\mathfrak{m}/I)$ is given by

$$A(-3) \oplus A(-5) \xrightarrow{\begin{pmatrix} x & y^3 \\ -y-z & -z^3 \\ 0 & -x \end{pmatrix}} A(-2) \oplus A(-2) \oplus A(-4) \xrightarrow{\begin{pmatrix} xy+xz & x^2 & y^4+y^3z-xz^3 \end{pmatrix}} A$$

So

$$\begin{aligned}
\mathrm{HP}_{\mathrm{Gr}_\mathfrak{m}(A_\mathfrak{m}/I)}(t) &= \frac{1-(t^2+t^2+t^4)+(t^3+t^5)}{(1-t)^3} \\
&= \frac{1-2t^2+t^3-t^4+t^5}{(1-t)^3} \\
&= \frac{1+2t+t^2+t^3}{1-t}.
\end{aligned}$$

This tells us that $\dim(A_\mathfrak{m}/I) = 1$.

Theorem 18.3. *(Krull's Principal Ideal Theorem) Let A be a Noetherian ring, $x \in A$ a nonzerodivisor, and $\mathfrak{p} \in$ minAss(A/x). Then codim$(\mathfrak{p}) = 1$.*

Proof. Let $\langle x \rangle = Q_1 \cap \cdots \cap Q_r$ be an irredundant primary decomposition. We may assume that $\mathfrak{p} = \sqrt{Q_1}$. As $\mathfrak{p} \in \mathrm{minAss}(A/x)$, we have $\sqrt{Q_i} \not\subset \mathfrak{p}$ for $i > 1$. Especially $xA_\mathfrak{p} = Q_1 A_\mathfrak{p}$ is a $(\mathfrak{p}A_\mathfrak{p})$-primary ideal. From the characterization of the dimension of local rings, we know that the minimal number of generators of a $(\mathfrak{p}A_\mathfrak{p})$-primary ideal is equal to the dimension of A. Therefore $\dim(A_\mathfrak{p}) \leq 1$. This implies that $\mathrm{codim}(\mathfrak{p}) \leq 1$. If $\mathrm{codim}(\mathfrak{p}) = 0$, then $\mathfrak{p} \in \mathrm{minAss}(A)$, and therefore x is a zerodivisor. This is a contradiction to the assumption, and proves the theorem. □

Remark 33. In the proof, we didn't need to use the fact that x is a nonzerodivisor. We mainly needed x to not be contained in a minimal associated prime of A.

Example 18.5. Let's use Krull's Principal Ideal Theorem to find the dimension of $A = \Bbbk[x,y,z]/\langle xy, xz \rangle$. Since $\mathrm{Ass}(\langle xz, yz \rangle) = \{\langle x,y \rangle, \langle z \rangle\}$, a nonzerodivisor of A is given by $x - z$. The associated primes of $\langle xy, xz, x-z \rangle$ are $\mathrm{Ass}(\langle xz, yz, x-z \rangle) = \{\langle x,z \rangle, \langle x,y,z \rangle\}$, with the minimal associated prime being $\langle x,z \rangle$. Krull's Principal Ideal Theorem tells us that the prime $\langle x,z \rangle$ contains exactly one prime of A, namely, $\langle z \rangle$. Next we pass to the quotient $A/\langle xz, yz, x-z \rangle$. A nonzerodivisor here is given by $y-1$. There is only one associated primes of $\langle xy, xz, x-z, y-1 \rangle$, which is just $\langle x, y-1, z \rangle$. Again, Krull's Principal Ideal Theorem tells us that the prime $\langle x, y-1, z \rangle$ contains exactly one prime $A/\langle xz, yz, x-z \rangle$, namely $\langle x,z \rangle$. We get a picture that looks like this

$$\begin{tikzcd}
 & & \langle x,y-1,z\rangle \\
 & \langle x,z\rangle \arrow[ur, dash] & \langle x-z,xz,yz,y-1\rangle \arrow[u, dash] \\
\langle z\rangle \arrow[ur, dash] & \langle x-z,xz,yz\rangle \arrow[u, dash] \arrow[ur, dash] & \\
\langle xz,yz\rangle \arrow[u, dash] \arrow[ur, dash] & &
\end{tikzcd}$$

Something interesting happens when we localize at $\langle x,y,z\rangle$. Indeed, we proceed as usual, we first choose the nonzero divisor $x-z$, but now every element in $A_{\langle x,y,z\rangle}/\langle xz,yz,x-z\rangle$ is a zerodivisor. However, we don't really need to pick another zerodivisor at this point, we just need to pick an element not in minass $(\langle xz,yz,x-z\rangle) = \langle x,z\rangle$. In particular, the element y works.

19 Regular Local Rings

Throughout this section, let $R=(R,\mathfrak{m},\Bbbk)$ be a local noetherian ring. Set $\delta = \operatorname{depth} R$ to be the depth of R (i.e. the maximal length of a regular sequence contained in $\mathfrak{m}$), set $d=\dim R$ to be the dimension of R (i.e. the maximal length of a chain of prime ideals of R), and set $e = \operatorname{edim} R$ to be the embedded dimension of R (i.e. the minimal number of generators of $\mathfrak{m}$ or equivalently the $\Bbbk$-dimension of $\mathfrak{m}/\mathfrak{m}^2$ by Nakayama's lemma). In general we have inequalities:

$$\delta \le d \le e.$$

Indeed, the inequality $d\le e$ follows from Krull's principal ideal theorem, whereas the inequality $\delta \le d$ follows from the fact that $x\in R$ is a nonzerodivisor if and only if it avoids all associated primes of R (so in particular it avoids the minimal primes of R) thus $\delta_{R/x} = \delta - 1$ and $d_{R/x} = d-1$. We give R a special name when we have $d=e$, and in this case, it will turn out that we in fact have $\delta = d = e$ as well.

Definition 19.1. We say R is **regular** if $d=e$. In this case, every minimal system of generators of $\mathfrak{m}$ has d elements. Such a minimal system of generators is a system of parameters for R; it is called a **regular system of parameters**. If S is any commutative noetherian ring (not necessarily local), then we say S is **regular** if $S_{\mathfrak{q}}$ is regular for every prime $\mathfrak{q}$ of S.

Suppose that R is regular and let $\boldsymbol{x} = x_1,\dots,x_d$ be a system of parameters for R (so $\langle \boldsymbol{x}\rangle = \mathfrak{m}$ since R is regular). The reason why we call $\boldsymbol{x}$ is a *regular* system of parameters is because $\boldsymbol{x}$ is a regular R-sequence contained in $\mathfrak{m}$! Indeed, this follows from the following proposition:

Proposition 19.1. *Suppose R is a regular local ring. Then R is an integral domain.*

Proof. We do induction on $\dim R = d$. In case $d=0$, we must have $\mathfrak{m}=0$, so R is a field, and the result is trivial. Thus we may suppose that $d>0$. By Nakayama's lemma, we have $\mathfrak{m}^2 \neq \mathfrak{m}$, so by prime avoidance and the finiteness of the set of minimal primes of R, we may find and element $x\in\mathfrak{m}$ that is outside the minimal primes of R, and also outside $\mathfrak{m}^2$. Set $S=R/x$ and let $\mathfrak{n}=\mathfrak{m}S$ be the maximal ideal of S. By the choice of x, we have $\dim S = d-1$. Also $\mathfrak{n}/\mathfrak{n}^2 = \mathfrak{m}/(\mathfrak{m}^2+\langle x\rangle)$ is a proper homomorphic image of $\mathfrak{m}/\mathfrak{m}^2$, so it can be generated by $d-1$ elements. By Nakayama's lemma, $\mathfrak{n}$ can be generated by $d-1$ elements, so S is regular of dimension $d-1$. By induction, S is a domain; that is $\langle x\rangle$ is a prime ideal. Since we chose x outside the minimal primes, $\langle x\rangle$ is not a minimal prime of R. Thus $\langle x\rangle$ contains some minimal prime ideal $\mathfrak{p}$ of R.

We claim that $\mathfrak{p}=0$ (which will imply that R is a domain). Indeed, if $y\in\mathfrak{p}$ is any element, then we may write $y=rx$ for some $r\in R$. Since x is not in $\mathfrak{p}$, we must have $r\in\mathfrak{p}$. This shows that $\mathfrak{p}=x\mathfrak{p}$. It follows by Nakayama's lemma $\mathfrak{p}=0$, and R is a domain as required. □

Corollary 20. *Suppose R is a regular local ring and let $\boldsymbol{x} = x_1,\dots,x_d$ be a system of parameters for R. Then $\boldsymbol{x}$ is an R-sequence contained in $\mathfrak{m}$.*

Proof. For each $1\le i\le d$, observe that $R/\langle x_1,\dots,x_i\rangle$ is a regular local ring. Indeed set $\overline{R} = R/\langle x_1,\dots,x_i\rangle$ and set $\overline{\mathfrak{m}} = \mathfrak{m}\overline{R}$. Then since $\mathfrak{m} = \langle x_1,\dots,x_d\rangle$, we clearly have $\overline{\mathfrak{m}} = \langle \overline{x}_{i+1},\dots,\overline{x}_d\rangle$. In particular, $\dim \overline{R} = d-i$ since $\overline{x}_{i+1},\dots,\overline{x}_d$ is a system of parameters for $\overline{R}$. It follows that $\overline{R}$ is a regular local ring, hence it is an integral domain by Proposition (19.1). Since $R/\langle x_1,\dots,x_i\rangle$ is an integral domain for all $1\le i\le d$, it follows that $\boldsymbol{x}$ is an R-sequence. □

19.0.1 Jacobian Criterion

The following theorem gives a criterion to help us determine when finitely generated $\Bbbk$-algebras are regular.

Theorem 19.1. *Let $R = \Bbbk[x_1, \dots, x_n] = \Bbbk[\boldsymbol{x}]$, let $\mathfrak{m} = \langle x_1, \dots, x_n \rangle$, let $\boldsymbol{f} = f_1, \dots, f_m$ be a sequence of polynomials in R, and let $A = R_{\mathfrak{m}}/\boldsymbol{f}$. Set $\mathrm{J}_{\boldsymbol{f}} = (\partial_{x_j} f_i)$ to be the Jacobian matrix of $\boldsymbol{f}$:*

$$\mathrm{J}_{\boldsymbol{f}} = \mathrm{J}_{\boldsymbol{f}}(\boldsymbol{x}) = \begin{pmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_n} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_m & \cdots & \partial_{x_n} f_m \end{pmatrix}.$$

Set $e = \operatorname{edim} A$ and set $r = \operatorname{rank} \mathrm{J}_{\boldsymbol{f}}(0)$. Then

$$e = n - r.$$

In particular, if $r = m \leq n$, then A is a regular local ring.

Proof. Let $\mathfrak{n}$ be the maximal ideal of A. We have

$$\begin{aligned} \operatorname{edim} A &= \dim_{\Bbbk}(\mathfrak{n}/\mathfrak{n}^2) \\ &= \dim_{\Bbbk}((\mathfrak{m}/\boldsymbol{f})/(\mathfrak{m}^2 + \boldsymbol{f})/\boldsymbol{f})) \\ &= \dim_{\Bbbk}(\mathfrak{m}/(\mathfrak{m}^2 + \boldsymbol{f})) \\ &= \dim_{\Bbbk}((\mathfrak{m}/\mathfrak{m}^2)/((\mathfrak{m}^2 + \boldsymbol{f})/\mathfrak{m}^2)) \\ &= \dim_{\Bbbk}(\mathfrak{m}/\mathfrak{m}^2) - \dim_{\Bbbk}((\mathfrak{m}^2 + \boldsymbol{f})/\mathfrak{m}^2) \\ &= n - \dim_{\Bbbk}((\mathfrak{m}^2 + \boldsymbol{f})/\mathfrak{m}^2). \end{aligned}$$

The last dimension is equal to the number of linearly independent linear forms among the f_i mod $\mathfrak{m}^2$. This is equal to $\operatorname{rank} \mathrm{J}_{\boldsymbol{f}}(0)$. Indeed, for each $1 \leq i \leq m$, we break up f_i into a sum of its homogeneous pieces:

$$f_i = f_{i,0} + f_{i,1} + \cdots + f_{i,d_i},$$

where $f_{i,j}$ is the degree j part of f_i (in particular note that $f_{i,0} = f_i(0) = 0$ since $f_i \in \mathfrak{m}$). The $f_{i,1}$ are the linear forms of the f_i (i.e. the components of degree 1). Write

$$f_{i,1} = c_{i,1}x_1 + c_{i,2}x_2 + \cdots + c_{i,n}x_n$$

where $c_{i,j} \in \Bbbk$. Then note that

$$\mathrm{J}_{\boldsymbol{f}}(0) = \begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{m,1} & \cdots & c_{m,n} \end{pmatrix}.$$

Then the rank of $\mathrm{J}_{\boldsymbol{f}}(\mathbf{0})$ is precisely equal ot the number of linearly independent forms among the f_i mod $\mathfrak{m}^2$. For the last part of the theorem, set $d = \dim A$ and note that

$$\begin{aligned} d &\geq n - m \\ &= n - r \\ &= e \\ &\geq d. \end{aligned}$$

It follows that $d = e$ and hence A is regular. □

19.0.2 Associated Graded Ring

Proposition 19.2. *Let $(R, \mathfrak{m}, \Bbbk)$ be a local ring of dimension d. Equip R with the $\mathfrak{m}$-adic filtration $R = (\mathfrak{m}^n)$. The following conditions are equivalent:*

1. $\operatorname{gr} R = \Bbbk[t_1, \dots, t_d]$ *is a polynomial ring in d variables;*

2. *R is regular of dimension d.*

3. $\mathfrak{m}$ *can be generated by d elements.*

Proposition 19.3. *Let $(R, \mathfrak{m}, \Bbbk)$ be a local noetherian ring of dimension d such that R is equicharacteristic. Equip R with the $\mathfrak{m}$-adic filtration $R = (\mathfrak{m}^n)$. Then R is regular if and only if its completion is a formal power series ring over a field.*

Proof. We may assume that $\Bbbk \subseteq R$. Let $G = \operatorname{gr} R$ be the associated graded ring of R. Equip G with its canonical filtration $G = (G_{\geq n})$. In particular,

$$G/G_{\geq n} = \Bbbk \oplus (\mathfrak{m}/\mathfrak{m}^2) \oplus \cdots \oplus (\mathfrak{m}^{n-1}/\mathfrak{m}^n) \simeq R/\mathfrak{m}^n,$$

where the isomorphism holds as $\Bbbk$-vector spaces. The key point is that R is regular if and only if

$$\Bbbk[\boldsymbol{t}]_{\leq(n-1)} = G/G_{\geq n} \simeq R/\mathfrak{m}^n$$

holds as R-algebras. In particular, we have $\Bbbk[\![\boldsymbol{t}]\!] = \widehat{G} = \widehat{R}$. $\square$

In mixed characteristic, and R is a regular local ring, then its completion may be of the form $\widehat{R} = V[\![\boldsymbol{t}]\!] = V[\![t_1, \dots, t_d]\!]$ where $V = (V, p)$ is a discrete valuation domain. However there is a frequently more difficult ramified case where the ring has the form $V[\![\boldsymbol{t}]\!]/\langle p - F\rangle$ where F is in the square of the maximal ideal $\langle p, \boldsymbol{t}\rangle$. Such a ring, in general, is regular but *not* a formal power series ring over a discrete valuation domain. For a specific example of this type, consider

$$V[\![x, y, z]\!]/\langle p - x^3 - y^5 - z^7\rangle.$$

Serre proved that if R is regular local and its completion is a formal series over a field or discrete valuation domain, then the following hold for all finitely generated nonzero R-modules M and N such that $\ell(M \otimes_R N) < \infty$:

1. (dimension inequality) $\dim M + \dim N \leq \dim R$;
2. (vanishing) if $\dim M + \dim N < \dim R$, then $\chi(M, N) = 0$;
3. (positivity) if $\dim M + \dim N = \dim R$, then $\chi(M, N) > 0$.

Serre also proved (1) in general and conjecture that (2) and (3) hold in general as well. The remaining case is the ramified case in mixed characteristic. Serre also proved the case when either M or N is a complete intersection (i.e. of the form $R/\langle \boldsymbol{r}\rangle$ where $\boldsymbol{r} = r_1, \dots, r_m$ is a regular sequence). Indeed, in that case we have

$$\operatorname{Tor}^R(R/\boldsymbol{r}, N) = \mathrm{H}(\boldsymbol{r}, N),$$

where $\mathrm{H}(\boldsymbol{r}, N)$ is the Koszul homlogy, and he showed how to calculate intersection multiplicities in terms of the alternating sums of lengths of Koszul homologies.

19.0.3 Regular Local Rings are UFDs

In this subsection we wish to prove that regular local rings are unique factorization domains. We begin with a lemma. Recall that if R is an integral domain, then R is a PID if and only if every prime ideal is principal (one can then use this to show that R is a PID if and only if every ideal is principal). Thus to check if an integral domain R is a PID, it suffices to check a certain condition holds for all primes $\mathfrak{p}$ of R. If R is a *noetherian* domain, then there is the following analog of checking if R is a UFD:

Lemma 19.2. *Let R be a noetherian domain. Then R is a UFD if and only if every height 1 prime ideal of R is principal.*

Remark 34. Recall that R is a UFD if and only if every irreducible element in R is a prime element. We will use characterization of UFDs in the proof below.

Proof. Assume R is a UFD and let $\mathfrak{p}$ be a height 1 prime ideal of R. Choose a nonzero $x \in \mathfrak{p}$ and let $x = \pi_1 \cdots \pi_n$ be a factorization of x into irreducibles. Since $\mathfrak{p}$ is prime, we see that $\pi_i \in \mathfrak{p}$ for some i. Since R is a UFD, we see that $\langle \pi_i\rangle$ is a prime ideal. Since $\mathfrak{p}$ has height 1 and $\mathfrak{p} \supseteq \langle \pi_i\rangle$, we must have $\mathfrak{p} = \langle \pi_i\rangle$.

Conversely, assume that every height 1 prime ideal is principal. Since R is noetherian, every nonzero nonunit element can be factored into irreducibles, so it suffices to prove that an irreducible element π is prime. Let $\mathfrak{p}$ be a prime ideal of R which is minimal over $\langle \pi\rangle$. Then $\mathfrak{p}$ has height 1 by Krull's principal ideal theorem, thus $\mathfrak{p} = \langle x\rangle$ for some nonzero nonunit $x \in R$. Hence $\pi = xy$ and y is a unit as π is irreducible and x is a nonzero nonunit. Thus $\langle \pi\rangle = \mathfrak{p}$ which implies π is prime. $\square$

We need another lemma, but in order to state it we need to explain what *invertible* modules are:

Definition 19.2. Let R be a ring. An R-module M is called **invertible** if the functor

$$M \otimes_R - \colon \mathbf{Mod}_R \to \mathbf{Mod}_R$$

given by $N \mapsto M \otimes_R N$ is an equivalence of categories. An invertible R-module is said to be **trivial** if it is isomorphic to R as an R-module.

Lemma 19.3. *Let M be an R-module. The following are equivalent:*

1. *M is finite locally free module of rank 1,*
2. *M is invertible,*
3. *there exists an R-module N such that $M \otimes_R N \cong R$ (in which case, we must have $N \cong \mathrm{Hom}_R(M, R) := M^\star$).*

The set of isomorphism classes of these modules is called the **class group** or **Picard group** of R, denoted $\mathrm{Pic}\, R$. The group structure is determined by assigning to the isomorphism classes of the invertible modules L and L' the isomorphism class of $L \otimes_R L'$. The inverse of an invertible module L is the module $L^{\otimes -1} := \mathrm{Hom}_R(L, R)$.

Lemma 19.4. *Let R be a regular local ring and let $x \in R$. Then $\mathrm{Pic}(R_x) = 0$.*

Proof. Let L be an invertible R_x-module. In particular, L is a finite R_x-module, thus there exists a finite R-module M such that $M_x \cong L$. Since R is regular, there exists a finite free resolution F of M over R. Thus F_x is a finite free resolution of $M_x \cong L$ over R_x. It follows that $[L] = n[R_x]$ in $\mathrm{K}_0(R)$ for some $n \in \mathbb{Z}$. Now apply the map $\det\colon \mathrm{K}_0(R_x) \to \mathrm{Pic}(R_x)$ given by $[L] \mapsto \wedge^n(L) := \det L$. □

Proposition 19.4. *A regular local ring is a UFD.*

19.1 K-groups

Let R be a ring. In this subsection, we introduce two abelian groups denoted $\mathrm{K}_0'(R)$ and $\mathrm{K}_0(R)$. First we construction $\mathrm{K}_0'(R)$. Let $A' = \mathbb{Z}[\Sigma']$ where

$$\Sigma' = \{\{R^n/K\} \mid n \geq 0 \text{ and } K \text{ is an } R\text{-submodule of } R^n\}.$$

In particular A' is an abelian group consisting of all finite $\mathbb{Z}$-linear combinations of elements of the for $[R^n/K]$. Next let B' be the subgroup of A' generated by elements of the form

$$\{R^{n_2}/K_2\} - \{R^{n_1}/K_1\} - \{R^{n_3}/K_3\}$$

such that there exists a short exact sequence of the form

$$0 \longrightarrow R^{n_1}/K_1 \longrightarrow R^{n_2}/K_2 \longrightarrow R^{n_3}/K_3 \longrightarrow 0 \tag{58}$$

We set $\mathrm{K}_0'(R) := A'/B'$ and call this the 0**th** K'**-group** of R. The image of $\{R^n/K\}$ in $\mathrm{K}_0'(R)$ is denoted $[R^n/K]$. For each finite R-module M, we set $[M] = [R^n/K]$ where $R^n/K \cong M$. Note that this is well-defined for if $R^n/K \cong R^{n'}/K'$, then the short exact sequence

$$0 \longrightarrow 0 \longrightarrow R^n/K \longrightarrow R^{n'}/K' \longrightarrow 0 \tag{59}$$

tells us that $[R^n/K] = [R^{n'}/K']$. Thus we can consider $\mathrm{K}_0'(R)$ as the free abelian group generated by elements of the form $[M]$ where M is a finite R-module modulo relations of the form $[M_2] = [M_1] + [M_3]$ whenever we have a short exact sequence of the form

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{60}$$

The reason why we didn't let Σ be the collection of all finite R-modules to start with is because that doesn't form a set; it's a proper class.

Remark 35. Note that $[M \oplus N] = [M] + [N]$ since we have the short exact sequence

$$0 \longrightarrow M \longrightarrow M \oplus N \longrightarrow N \longrightarrow 0 \tag{61}$$

We can define a multiplication on $K_0'(R)$ by setting

$$[M][N] := [M \otimes_R N].$$

This is well-defined since if $M \cong M'$ and $N \cong N$, then $M \otimes_R N \cong M' \otimes_R N'$. This gives $K_0'(R)$ the structure of a ring since

$$\begin{aligned}
[M_1]([M_2] + [M_3]) &= [M_1][M_2 \oplus M_3] \\
&= [M_1 \otimes_R (M_2 \oplus M_3)] \\
&= [(M_1 \otimes_R M_2) \oplus (M_1 \otimes_R M_3)] \\
&= [M_1 \otimes_R M_2] + [M_1 \otimes_R M_3] \\
&= [M_1][M_2] + [M_1][M_3],
\end{aligned}$$

and similarly we have right distributivity as well. The identity element then is clearly $[R]$ since $R \otimes_R M \cong M$. Also this is clearly a commutative ring since $M \otimes_R N \cong N \otimes_R M$.

Lemma 19.5. *Assume R is an Artinian. Then the length function defines a natural abelian group homomorphism $\ell_R \colon K_0'(R) \to \mathbb{Z}$ given by*

$$\ell_R([M]) = \ell_R(M)$$

for all finite R-modules M.

Proof. Note that ℓ_R is well-defined since length is constant on isomorphism classes. Furthermore, the length of any finite R-module is finite since every finite R-module is a quotient of R^n which has finite length. Finally note that this is a homomorphism because the length function is additive on short exact sequences. □

Now we construct $K_0(R)$. Let $A = \mathbb{Z}[\Sigma]$ where

$$\Sigma = \{\{R^n/Q\} \mid n \geq 0 \text{ and } Q \text{ is a (necessarily finite) projective } R\text{-submodule of } R^n\}.$$

Next let B be the subgroup of A generated by elements of the form

$$\{R^{n_2}/Q_2\} - \{R^{n_1}/Q_1\} - \{R^{n_3}/Q_3\}$$

where the Q_i are projective R-submodules of R^{n_i} for each i such that there exists a short exact sequence of the form

$$0 \longrightarrow R^{n_1}/K_1 \longrightarrow R^{n_2}/K_2 \longrightarrow R^{n_3}/K_3 \longrightarrow 0 \tag{62}$$

We set $K_0(R) := A/B$ and call this the 0**th K-group** of R. The image of $\{R^n/K\}$ in $K_0(R)$ is denoted $[R^n/K]$. For each finite projective R-module P, we set $[P] = [R^n/Q]$ where $R^n/Q \cong P$. Thus we can consider $K_0(R)$ as the free abelian group generated by elements of the form $[P]$ where P is a finite projective R-module modulo relations of the form $[P_2] = [P_1] + [P_3]$ whenever we have a short exact sequence of the form

$$0 \longrightarrow P_1 \longrightarrow P_2 \longrightarrow P_3 \longrightarrow 0 \tag{63}$$

Remark 36. Observe that if

$$0 \longrightarrow P_1 \longrightarrow P_2 \longrightarrow P_3 \longrightarrow P_4 \longrightarrow 0 \tag{64}$$

is an exact sequence of projective R-module, then it breaks up into two exact sequences of projective R-modules:

$$0 \longrightarrow P_1 \longrightarrow P_2 \longrightarrow Q \longrightarrow 0 \qquad \text{and} \qquad 0 \longrightarrow Q \longrightarrow P_3 \longrightarrow P_4 \longrightarrow 0 \tag{65}$$

Thus we have

$$\begin{aligned}
[P_4] - [P_3] + [P_2] - [P_1] &= [P_4] - [P_3] + [P_2] - [P_1] + [Q] - [Q] \\
&= ([P_4] - [P_3] - [Q]) - ([P_2] - [P_1] - [Q]) \\
&= 0.
\end{aligned}$$

More generally, if P is an exact R-complex consisting of projective R-modules which has finite length, then we have $\sum_i (-1)^i [P_i] = 0$.

Note that we have an obvious map $K_0(R) \to K_0'(R)$ which in general is not an isomorphism.

Example 19.1. Let $\Bbbk$ be a field. Then $\mathrm{K}_0(\Bbbk) = \mathrm{K}'_0(\Bbbk) \cong \mathbb{Z}$ with the isomorphism given by the dimension function (which is also the length function).

Proposition 19.5. *Let R be a PID. Then $\mathrm{K}_0(R) = \mathrm{K}'_0(R) = \mathbb{Z}$.*

Proof. Let M be a finite R-module. By the structure theorem of finite modules over a PID, we see that M has the form $M \cong R^m \oplus M_{\mathrm{tor}}$ where $r \geq 0$ and where M_{tor} is the torsion-part of M. The torsion part can be presented using a short exact sequence of the form

$$0 \longrightarrow R^n \longrightarrow R^n \longrightarrow M_{\mathrm{tor}} \longrightarrow 0 \tag{66}$$

thus

$$\begin{aligned}[M] &= [R^m] \oplus [M_{\mathrm{tor}}] \\ &= [R^m] \\ &= m[R].\end{aligned}$$

It is straightforward to see that this point that $\mathrm{K}_0(R) = \mathrm{K}'_0(R)$ and that the isomorphism $\mathrm{K}'_0(R) \to \mathbb{Z}$ is given by $[M] \mapsto \operatorname{rank} M$. □

Example 19.2. Let $R = \Bbbk[x]$ where $\Bbbk$ is a field. Then R is a PID, thus $\mathrm{K}_0(R) = \mathrm{K}'_0(R) \cong \mathbb{Z}$.

Proposition 19.6. *Let $(R, \mathfrak{m}, \Bbbk)$ be a local ring. The map $\operatorname{rank}_R \colon \mathrm{K}_0(R) \to \mathbb{Z}$ defined by $[P] \mapsto \operatorname{rank} P$ is an isomorphism.*

Proof. This follows from the fact that every finite projective R-module is free. □

Proposition 19.7. *There is a map $c \colon \{\text{perfect } R\text{-complexes}\} \to \mathrm{K}_0(R)$ with the following properties:*

1. *$c(A[n]) = (-1)^n c(A)$*
2. *if $A \to B \to C \to A[1]$ is a distinguished triangle of perfect complexes, then $c(B) = c(A) + c(C)$.*
3. *if A is quasiisomorphic to a finite complex P consisting of finite projective modules, then $c(A) = \sum (-1)^i [P_i]$.*

Proof. Let A be a perfect object in $\mathrm{D}(R)$. Thus we can represent A by a finite complex P of finite projective R-modules. We define c by setting

$$c(A) = \sum (-1)^i [P_i]$$

in $\mathrm{K}_0(R)$. To see that this is well-defined, suppose $Q \to P$ is a surjective map of finite complexes of finite projective R-modules and let K be the kernel. Then the short exact sequence

$$0 \longrightarrow K \longrightarrow Q \longrightarrow P \longrightarrow 0 \tag{67}$$

of graded R-modules splits since each P_i is projective. Therefore K is a finite complex consisting of finite projective R-modules and

$$c(Q) = c(L) + (P)$$

in $\mathrm{K}_0(R)$. Now suppose X is a finite complex consisting of finite projective R-modules such that X is acyclic. Setting $Z = \ker \mathrm{d}_X$, we see that we have short exact sequences

$$0 \longrightarrow Z \longrightarrow X \longrightarrow \Sigma Z \longrightarrow 0 \tag{68}$$

of graded R-modules. Note this automatically implies Z consists of finite projective R-modules, thus

$$\begin{aligned}c(X) &= \sum (-1)^i [X_i] \\ &= \sum (-1)^i ([Z_i] - [Z_{i-1}]) \\ &= 0.\end{aligned}$$

This shows that our construction is zero on acyclic complexes. It follows that c is well-defined and satisfies property (2). In particular, suppose P and Q are finite semiprojective R-complexes which represent the same object of $\mathrm{D}(R)$. Then we can represent the isomorphism by a map $\varphi \colon P \to Q$ of complexes. We obtain a short exact sequence of complexes

$$0 \longrightarrow Q \longrightarrow Q + eP \longrightarrow P \longrightarrow 0 \tag{69}$$

. Since φ is a quasi-isomorphism, the mapping cone $Q + eP$ is acyclic. Thus

$$\begin{aligned}0 &= c(Q + eP) \\ &= c(Q) + c(\Sigma P) \\ &= c(Q) - c(P).\end{aligned}$$

□

Lemma 19.6. *Let R be a ring and let*

$$0 \longrightarrow P_1 \longrightarrow P_2 \longrightarrow P_3 \longrightarrow 0 \tag{70}$$

be a short exact sequence of finite projective R-modules. Then there is a canonical isomorphism

$$\det\colon \det(P_1) \otimes \det(P_3) \to \det(P_2).$$

Proof. Consider the R-algebra maps $\wedge(P_1) \to \wedge(P_2)$ and $\wedge(P_2) \to \wedge(P_3)$. The first is injective and the second is surjective. Take an element $x \in \det P_1$ and an element $z \in \det P_3$. Choose $y \in \det P_2$ mapping to z and set

$$\gamma(x \otimes z) = x \wedge y \in \det P_2.$$

One checks that this is an isomorphism by localizing at primes. □

Proposition 19.8. *Let R be a ring. There is a map $\det\colon \mathrm{K}_0(R) \to \mathrm{Pic}(R)$ which sends $[P]$ to the class of the invertible module $\wedge^n P$ if P is finite locally free of rank n.*

Remark 37. Let A be a DVR. Recall that if $a, b \in A$, then we have the following inequalities

$$\begin{aligned} \nu(a) &\geq \min\{\nu(a+b), \nu(b)\} \\ \nu(a+b) &\geq \min\{\nu(a), \nu(b)\} \\ \nu(b) &\geq \min\{\nu(a), \nu(a+b)\}. \end{aligned}$$

On the other hand, if R is a local noetherian ring and

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{71}$$

is a short exact sequence of finitely generated R-modules with depths δ_1, δ_2, and δ_3 respectively, then we have the following inequalities

$$\begin{aligned} \delta_1 &\geq \min\{\delta_2, \delta_3 + 1\} \\ \delta_2 &\geq \min\{\delta_1, \delta_3\} \\ \delta_3 &\geq \min\{\delta_1 - 1, \delta_2\}. \end{aligned}$$

So it's almost the same, but you get these plus and minus ones which ultimately come from the fact that the connecting map for Ext shifts homological degree up by one. Another thing is that if $R \to R'$ is a flat local ring homomorphism of local noetherian rings, and if M and M' are finitely generated modules over R and R' respectively, then we have

$$\mathrm{depth}_{R'}(M \otimes_R M') = \mathrm{depth}_R(M) + \mathrm{depth}_{R'}(M'/\mathfrak{m}M').$$

This is analogous to the identity

$$\nu(ab) = \nu(a) + \nu(b).$$

So even here it's not quite the same either but there is an interesting analogy going on nonetheless.

20 Complete Intersections

21 Normal Rings

Lemma 21.1. *Let $\mathfrak{p} = 0 : e$ be an embedded prime of A. Then we must have $e^2 = 0$. In particular, if A is reduced then A has no embedded primes.*

Proof. Observe that $\mathfrak{p}e = 0$ is contained in every minimal prime of A. Since $\mathfrak{p}$ is embedded, it is not contained in any minimal prime of A, thus e must belong to every minimal prime of A. In other words, e must be nilpotent. In fact, since e belongs to every minimal prime of A, we have in particular $e \in \mathfrak{p}$, which implies $e^2 = 0$. □

Definition 21.1. Let A be a ring. We say A is **normal** if $A_{\mathfrak{p}}$ is an integrally closed domain for all primes $\mathfrak{p}$ of A.

Remark 38. In particular, a normal ring is necessarily reduced.

Lemma 21.2. *Let A be a reduced ring which has finitely many minimal primes. Then the following are equivalent:*

1. *A is a normal ring.*
2. *A is integrally closed in its total ring of fractions.*
3. *A is a finite product of normal domains.*

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the minimal primes of A, let S be the set of all regular elements of A, and let $K = A_S$ be the total quotient right of A. Since A has no embedded no embedded primes, we see that K no embedded primes either. In particular, each $\mathfrak{p}_{i,S}$ is a maximal ideal of K and we have

$$K = K_1 \times \cdots \times K_n$$

where $K_i := K_{\mathfrak{p}_i} = A_{\mathfrak{p}_i} = \kappa(\mathfrak{p}_i)$ is a field (here we are using the assumption that A is reduced as well as the fact that $\mathfrak{p}_i$ is a minimal prime of A to conclude that $A_{\mathfrak{p}_i} = \kappa(\mathfrak{p}_i)$). Let $e_i = (0, \dots, 1, \dots, 0)$ be the ith idempotent of K. If A is integrally closed in K, then it contains the idempotents e_i (since this is a root of the monic polynomial $x^2 - x$). Note that $e_i \in \mathfrak{p}_i$ and $1 - e_i \in \mathfrak{p}_j$ for all $i \neq j$ and so by the Chinese remainder theorem, we see that A is a product of n domains:

$$A = A_1 \times \cdots \times A_n$$

where $A_i := A/\mathfrak{p}_i$ has field of fractions K_i. Furthermore, each map $A_i \to K_i$ is integrally closed. Hence A is a finite product of normal domains. □

Remark 39. In particular, if $\operatorname{Spec} A$ is noetherian, normal, and connected, then A is an integrally closed domain.

Definition 21.2. Let A be a noetherian domain. We say A is a **Dedekind domain** if it is normal and has dimension ≤ 1.

21.1 Serre's criterion

Proposition 21.1. *Let A be a noetherian ring. Then A is normal if and only if it satisfies the following: for any prime $\mathfrak{p}$ of A*

1. *if $\mathfrak{p}$ has height ≤ 1, then $A_{\mathfrak{p}}$ is regular (i.e. $A_{\mathfrak{p}}$ is a discrete valuation ring).*
2. *if $\mathfrak{p}$ has height ≥ 2, then $A_{\mathfrak{p}}$ has depth ≥ 2.*

Proof. Assume A satisfies (1) and (2) for all primes $\mathfrak{p}$ of A. Note that (1) implies A is reduced. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ be the minimal primes of A. Then the total ring of fractions K of A is a direct product of fields:

$$K = K_1 \times \cdots \times K_k$$

where $K_i := A_{\mathfrak{p}_i} = \kappa(\mathfrak{p}_i)$ is a field for all i. If A is integrally closed in K, then A is a direct product of domains

$$A = A_1 \times \cdots \times A_k$$

where $A_i := A/\mathfrak{p}_i$ is integrally closed in its field of fractions K_i for all i. Thus it suffices to show that A is integrally closed in K. To this end, suppose that

$$(a/s)^m + b_{m-1}(a/s)^{m-1} + \cdots + b_0 = 0$$

where $a, b_i, s \in A$ for all i and s is regular. We want to show $a \in \langle s \rangle$. Let

$$\langle s \rangle = Q_1 \cap \cdots \cap Q_n$$

be an irredundant primary decomposition of $\langle s \rangle$ with $\mathfrak{q}_i = \sqrt{Q_i}$ being the associated primes of A/s. To show $a \in \langle s \rangle$, it suffices to show $a \in Q_i$ for each i. Note that condition (2) says each $\mathfrak{q}_i$ has height one. Indeed, if $\mathfrak{q}_i$ has height ≥ 2, then depth $A_{\mathfrak{q}_i} \geq 2$ implies $\mathfrak{q}_i$ contains an A/s-regular element, say $s' \in \mathfrak{q}_i$. However $\mathfrak{q}_i = s : x$ for some $x \in A \backslash \langle s \rangle$ which in particular implies s' is a zerodivisor on A/s. Next note that condition (1) implies $A_{\mathfrak{q}_i}$ is integrally closed and so $a/1 \in sA_{\mathfrak{q}_i} \subseteq Q_{i,\mathfrak{q}_i}$. It follows that $a \in \rho^{-1}(Q_{i,\mathfrak{q}_i}) = Q_i$.

Conversely, suppose that A is a normal ring. We first show (2) holds. Let $\mathfrak{q}$ be an associated prime of A/s where s is a nonzerodivisor. We need to show $\mathfrak{q}$ has height one. Replacing A by a localization if necessary, we may assume that $(A, \mathfrak{q})$ is a local ring. By definition, there exists an $x \in A \backslash \langle s \rangle$ such that $\mathfrak{q} = s : x$. Let $\alpha = x/s$ in K. If $\alpha\mathfrak{q} \subseteq \mathfrak{q}$, then $\mathfrak{q}$ is a faithful $A[\alpha]$-module and is a finitely generated A-module, thus α is integral over A and thus in A, a contradiction. hence $\alpha\mathfrak{q} = A$ or $\mathfrak{q} = \alpha^{-1}A$, which implies $\mathfrak{q}$ has height one by Krull's principal ideal theorem. To show (1), let $\mathfrak{q}$ be a prime ideal of height one. Localizing at $\mathfrak{q}$ if necessary, we may assume $\mathfrak{q}$ is a maximal ideal and the similar argument as above shows that $\mathfrak{q}$ is in fact principal. Thus A is a regular local ring. □

Proposition 21.2. *Let R be a noetherian ring, let I be an ideal of R, and let M be a finitely generated R-module. Then*

$$\operatorname{depth}(I, M) = \inf_{\mathfrak{p} \in \mathrm{V}(I)} \{\operatorname{depth} M_{\mathfrak{p}}\}.$$

In particular, if $\boldsymbol{x} = x_1, \dots, x_\delta$ is a maximal M-sequence contained in I and $\mathfrak{p} \in \mathrm{V}(I)$ is an associated prime of $M/\boldsymbol{x}$, then $\operatorname{depth}(I, M) = \operatorname{depth} M_{\mathfrak{p}}$.

Proof. If $\mathfrak{p}$ is any prime that contains I, then we have

$$\operatorname{depth}(I, M) \leq \operatorname{depth}(\mathfrak{p}, M) \leq \operatorname{depth} M_{\mathfrak{p}}.$$

For the converse direction, let $\boldsymbol{x}$ be a maximal M-sequence contained in I. Then I consists of zerodivisors on $M/\boldsymbol{x}$ which implies there exists an associated prime $\mathfrak{p}$ of $M/\boldsymbol{x}$ such that $\mathfrak{p} \in \mathrm{V}(I)$ (here we are using the assumption that R is noetherian and M is finitely generated). Then $\mathfrak{p}_{\mathfrak{p}}$ is an associated prime of $M_{\mathfrak{p}}/\boldsymbol{x}$ which means $\mathfrak{p}_{\mathfrak{p}}$ consists of zerodivisors on $M_{\mathfrak{p}}/\boldsymbol{x}$. However this in turn implies $\operatorname{depth} M_{\mathfrak{p}} = \operatorname{depth}(I, M)$. □

Corollary 21. *Let R be a noetherian ring and let $\mathfrak{p}$ be a prime ideal of R. Then*

$$\operatorname{depth}(\mathfrak{p}, R) = \operatorname{depth} R_{\mathfrak{p}}.$$

Proof. Note that if $\boldsymbol{x} = x_1, \dots, x_\delta$ be a maximal regular sequence contained in $\mathfrak{p}$, then $\mathfrak{p}$ is an associated prime of $R/\boldsymbol{x}$. Indeed, if it weren't, then by prime avoidance, we could choose an $x \in \mathfrak{p}$ which avoid all associated primes of $R/\boldsymbol{x}$, and then $x_1, \dots, x_\delta, x$ would be a regular sequence contained in $\mathfrak{p}$ of length $\delta + 1$, which is a contradiction. □

22 Henselian Rings

Let $(A, \mathfrak{m})$ be a local ring and let $A \to B$ be an integral injective ring homomorphism which makes B a finite A-algebra. Then B has finitely many maximal ideals, say $\mathfrak{n}_1, \dots, \mathfrak{n}_n$, all of which lie over $\mathfrak{m}$. Furthermore, note that B is a product of local rings if and only if the canonical homomorphism $B \to \prod_i B_{\mathfrak{n}_i}$ is an isomorphism.

Definition 22.1. A local ring A is called **henselian** if every finite A-algebra is a product of local rings.

Remark 40. Let A be a henselian local ring and let B be a finite local A-algebra. Then B is also henselian. Indeed, if C is a finite B-algebra, then it is in particular a finite A-algebra, and thus a product of local rings.

Example 22.1. Let $\mathbb{k}$ be a field. Then $\mathbb{k}$ is henselian since any finite $\mathbb{k}$-algebra is artinian, and hence a product of local artinian rings by the structure theorem on artinian rings.

Example 22.2. Let $(A, \mathfrak{m}, \mathbb{k})$ be a complete local ring. Then A is henselian.

Lemma 22.1. *Let A be a ring, let $f \in B := A[\boldsymbol{t}] = A[t_1, \dots, t_n]$ and call f **primitive** if the ideal of A generated by the coefficients of f is A.*

1. *If f is primitive, then f is B-regular and B/f is A-flat.*

2. *Assume $n = 1$. Then f is primitive if and only if $Y := \operatorname{Spec}(B/f) \to \operatorname{Spec} A := X$ is quasi-finite.*

Proof. The polynomial f is primitive if and only if the image of f in $\kappa(\mathfrak{p})[\boldsymbol{t}]$ is non-zero for all prime ideals $\mathfrak{p}$ of A. Therefore multiplication on f induced on fibers over $Y \to X$ is injective. As B is a flat A-algebra of finite presentation, it follows that multiplication by f on B is injective and has A-flat cokernel. Now assume $n = 1$. Clearly B is an algebra of finite type. We have

$$\begin{aligned} Y \to X \text{ is quasi-finite} &\iff \text{The fibers of } Y \to X \text{ are finite} \\ &\iff \kappa(\mathfrak{p})[\boldsymbol{t}]/f_{\mathfrak{p}} \text{ is finite } \kappa(\mathfrak{p})\text{-algebra for all } \mathfrak{p} \in X \\ &\iff f_{\mathfrak{p}} \neq 0 \text{ for all } \mathfrak{p} \in X. \end{aligned}$$

□

Part III
Field Theory

23 Definition of a Field

Definition 23.1. A **field** is a commutative ring with the property that every nonzero element is a unit.

Let K be a field. Observe that K is an integral domain. Indeed, if $a, b \in K$ with $a \neq 0$ and $ab = 0$, then

$$\begin{aligned} 0 &= a^{-1} \cdot 0 \\ &= a^{-1}ab \\ &= b. \end{aligned}$$

Conversely, any finite integral domain is automatically a field:

23.0.1 Finite Rings are Integral Domains if and only if they are Fields

Proposition 23.1. *Let R be a finite ring. Then R is an integral domain if and only if R is a field.*

Proof. One direction is clear, for the other direction, let a be a nonzero element in R. Since R is an integral domain, the multiplication by a map $\mathrm{m}_a \colon R \to R$ given by

$$\mathrm{m}_a(b) = ab$$

for all $b \in R$ is injective. Since R is finite and m_a is injective, the multiplication by a map must also be surjective. Thus there exists a $b \in R$ such that

$$\begin{aligned} 1 &= \mathrm{m}_a(b) \\ &= ab. \end{aligned}$$

Thus a is a unit. □

23.0.2 Integral Domains with Positive Characteristic must have Prime Characteristic

Proposition 23.2. *Let R be an integral domain. If* $\operatorname{char} R > 0$, *then* $\operatorname{char} R$ *is prime.*

Proof. Let us denote $n = \operatorname{char} R$. We will show that n is a prime. Assume for a contradiction that n is not a prime. Then there exists $1 < k, m < n$ such that

$$\begin{aligned} 0 &= n \cdot 1_R \\ &= (km) \cdot 1_R \\ &= (k \cdot 1_R)(m \cdot 1_R). \end{aligned}$$

Since $n = \operatorname{char} R$, we must have $(k \cdot 1_R) \neq 0$ and $(m \cdot 1_R) \neq 0$. But this contradicts the fact that R is an integral domain. □

Corollary 22. *Every finite field has prime characteristic.*

Proof. Every finite ring has positive characteristic and every field is an integral domain. Thus the corollary follows immediately from (25.2). □

23.0.3 Finite Subgroup of Multiplicative Group of Field is Cyclic

Lemma 23.1. *Let A be a finite abelian group. The order of every element must divide the maximal order.*

Proof. From the fundamental theorem of finite abelian groups, we have an isomorphism

$$A \cong \mathbb{Z}/k_1 \oplus \cdots \oplus \mathbb{Z}/k_n$$

where $k_1 \mid \cdots \mid k_n$. Let $e_1, \dots, e_n$ denote the standard $\mathbb{Z}$-basis for $\mathbb{Z}^n$, and let $\bar{e}_i$ denote the corresponding coset in $\mathbb{Z}_{k_i}$ for each $1 \leq i \leq n$. Since $k_i \mid k_n$ we see that k_n kills each $\mathbb{Z}/k_i$ for all $1 \leq i \leq n$. Therefore k_n kills all of A. In particular, the order of every element must divide k_n, which is in fact the maximal order as $k_n = \operatorname{ord}(\bar{e}_{i_n})$. □

Lemma 23.2. *The number of roots of a polynomial over a field is at most the degree of the polynomial.*

Proof. Let K be a field and let $f(T)$ be a polynomial coefficients in K. By replacing K with a splitting field of $f(T)$ if necessary, we may assume that $f(T)$ splits into linear factors over K, say

$$f(T) = (T - \alpha_1) \cdots (T - \alpha_n).$$

where $\alpha_1, \dots \alpha_n \in K$ and $n = \deg f(T)$. Let $\alpha \in K$. Then we have

$$\begin{aligned} f(\alpha) = 0 &\iff (\alpha - \alpha_1) \cdots (\alpha - \alpha_n) = 0 \\ &\iff \alpha - \alpha_i = 0 \text{ for some } i \\ &\iff \alpha = \alpha_i \text{ for some } i, \end{aligned}$$

where we obtained the second line from the first line from the fact that K is an integral domain. Therefore $f(T)$ has *at most* n roots. □

Proposition 23.3. *Let K be a field and let G be a finite subgroup of $K^\times$. Then G is cyclic.*

Proof. Let $n = |G|$ and let m be the maximal order among all elements in G. We will show $m = n$. By Lagrange's Theorem, we have $m \mid n$, and hence $m \leq n$. It follows from Lemma (80.1) that every order of every element must divide the maximal order. In particular, we have $x^m = 1$ for all $x \in G$. Therefore all numbers in G are roots of the polynomial $T^m - 1$. By Lemma (80.2), the number of roots of a polynomial over a field is at most the degree of the polynomial, so $n \leq m$. Combining both inequalities gives us $m = n$. □

23.0.4 Finite Fields have Prime Power Order

Theorem 23.3. *Let F be a finite field. Then F has prime power order.*

Proof. Let F be a finite field. Corollary (26) tells us that the characteristic of F is prime, denote it by $p = \operatorname{char} F$. Then $\mathbb{Z}/(p)$ embeds as a subring of F. In particular, we can view F as a finite-dimensional $\mathbb{Z}/(p)$-vector space. Letting $n = \dim_{\mathbb{Z}/(p)}(F)$ and picking a basis $\{e_1, \dots, e_n\}$ for F over $\mathbb{Z}/(p)$, elements of F can be written uniquely as

$$c_1 e_1 + \cdots + c_n e_n$$

where $c_i \in \mathbb{Z}(p)$ for all $1 \leq i \leq n$. Each coefficient has p choices, so $|F| = p^n$. □

23.0.5 Classification of Finite Fields

Theorem 23.4. *Every finite field is isomorphic to $\mathbb{F}_p[X]/(\pi(X))$ for some prime p and some monic irreducible $\pi(X)$ in $\mathbb{F}_p[X]$.*

Proof. Let F be a finite field. By Theorem (25.5), F has order p^n for some prime p and positive integer n, and there is a field embedding $\mathbb{F}_p \hookrightarrow F$. The group $F^\times$ is cyclic by Proposition (25.3). Let γ be a generator of $F^\times$. Evaluation at γ, namely $f(X) \mapsto f(\gamma)$, is a ring homomorphism $\mathrm{ev}_\gamma \colon \mathbb{F}_p[X] \to F$ that fixes $\mathbb{F}_p$. Since every number in F is 0 or a power of γ, ev_γ is onto ($0 = \mathrm{ev}_\gamma(0)$ and $\gamma^r = \mathrm{ev}_\gamma(X^r)$ for any $r \geq 0$). Therefore

$$\mathbb{F}_p[X]/\ker \mathrm{ev}_\gamma \cong F.$$

The kernel of ev_γ is a maximal ideal in $\mathbb{F}_p[X]$, so it must be $(\pi(X))$ for some monic irreducible $\pi(X)$ in $\mathbb{F}_p[X]$. □

24 Polynomials

24.1 Roots and Irreducibles

Definition 24.1. Let K be a field and let $f(X)$ be a polynomial in $K[X]$. A number $\alpha \in K$ is called a **root of** $f(X)$ if $f(\alpha) = 0$.

Proposition 24.1. *Let K be a field, let $f(X)$ be a nonconstant polynomial in $K[X]$, and let $\alpha \in K$. Then α is a root of $f(X)$ if and only if $X - \alpha$ divides $f(X)$.*

Proof. Suppose $X - \alpha$ divides $f(X)$. Then

$$f(X) = (X - \alpha)g(X) \tag{72}$$

for some $g(X) \in K[X]$. Substituting α for X in both sides of (72) gives us $f(\alpha) = 0$.

Conversely, suppose α is a root of $f(X)$. Since $K[X]$ is Euclidean domain and $\deg f(X) \geq 1$, there exists nonzero a nonzero polynomial $q(X)$ in $K[X]$ and a constant $r \in K$ such that

$$f(X) = (X - \alpha)q(X) + r \tag{73}$$

Substituting α for X in both sides of (73) gives us $r = 0$. In particular, $f(X) = (X - \alpha)q(X)$ and hence $X - \alpha$ divides $f(X)$. □

For most fields K, there are polynomials in $K[X]$ without a root in K (for instance consider $X^2 + 1$ in $\mathbb{R}[X]$). If we are willing to enlarge the field, then we can discover some roots. This is due to Kronecker, by the following argument.

Theorem 24.1. *Let K be a field and $f(X)$ be nonconstant in $K[X]$. There is a field extension of K containing a root of $f(X)$.*

Proof. Choose an irreducible polynomial $\pi(X)$ such that $\pi(X) \mid f(X)$. If L is an extension of K in which $\pi(\alpha) = 0$ for some $\alpha \in L$, then $f(\alpha) = 0$ too. Therefore it suffices to find a field extension of K in which $\pi(X)$ has a root. Set $L = K[X]/\langle\pi(X)\rangle$. Since $\pi(X)$ is irreducible in $K[X]$, L is a field. Inside of L we have K as a subfield: the congruence classes represented by constants. There is a also a root of $\pi(X)$ in L, namely the class of X. Indeed, writing $\overline{X}$ for the congruence class of X in L, the congruence $\pi(X) \equiv 0 \bmod \pi(X)$ becomes the equation $\pi(\overline{X}) = 0$ in L. ☐

By repeating the construction in the proof of Theorem (24.1) several times, we can always create a field with a full set of roots for our polynomial. We state this as a corollary, and give a proof by induction on the degree.

Corollary 23. *Let K be a field and $f(X) = c_m X^m + \cdots + c_0$ be in $K[X]$ with degree $m \geq 1$. There is a field $L \supset K$ such that in $L[X]$ we have*

$$f(X) = c_m(X - \alpha_1)\cdots(X - \alpha_m).$$

Proof. We induct on the degree m. The case $m = 1$ is clear, using $L = K$. By Theorem (24.1), there is a field $L \supset K$ such that $f(X)$ has a root in L, say α_1. Then in $L[X]$,

$$f(X) = (X - \alpha_1)g(X),$$

where $\deg g(X) = m - 1$. The leading coefficient of $g(X)$ is also c_m.

Since $g(X)$ has smaller degree than $f(X)$, by induction on the degree there is a field $E \supset L$ such that $g(X)$ decomposes into linear factors in $E[X]$, so we get the desired factorization of $f(X)$ in $E[X]$. ☐

Corollary 24. *Let $f(X)$ and $g(X)$ be nonconstant in $K[X]$. They are relatively prime in $K[X]$ if and only if they do not have a common root in any extension field of K.*

Proof. Assume $f(X)$ and $g(X)$ are relatively prime in $K[X]$. Then we can write

$$f(X)u(X) + g(X)v(X) = 1 \tag{74}$$

for some $u(X)$ and $v(X)$ in $K[X]$. If there were an α in a field extension of K which is a common root of $f(X)$ and $g(X)$, then substituting α for X in (74) makes the left side 0 while the right side 1. This is a contradiction, so $f(X)$ and $g(X)$ have no common root in any field extension of K.

Now assume $f(X)$ and $g(X)$ are not relatively prime in $K[X]$. Say $h(X) \in K[X]$ is a (nonconstant) common factor. There is a field extension of K in which $h(X)$ has a root, and this root will be a common root of $f(X)$ and $g(X)$. ☐

Although adjoining one root of an irreducible in $\mathbb{Q}[X]$ to the rational numbers does not always produce the other roots in the same field (such as with $X^3 - 2$), the situation in $\mathbb{F}_p[X]$ is much simpler. We will see later that for an irreducible in $\mathbb{F}_p[X]$, a larger field which contains one root must contain *all* the roots.

24.2 Divisibility and Roots in $K[X]$

It turns out that Proposition (24.1) can be improved as follows:

Theorem 24.2. *Let K be a field, let $\pi(X)$ be irreducible in $K[X]$, let α be a root of $\pi(X)$ in some larger field, and let $f(X)$ be a polynomial in $K[X]$. Then α is a root of $f(X)$ if and only if $\pi(X)$ divides $f(X)$.*

Proof. Suppose $\pi(X)$ divides $f(X)$. Then

$$f(X) = \pi(X)g(X) \tag{75}$$

for some $g(X) \in K[X]$. Substituting α for X in both sides of (75) gives us $f(\alpha) = 0$.

Conversely, suppose α is a root of $f(X)$. Then $f(X)$ and $\pi(X)$ have a common root, so by Corollary (24) they have a common factor in $K[X]$. Since $\pi(X)$ is irreducible, this means $\pi(X)$ divides $f(X)$ in $K[X]$. ☐

Example 24.1. Take $K = \mathbb{Q}$ and $\pi(X) = X^2 - 2$. It has a root $\sqrt{2} \in \mathbb{R}$. For any $h(X) \in \mathbb{Q}[X]$, we have $h(\sqrt{2}) = 0$ if and only if $(X^2 - 2) \mid h(X)$. This equivalence breaks down if we allow $h(X)$ to come from $\mathbb{R}[X]$: try $h(X) = X - \sqrt{2}$.

Theorem 24.3. *Let L/K be a field extension and let $f(X)$ and $g(X)$ be in $K[X]$. Then $f(X) \mid g(X)$ in $K[X]$ if and only if $f(X) \mid g(X)$ in $L[X]$.*

Proof. It is clear the divisibility in $K[X]$ implies divisibility in the larger $L[X]$. Conversely, suppose $f(X) \mid g(X)$ in $L[X]$. Then
$$g(X) = f(X)h(X)$$
for some $h(X) \in L[X]$. By the division algorithm in $K[X]$,
$$g(X) = f(X)q(X) + r(X),$$
where $q(X)$ and $r(X)$ are in $K[X]$ and $r(X) = 0$ or $\deg r < \deg f$. Comparing these two formulas for $g(X)$, the uniqueness of the division algorithm in $L[X]$ implies $q(X) = h(X)$ and $r(X) = 0$. Therefore $g(X) = f(X)q(X)$, so $f(X) \mid g(X)$ in $K[X]$. □

24.3 Raising to the pth Power in Characteristic p

Lemma 24.4. *Let A be a commutative ring with prime characteristic p. Pick any a and b in A. Then*

1. $(a+b)^p = a^p + b^p$.
2. *When A is a domain, $a^p = b^p$ implies*

Proof. 1. By the binomial theorem,
$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p.$$
For $1 \le k \le p-1$, the integer $\binom{p}{k}$ is a multiple of p, so the intermediate terms are 0 in A.

2. Suppose A is a domain and $a^p = b^p$. Then $0 = a^p - b^p = (a-b)^p$. Since A is a domain, $a - b = 0$, so $a = b$. □

Lemma 24.5. *Let F be a field containing $\mathbb{F}_p$. For $c \in F$, we have $c \in \mathbb{F}_p$ if and only if $c^p = c$.*

Proof. Every element c of $\mathbb{F}_p$ satisfies the equation $c^p = c$. Conversely, solutions to this equation are roots of $X^p - X$, which has at most p roots in F. The elements of $\mathbb{F}_p$ already fulfill this upper bound, so there are no further roots in characteristic p. □

Theorem 24.6. *For any $f(X) \in \mathbb{F}_p[X]$, we have $f(X)^{p^r} = f(X^{p^r})$ for $r \ge 0$. If F is a field of characteristic p other than $\mathbb{F}_p$, this is not always true in $F[X]$.*

Proof. Writing
$$f(X) = c_m X^m + c_{m-1} X^{m-1} + \cdots + c_0,$$
we have
$$\begin{aligned} f(X)^p &= (c_m X^m + c_{m-1} X^{m-1} + \cdots + c_0)^p \\ &= c_m^p X^{pm} + c_{m-1}^p X^{p(m-1)} + \cdots + c_0^p \\ &= c_m X^{pm} + c_{m-1} X^{p(m-1)} + \cdots + c_0 \\ &= f(X^p) \end{aligned}$$
since $c^p = c$ for any $c \in \mathbb{F}_p$. Applying this r times gives us $f(X)^{p^r} = f(X^{p^r})$.

If F has characteristic p and is not $\mathbb{F}_p$, then F contains an element c which is not in $\mathbb{F}_p$. Then $c^p \neq c$ by Lemma (24.5), so the constant polynomial $f(X) = c$ does not satisfy $f(X)^p = f(X^p)$.

□

Let $f(X) \in \mathbb{F}_p[X]$ be nonconstant, with degree m. Let $L \supseteq \mathbb{F}_p$ be a field over which $f(X)$ decomposes into linear factors. It is possible that some of the roots of $f(X)$ are multiple roots. As long as that does not happen, the following corollary says something about the pth power of the roots.

Corollary 25. *When $f(X) \in \mathbb{F}_p[X]$ has distinct roots, raising all roots of $f(X)$ to the pth power permutes the roots:*
$$\{\alpha_1^p, \ldots, \alpha_m^p\} = \{\alpha_1, \ldots, \alpha_m\}.$$

Proof. Let $S = \{\alpha_1, \ldots, \alpha_m\}$. Since $f(X^p) = f(X)^p$, the pth power of each root of $f(X)$ is again a root of $f(X)$. Therefore raising to the pth power defines a function $\varphi \colon S \to S$. This function is injective since the pth power map is injective, which implies the function is surjective since S is finite. □

24.4 Roots of Irreducibles in $\mathbb{F}_p[X]$

All the roots of an irreducible polynomial in $\mathbb{Q}[X]$ are not generally expressible in terms of a particular root, with $X^3 - 2$ being a typical example. (The field $\mathbb{Q}(\sqrt[3]{2})$ contains only one root to this polynomial, not all 3 roots.) However, the situation is markedly simpler over finite fields. In this section we will make explicit the relations among the roots of an irreducible polynomial in $\mathbb{F}_p[X]$. In short, we can obtain all roots from any one root by repeatedly taking pth powers.

Theorem 24.7. *Let p be a prime and let $\pi(X)$ be a monic irreducible polynomial in $\mathbb{F}_p[X]$ of degree n. Then the ring $\mathbb{F}_p[X]/\langle\pi(X)\rangle$ is a field of order p^n.*

Proof. The cosets mod $\pi(X)$ are represented by remainders

$$c_0 + c_1X + \cdots + c_{n-1}X^{n-1}, \qquad c_i \in \mathbb{F}_p$$

and there are p^n of these. Since the modulus $\pi(X)$ is irreducible, the ring $\mathbb{F}_p[X]/\langle\pi(X)\rangle$ is a field. $\square$

Theorem 24.8. *Let $\pi(X)$ be irreducible of degree d in $\mathbb{F}_p[X]$.*

1. *In $\mathbb{F}_p[X]$, we have $\pi(X) \mid (X^{p^d} - X)$.*

2. *For $n \geq 0$, we have $\pi(X) \mid (X^{p^n} - X)$ if and only if $d \mid n$.*

Proof. This divisibility in 1 is the same as the congruence $X^{p^d} \equiv X \mod \pi(X)$, or equivalently the equation $\overline{X}^{p^d} = \overline{X}$ in $\mathbb{F}_p[X]/(\pi(X))$. Such an equation follows immediately from the Lemmas above, using the field $\mathbb{F}_p[X]/(\pi(X))$.

To prove ($\Longleftarrow$) in 2, write $n = kd$. Starting with $X \equiv X^{p^d} \mod \pi(X)$ and applying the p^dth power to both sides k times, we obtain

$$\begin{aligned} X &\equiv X^{p^d} \mod \pi(X) \\ &\equiv X^{p^{2d}} \mod \pi(X) \\ &\vdots \\ &\equiv X^{p^{kd}} \mod \pi(X) \\ &= X^{p^n} \mod \pi(X). \end{aligned}$$

Thus $\pi(X) \mid (X^{p^n} - X)$ in $\mathbb{F}_p[X]$.

Now we prove ($\Longrightarrow$) in 2. We assume

$$X^{p^n} \equiv X \mod \pi(X)$$

and we want to show $d \mid n$. Write $n = dq + r$ with $0 \leq r < d$. We will show $r = 0$. Observe that

$$\begin{aligned} X &\equiv X^{p^n} \mod \pi(X) \\ &\equiv (X^{p^{dq}})^{p^r} \mod \pi(X) \\ &\equiv X^{p^r} \mod \pi(X) \end{aligned}$$

This tells us that one particular element of $\mathbb{F}_p[X]/(\pi(X))$, the class of X, is equal to its own p^rth power. More generally, for any $f(X) \in \mathbb{F}_p[X]$, we have

$$\begin{aligned} f(X)^{p^r} &\equiv f(X^{p^r}) \mod \pi(X) \\ &\equiv f(X) \mod \pi(X). \end{aligned}$$

Therefore in $\mathbb{F}_p[X]/(\pi(X))$ the congruence class of $f(X)$ is equal to its own p^rth power. As $f(X)$ is a general polynomial in $\mathbb{F}_p[X]$, we have proved every element of $\mathbb{F}_p[X]/(\pi(X))$ is its own p^rth power (in $\mathbb{F}_p[X]/(\pi(X))$).

Consider now the polynomial $T^{p^r} - T$. When $r > 0$, this is a polynomial with degree $p^r > 1$, and we have found p^d different roots of this polynomial in $\mathbb{F}_p[X]/(\pi(X))$ (namely, every element of this field is a root). Therefore $p^d \leq p^r$, so $d \leq r$. But, recalling where r came from, $r < d$. This is a contradiction, so $r = 0$. This proves $d \mid n$. $\square$

Theorem 24.9. *Let $\pi(X)$ be irreducible in $\mathbb{F}_p[X]$ with degree d and $F \supseteq \mathbb{F}_p$ be a field which $\pi(X)$ has a root, say α. Then $\pi(X)$ has roots $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$. These d roots are distinct; more precisely, when i and j are nonnegative, then $\alpha^{p^i} = \alpha^{p^j}$ if and only if $i \equiv j \mod d$.*

Proof. Since $\pi(X)^p = \pi(X^p)$, we see α^p is also a root of $\pi(X)$, and likewise, $\alpha^{p^2}, \alpha^{p^3}$, and so on by iteration. Once we reach α^{p^d} we have cycled back to the start: $\alpha^{p^d} = \alpha$ by Theorem (25.12).

Now we will show for $i, j \geq 0$ that $\alpha^{p^i} = \alpha^{p^j}$ if and only if $i \equiv j \mod d$. Since $\alpha^{p^d} = \alpha$, the implication ($\Longleftarrow$) is straightforward. To argue in the other direction, we may suppose without loss of generality that $i \leq j$, so $j = i + k$ with $k \geq 0$. Then

$$\alpha^{p^i} = \alpha^{p^{i+k}} = (\alpha^{p^k})^{p^i}.$$

Applying Lemma (24.4) to this equality i times, with $A = F$, we have $\alpha = \alpha^{p^k}$. Therefore α is a root of $X^{p^k} - X$, so $\pi(X) \mid (X^{p^k} - X)$ in $\mathbb{F}_p[X]$. We conclude $d \mid k$ by the previous Theorem.

□

Since $\pi(X)$ has at most $d = \deg \pi$ roots in any field, Theorem (25.13) tells us $\alpha, \alpha^p, \ldots, \alpha^{p^{d-1}}$ are a complete set of roots of $\pi(X)$ and these roots are distinct.

Example 24.2. The polynomial $X^3 + X + 1$ is irreducible in $\mathbb{F}_2[X]$. In the field $F = \mathbb{F}_2[t]/(t^3 + t + 1)$, one root of the polynomial is $\bar{t}$. The other roots are $\bar{t}^2$ and $\bar{t}^4$. If we wish to write the third root without going beyond the second power of $\bar{t}$, note $t^4 \equiv t^2 + t \mod t^3 + t + 1$. Therefore, the roots of $X^3 + X + 1$ in F are $\bar{t}, \bar{t}^2$, and $\bar{t}^2 + \bar{t}$.

24.5 Finding Irreducibles in $\mathbb{F}_p[X]$

A nice application of Theorem (25.12) is the next result, which is due to Gauss. It describes all irreducible polynomials of a given degree in $\mathbb{F}_p[X]$ as factors of a certain polynomial.

Theorem 24.10. *Let $n \geq 1$. In $\mathbb{F}_p[X]$,*

$$X^{p^n} - X = \prod_{d \mid n} \prod_{\substack{\deg \pi = d \\ \pi \text{ monic}}} \pi(X), \tag{76}$$

where $\pi(X)$ is irreducible.

Proof. From Theorem (25.12), the irreducible factors of $X^{p^n} - X$ in $\mathbb{F}_p[X]$ are the irreducibles with degree dividing n. What remains is to show that each monic irreducible factor of $X^{p^n} - X$ appears only once in the factorization. Let $\pi(X)$ be an irreducible factor of $X^{p^n} - X$ in $\mathbb{F}_p[X]$. We want to show $\pi(X)^2$ does not divide $X^{p^n} - X$.

There is a field F in which $\pi(X)$ has a root, say α. We will work in $F[X]$. Since $\pi(X) \mid (X^{p^n} - X)$, we have

$$X^{p^n} - X = \pi(X)k(X),$$

so $\alpha^{p^n} = \alpha$. Then in $F[X]$,

$$\begin{aligned} X^{p^n} - X &= X^{p^n} - X - 0 \\ &= X^{p^n} - X - (\alpha^{p^n} - \alpha) \\ &= (X - \alpha)^{p^n} - (X - \alpha) \\ &= (X - \alpha)((X - \alpha)^{p^n - 1} - 1). \end{aligned}$$

The second factor in the last expression does not vanish at α, so $(X - \alpha)^2$ does not divide $X^{p^n} - X$. Therefore $\pi(X)^2$ does not divide $X^{p^n} - X$ in $\mathbb{F}_p[X]$. □

Example 24.3. We factor $X^{2^n} - X$ in $\mathbb{F}_2[X]$ for $n = 1, 2, 3, 4$. We have

$$\begin{aligned} X^2 - X &= X(X+1) \\ X^4 - X &= X(X+1)(X^2+X+1) \\ X^8 - X &= X(X+1)(X^3+X+1)(X^3+X^2+1) \\ X^{16} - X &= X(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1) \end{aligned}$$

Let $\mathrm{N}_p(n)$ be the number of monic irreducibles of degree n in $\mathbb{F}_p[X]$. For instance, $\mathrm{N}_p(1) = p$. On the right side of (76), for each d dividing n there are $\mathrm{N}_p(d)$ different monic irreducible factors of degree d. Taking degrees of both sides of (76) gives us

$$p^n = \sum_{d \mid n} d\mathrm{N}_p(d)$$

for all $n \geq 1$. Looking at this formula over all n lets us invert it to get a formula for $\mathrm{N}_p(n)$. For example

$$\mathrm{N}_p(2) = \frac{p^2 - p}{2}, \quad \mathrm{N}_p(3) = \frac{p^3 - p}{3}, \quad \text{and} \quad \mathrm{N}_p(12) = \frac{p^{12} - p^6 - p^4 + p^2}{12}.$$

A general formula for $\mathrm{N}_p(n)$ can be written down using the Möbius inversion formula.

24.6 Cyclotomic Polynomials and Roots of Unity

Let K be a field and let n be a positive integer. An n**th root of unity** in K is a solution to $X^n = 1$, or equivalently, it is a root of $X^n - 1$. There are at most n different nth roots of unity in a field since $X^n - 1$ has at most n roots in K. A **root of unity** is an nth root of unity for some n.

Example 24.4. The only roots of unity in $\mathbb{R}$ are ± 1, while in $\mathbb{C}$ there are n different nth roots of unity for each n, namely $\zeta_n := e^{2\pi i k/n}$ for $0 \leq k \leq n-1$ and they form a group of order n. In characteristic p there is no pth root of unity besides 1: if $X^p = 1$ in characteristic p, then $0 = X^p - 1 = (X-1)^p$, so $x = 1$.

Proposition 24.2. *The set of all nth roots of unity in K forms a cyclic group.*

Proof. Let S denote the set of all of all nth roots of unity in K. Then S is contained in $K^\times$ since 0 is not an nth root of unity. Also S is nonempty since 1 is an nth root of unity. Furthermore, if $\alpha, \beta \in S$, then

$$\begin{aligned}(\alpha\beta^{-1})^n &= \alpha^n \beta^{-n} \\ &= 1 \cdot 1 \\ &= 1.\end{aligned}$$

It follows that S is a subgroup of $K^\times$. Finally, S is finite since it contains at most n elements, and thus it follows from Proposition (25.3) that S is cyclic. □

Definition 24.2. We say an nth root of unity is **primitive** if it has order n.

24.6.1 Cyclotomic Extensions

For any field K, an extension of the form $K(\zeta)$, where ζ is a root of unity, is called a **cyclotomic** extension of K. The important algebraic fact we will explore is that cyclotomic extensions of every field have an abelian Galois group; we will look especially at cyclotomic extensions of $\mathbb{Q}$ and finite fields.

24.6.2 Irreducibility of the Cyclotomic Polynomials

Fix $n \geq 1$ and $K_n/\mathbb{Q}$ a splitting field of $X^n - 1$. Define

$$\Phi_n(X) = \prod (X - \zeta) \in K_n[X],$$

where ζ runs over all primitive nth roots of unity in K_n (i.e. all generators of the intrinsic order n cyclic group of solutions to $T^n - 1 = 0$ in K_n). The polynomial Φ_n is called the n**th cyclotomic polynomial**. It is clear from the intrinsic nature of primitive nth roots of unity that the action of $\mathrm{Gal}(K_n/\mathbb{Q})$ permutes these around. Hence, even without knowing if $\mathrm{Gal}(K_n/\mathbb{Q})$ is "big", it is clear that the monic polynomial $\Phi_n(X)$ is invariant under the action of $\mathrm{Gal}(K_n/\mathbb{Q})$. Hence, by Galois theory the coefficients of Φ_n must lie in $\mathbb{Q}$! Its degree is clearly $|(\mathbb{Z}/n\mathbb{Z})^\times|$. The main aim is therefore to prove

Theorem 24.11. *(Gauss) The polynomial* $\Phi_n \in \mathbb{Q}[X]$ *is irreducible.*

Proof. By construction, $\Phi_n \in \mathbb{Q}[X]$ is monic, and over the extension field K_n we see that Φ_n divides $X^n - 1$ in $K_n[X]$. Since $\Phi_n \in \mathbb{Q}[X]$ and $X^n - 1 \in \mathbb{Q}[X]$, it follows from Theorem (24.3) that Φ_n divides $X^n - 1$ in $\mathbb{Q}[X]$. By Gauss' Lemma, since $X^n - 1 \in \mathbb{Q}[X]$ has integral coefficients, any monic factorization in $\mathbb{Q}[X]$ is necessarily in $\mathbb{Z}[X]$. That is, if we write $X^n - 1 = \Phi_n h$ with $h \in \mathbb{Q}[X]$, then since h is visibily monic (as $X^n - 1$ and Φ_n are monic) it follows that both Φ_n and h must lie in $\mathbb{Z}[X]$.

Now suppose that Φ_n is not irreducible in $\mathbb{Q}[X]$, so there is a factorization $\Phi_n = fg$ in $\mathbb{Q}[X]$ with f and g of positive degree. We may also suppose f is irreducible. By Gauss' Lemma applied to the monic factorization $fg = \Phi_n$ with $\Phi_n \in \mathbb{Z}[X]$, we must have $f, g \in \mathbb{Z}[X]$. We seek to derive a contradiction. In $K_n[X]$ we have the monic factorization $\Phi_n = \prod (X - \zeta)$ where the product runs over all primitive nth roots of unity in K_n. Since f and g both have positive degree, there must exist distinct primitive nth roots of unity ζ and ζ' in K_n such that $X - \zeta$ is a factor of f and $X - \zeta'$ is a factor of g , that is, $f(\zeta) = 0$ and $g(\zeta') = 0$ in K_n.

We can write $\zeta' = \zeta^r$ for a unique $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ since ζ and ζ' are primitive nth roots of unity. Since $\zeta \neq \zeta'$, we must have $r \neq 1$. Choose a positive integer representing this residue class r, and denote it by r, so $r > 1$ and $\gcd(r, n) = 1$. Consider the prime factorization $r = \prod p_j$ with primes p_j not necessarily pairwise distinct. To go from ζ to $\zeta' = \zeta^r$ we successively raise to exponents p_1, then p_2, etc. Since $f(\zeta) = 0$ and $g(\zeta') = 0$, so $f(\zeta') \neq 0$ and $g(\zeta) \neq 0$ (as the factorization $\Phi_n = fg$ and separability of Φ_n forces f and g to have no common roots), there must exist a least j for which $\zeta^{p_1 \cdots p_{j-1}}$ is a root of f and its p_jth power is a root of g. Thus, there is a primitive nth root of unity ζ_0 and prime $p \nmid n$ such that $f(\zeta_0) = 0$ and $g(\zeta_0^p) = 0$. We shall deduce a contradiction.

Since f is irreducible over $\mathbb{Q}$, it must be the minimal polynomial of ζ_0. But $g(\zeta_0^p) = 0$, so $g(X^p) \in \mathbb{Q}[X]$ has ζ_0 as a root. Thus $f \mid g(X^p)$ in $\mathbb{Q}[X]$. We can therefore write $g(X^p) = fq$ in $\mathbb{Q}[X]$, with q necessarily monic. Since $g(X^p)$ has coefficients in $\mathbb{Z}$, Gauss' Lemma once again ensures that $q \in \mathbb{Z}[X]$. Thus, the identity $g(X^p) = fq$ takes place in $\mathbb{Z}[X]$. Now reduce mod p! In $\mathbb{F}_p[X]$, we get

$$\overline{f}\overline{q} = \overline{g}(X^p) = \overline{g}(X)^p,$$

the final equality using the fact that $a^p = a$ for all $a \in \mathbb{F}_p$. Monoicity of f and g with positive degree ensures that $\overline{f}, \overline{g} \in \mathbb{F}_p[X]$ have positive degree. From the divisibility relation $\overline{f} \mid \overline{g}^p$ we conclude that $\overline{f}$ and $\overline{g}$ must have a nontrivial irreducible factor in common. Hence, the product $\overline{f}\overline{g}$ has a nontrivial irreducible factor appearing with multiplicity more than 1. But in $\mathbb{Q}[X]$ we have $fg = \Phi_n \mid (X^n - 1)$ in $\mathbb{F}_p[X]$. It follows that $X^n - 1 \in \mathbb{F}_p[X]$ has a nontrivial square factor and hence is not separable. But this is absurd, since p doesn't divide n and hence the derivative test ensures that $X^n - 1 \in \mathbb{F}_p[X]$ is separable! Contradiction. □

25 Finite Fields

Theorem 25.1. *Let p be a prime and let $\pi(X)$ be a monic irreducible polynomial in $\mathbb{F}_p[X]$ of degree n. Then the ring $\mathbb{F}_p[X]/\langle \pi(X) \rangle$ is a field of order p^n.*

Proof. The cosets mod $\pi(X)$ are represented by remainders

$$c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}, \qquad c_i \in \mathbb{F}_p$$

and there are p^n of these. Since the modulus $\pi(X)$ is irreducible, the ring $\mathbb{F}_p[X]/\langle \pi(X) \rangle$ is a field. □

We will see that every finite field is isomorphic to a field of the form $\mathbb{F}_p[X]/\langle \pi(X) \rangle$, so these polynomial constructions gives us working models over any finite field.

Theorem 25.2. *Let K be a finite field. Then $K^\times$ is cyclic.*

Proof. Let $q = |K|$, so $|K^\times| = q - 1$. Let m be the maximal order among all elements in $K^\times$. We will show $m = q - 1$. By Lagrange's Theorem, we have $m \mid q - 1$, and hence $m \leq q - 1$. It is a theorem from group theory that every order of every element must divide the maximal order. In particular, we have $x^m = 1$ for all $x \in K^\times$. Therefore all numbers in $K^\times$ are roots of the polynomial $X^m - 1$. The number of roots of a polynomial over a field is at most the degree of the polynomial, so $q - 1 \leq m$. Combining both inequalities gives us $m = q - 1$. □

25.0.1 Finite Rings are Integral Domains if and only if they are Fields

Proposition 25.1. *Let R be a finite ring. Then R is an integral domain if and only if R is a field.*

Proof. One direction is clear, for the other direction, let a be a nonzero element in R. Since R is an integral domain, the multiplication by a map $\mathrm{m}_a \colon R \to R$ given by

$$\mathrm{m}_a(b) = ab$$

for all $b \in R$ is injective. Since R is finite and m_a is injective, the multiplication by a map must also be surjective. Thus there exists a $b \in R$ such that

$$\begin{aligned} 1 &= \mathrm{m}_a(b) \\ &= ab. \end{aligned}$$

Thus a is a unit. □

25.0.2 Integral Domains with Positive Characteristic must have Prime Characteristic

Proposition 25.2. *Let R be an integral domain. If $\operatorname{char} R > 0$, then $\operatorname{char} R$ is prime.*

Proof. Let us denote $n = \operatorname{char} R$. We will show that n is a prime. Assume for a contradiction that n is not a prime. Then there exists $1 < k, m < n$ such that

$$\begin{aligned} 0 &= n \cdot 1_R \\ &= (km) \cdot 1_R \\ &= (k \cdot 1_R)(m \cdot 1_R). \end{aligned}$$

Since $n = \operatorname{char} R$, we must have $(k \cdot 1_R) \neq 0$ and $(m \cdot 1_R) \neq 0$. But this contradicts the fact that R is an integral domain. □

Corollary 26. *Every finite field has prime characteristic.*

Proof. Every finite ring has positive characteristic and every field is an integral domain. Thus the corollary follows immediately from (25.2). □

25.0.3 Finite Subgroup of Multiplicative Group of Field is Cyclic

Lemma 25.3. *Let A be a finite abelian group. Then the order of every element must divide the maximal order.*

Proof. From the fundamental theorem of finite abelian groups, we have an isomorphism

$$A \cong \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_n}$$

where $k_1 \mid \cdots \mid k_n$. Let $e_1, \dots, e_n$ denote the standard $\mathbb{Z}$-basis for $\mathbb{Z}^n$, and let $\bar{e}_i$ denote the corresponding coset in $\mathbb{Z}_{k_i}$ for each $1 \leq i \leq n$. Since $k_i \mid k_n$ we see that k_n kills each $\mathbb{Z}_{k_i}$ for all $1 \leq i \leq n$. Therefore k_n kills all of A. In particular, the order of every element must divide k_n, which is in fact the maximal order as $k_n = \mathrm{ord}(\bar{e}_{i_n})$. □

Lemma 25.4. *The number of roots of a polynomial over a field is at most the degree of the polynomial.*

Proof. Let K be a field and let $f(T)$ be a polynomial coefficients in K. By replacing K with a splitting field of $f(T)$ if necessary, we may assume that $f(T)$ splits into linear factors over K, say

$$f(T) = (T - \alpha_1) \cdots (T - \alpha_n).$$

where $\alpha_1, \dots \alpha_n \in K$ and $n = \deg f(T)$. Let $\alpha \in K$. Then we have

$$\begin{aligned} f(\alpha) = 0 &\iff (\alpha - \alpha_1) \cdots (\alpha - \alpha_n) = 0 \\ &\iff \alpha - \alpha_i = 0 \text{ for some } i \\ &\iff \alpha = \alpha_i \text{ for some } i, \end{aligned}$$

where we obtained the second line from the first line from the fact that K is an integral domain. Therefore $f(T)$ has *at most* n roots. □

Proposition 25.3. *Let K be a field and let G be a finite subgroup of $K^\times$. Then G is cyclic.*

Proof. Let $n = |G|$ and let m be the maximal order among all elements in G. We will show $m = n$. By Lagrange's Theorem, we have $m \mid n$, and hence $m \leq n$. It follows from Lemma (80.1) that every order of every element must divide the maximal order. In particular, we have $x^m = 1$ for all $x \in G$. Therefore all numbers in G are roots of the polynomial $T^m - 1$. By Lemma (80.2), the number of roots of a polynomial over a field is at most the degree of the polynomial, so $n \leq m$. Combining both inequalities gives us $m = n$. □

25.0.4 Finite Fields have Prime Power Order

Theorem 25.5. *Let F be a finite field. Then F has prime power order.*

Proof. Let F be a finite field. Corollary (26) tells us that the characteristic of F is prime, denote it by $p = \mathrm{char}\, F$. Then $\mathbb{Z}/(p)$ embeds as a subring of F. In particular, we can view F as a finite-dimensional $\mathbb{Z}/(p)$-vector space. Letting $n = \dim_{\mathbb{Z}/(p)}(F)$ and picking a basis $\{e_1, \dots, e_n\}$ for F over $\mathbb{Z}/(p)$, elements of F can be written uniquely as

$$c_1 e_1 + \cdots + c_n e_n$$

where $c_i \in \mathbb{Z}(p)$ for all $1 \leq i \leq n$. Each coefficient has p choices, so $|F| = p^n$. □

25.0.5 Classification of Finite Fields

Theorem 25.6. *Every finite field is isomorphic to $\mathbb{F}_p[X]/\langle \pi(X) \rangle$ for some prime p and some monic irreducible $\pi(X)$ in $\mathbb{F}_p[X]$.*

Proof. Let F be a finite field. By Theorem (25.5), F has order p^n for some prime p and positive integer n, and there is a field embedding $\mathbb{F}_p \hookrightarrow F$. The group $F^\times$ is cyclic by Proposition (25.3). Let γ be a generator of $F^\times$. Evaluation at γ, namely $f(X) \mapsto f(\gamma)$, is a ring homomorphism $\mathrm{ev}_\gamma \colon \mathbb{F}_p[X] \to F$ that fixes $\mathbb{F}_p$. Since every number in F is 0 or a power of γ, ev_γ is onto ($0 = \mathrm{ev}_\gamma(0)$ and $\gamma^r = \mathrm{ev}_\gamma(X^r)$ for any $r \geq 0$). Therefore

$$\mathbb{F}_p[X]/\ker \mathrm{ev}_\gamma \cong F.$$

This implies the kernel of ev_γ is a maximal ideal in $\mathbb{F}_p[X]$, so it must be $\langle \pi(X) \rangle$ for some monic irreducible $\pi(X)$ in $\mathbb{F}_p[X]$. □

Fields of size 9 are of the form $\mathbb{F}_p[X]/\langle \pi(X)\rangle$ need $p=3$ and $\deg \pi = 2$. The monic irreducible quadratics in $\mathbb{F}_3[X]$ are x^2+1, x^2+x+2, and x^2+2x+2. In

$$\mathbb{F}_3[X]/\langle X^2+1\rangle, \quad \mathbb{F}_3[X]/\langle X^2+X+2\rangle, \quad \mathbb{F}_3[X]/\langle X^2+2x+2\rangle,$$

$\overline{X}$ is not a generator of the nonzero elements in the first field but is a generator of the nonzero elements in the second and third fields. So although $\mathbb{F}_3[X]/\langle X^2+1\rangle$ is the simplest choice among the three examples, it's not the one that would come out of the proof of Theorem (25.6) when we look for a model of fields of order 9 as $\mathbb{F}_3[X]/\langle \pi(X)\rangle$.

25.1 Finite Fields as Splitting Fields

We can describe any finite field as a splitting field of a polynomial depending only on the size of the field.

25.1.1 Field of Prime Power p^n is a Splitting Fields over $\mathbb{F}_p$ of $X^{p^n}-X$

Lemma 25.7. *A field of prime power order p^n is a splitting field over $\mathbb{F}_p$ of $X^{p^n}-X$.*

Proof. Let F be a field of order p^n. Then F contains a subfield isomorphic to $\mathbb{F}_p$. Explicitly, the subring of F generated by 1 is a field of order p. Every $t\in F$ satisfies $t^{p^n}=t$: if $t\neq 0$ then $t^{p^n-1}=1$ since $F^\times = F\backslash\{0\}$ is a multiplicative group of order p^n-1, and then multiplying through by t gives us $t^{p^n}=t$, which is also true when $t=0$. The polynomial $X^{p^n}-X$ has every element of F as a root, so F is a splitting field of $X^{p^n}-X$ over the field $\mathbb{F}_p$. $\square$

25.1.2 Existence of Field of Order p^n

Theorem 25.8. *For every prime power p^n, a field of order p^n exists.*

Proof. Taking our cue from the statement of Lemma (25.7), let F be a field extension of $\mathbb{F}_p$ over which $X^{p^n}-X$ splits completely. Inside F, the roots of $X^{p^n}-X$ form the set

$$S=\{t\in F \mid t^{p^n}=t\}.$$

This set has size p^n since the polynomial $X^{p^n}-X$ is separable over F:

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x}(X^{p^n}-X) &= p^n X^{p^n}-1\\ &= -1\end{aligned}$$

since $p=0$ in F, so $X^{p^n}-X$ has no roots in common with its derivative. It splits completely over F and has degree p^n, so it has p^n roots in F. We will show S is a subfield of F. It contains 1 and is easily closed under multiplication and (for nonzero solutions) inversion. It remains to show S is an additive group. Since $p=0$ in F, we have $(a+b)^p=a^p+b^p$ for all $a,b\in F$. Therefore the pth power map $t\mapsto t^p$ on F is additive. The map $t\mapsto t^{p^n}$ is also additive since it's the n-fold composite of $t\mapsto t^p$ with itself and the composition of homomorphisms is a homomorphism. The fixed points of an additive map are a group under addition, so S is a group under addition. Therefore S is a field of order p^n. $\square$

Corollary 27. *For every prime p and positive integer n, there is a monic irreducible of degree n in $\mathbb{F}_p[X]$, and moreover $\pi(X)$ can be chosen so that every nonzero element of $\mathbb{F}_p[X]/\langle\pi(X)\rangle$ is congruent to a power of X.*

Proof. By Theorem (25.8), a field F of order p^n exists. By (Theorem 25.6), the existence of an abstract field of order p^n implies the existence of a monic irreducible $\pi(X)$ in $\mathbb{F}_p[X]$ of degree n, and from the proof of Theorem (25.6) $\overline{X}$ generates the nonzero elements of $\mathbb{F}_p[X]/\langle\pi(X)\rangle$ since the isomorphism identifies $\overline{X}$ with a generator of $F^\times$. $\square$

It's worth appreciating the order in logic behind Theorem (25.8) and its corollary: to show we can construct a field of order p^n as $\mathbb{F}_p[X]/\langle\pi(X)\rangle$ where $\deg\pi=n$, the way we showed a $\pi(X)$ of degree n exists is by *first* constructing an abstract field F of order p^n (using the splitting field construction) and then prove F can be made isomorphic to $\mathbb{F}_p[X]/\langle\pi(X)\rangle$.

Remark 41. There is no simple formula for an irreducible of every degree in $\mathbb{F}_p[X]$ (just like there is no simple formula for every prime in $\mathbb{Z}$!). For example, binomial polynomials X^n-a are reducible when $p\mid n$. Trinomials X^n+aX^k+b with $a,b\in\mathbb{F}_p^\times$ and $0<k<n$ are often irreducible, but in some degrees there are no irreducible trinomials: none in $\mathbb{F}_2[X]$ of degree 8 or 13, in $\mathbb{F}_3[X]$ of degree 49 or 57, in $\mathbb{F}_5[X]$ of degree 35 or 70, or in $\mathbb{F}_7[X]$ of degree 124 or 163.

25.1.3 Irreducibles in $\mathbb{F}_p[X]$ of Degree n Must Divide $X^{p^n} - X$ and are Separable

Theorem 25.9. *Let π be an irreducible polynomial in $\mathbb{F}_p[X]$ of degree n. Then π divides $X^{p^n} - X$. In particular, π is separable.*

Proof. The field $\mathbb{F}_p[X]/\langle \pi \rangle$ has order p^n, so $t^{p^n} = t$ for all $t \in \mathbb{F}_p[X]/\langle \pi \rangle$. In other words, we can write this as $t^{p^n} - t = 0$ for all $t \in \mathbb{F}_p[X]/\langle \pi \rangle$. In particular, we have $X^{p^n} - X \equiv 0 \bmod \pi$. It follows that π divides $X^{p^n} - X$. Since $X^{p^n} - X$ is separable in $\mathbb{F}_p[X]$ (as it is relatively prime with its derivative), so its factor π is also separable. □

25.1.4 Finite Fields of the Same Size are Isomorphic

Theorem 25.10. *Any finite field of the same size are isomorphic.*

Proof. A finite field has prime power size, say p^n, and by Lemma (25.7), it is a splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. Any two splitting fields of a fixed polynomial over $\mathbb{F}_p$ are isomorphic, so any two fields of order p^n are isomorphic: they are splitting fields of $X^{p^n} - X$ over $\mathbb{F}_p$. □

The analogous theorem for finite groups and finite rings is false: having the same size does not usually imply isomorphism. For instance, $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ both have order 4 and they are nonisomorphic as additive groups and also as commutative rings.

Definition 25.1. Let p be a prime and let n be a positive integer. We write $\mathbb{F}_{p^n}$ for a finite field of order p^n. By Theorem (25.10), our choice of a finite field of order p^n is well-defined up to an isomorphism which fixes $\mathbb{F}_p$. As we shall soon see, there will be n such isomorphisms, and they will form the cyclic group $\mathbb{Z}/n\mathbb{Z}$.

25.1.5 Classification of Subfields of $\mathbb{F}_{p^n}$

Theorem 25.11. *A subfield of $\mathbb{F}_{p^n}$ has order p^d where $d \mid n$, and there is one such subfield for each d.*

Proof. Let F be a field with $\mathbb{F}_p \subseteq F \subseteq \mathbb{F}_{p^n}$. Set $d = [F : \mathbb{F}_p]$, so d divides $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. We will describe F in a way that only depends on $|F| = p^d$. Since $F^\times$ has order $p^d - 1$, for any $t \in F^\times$, we have $t^{p^d} = t$, and that holds even for $t = 0$. The polynomial $X^{p^d} - X$ has at most p^d roots in $\mathbb{F}_{p^n}$, and since F is a set of p^d different roots of it, we have

$$F = \{t \in \mathbb{F}_{p^n} \mid t^{p^d} = t\}.$$

This shows that there is at most one subfield of order p^d in $\mathbb{F}_{p^n}$, since the right side is completely determined as a subset of $\mathbb{F}_{p^n}$ from knowing p^d.

To prove for each d dividing n there is a subfield of $\mathbb{F}_{p^n}$ with order p^d, we turn things around and consider $\{t \in \mathbb{F}_{p^n} \mid t^{p^d} = t\}$. It is a field by the same proof that S is a field in the proof of Theorem (25.8). To show its size is p^d we want to show $X^{p^d} - X$ has p^d roots in $\mathbb{F}_{p^n}$. We'll do this in two ways. First,

$$\begin{aligned} d \mid n &\implies (p^d - 1) \mid (p^n - 1) \\ &\implies X^{p^d - 1} - 1 \mid X^{p^n - 1} - 1 \\ &\implies X^{p^d} - X \mid X^{p^n} - X, \end{aligned}$$

so since $X^{p^n} - X$ splits with distinct roots in $\mathbb{F}_{p^n}[X]$ so does its factor $X^{p^d} - X$. Second, $d \mid n \implies (p^d - 1) \mid (p^n - 1)$ and $\mathbb{F}_{p^n}^\times$ is cyclic of order $p^n - 1$, so it contains $p^d - 1$ solutions to $t^{p^d - 1} = 1$. Along with 0 we get p^d solutions in $\mathbb{F}_{p^n}$ so $t^{p^d} = t$. □

Example 25.1. In the diagram below are the subfields of $\mathbb{F}_{p^8}$ and $\mathbb{F}_{p^{12}}$

$$\begin{tikzcd}
\mathbb{F}_{p^8} \arrow[d, dash, "2"'] \\
\mathbb{F}_{p^4} \arrow[d, dash, "2"'] \\
\mathbb{F}_{p^2} \arrow[d, dash, "2"'] \\
\mathbb{F}_{p}
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{F}_{p^{12}} \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & & \\
\mathbb{F}_{p^4} \arrow[dr, dash, "2"'] & & \mathbb{F}_{p^6} \arrow[dl, dash, "3"] \arrow[dr, dash, "2"] & \\
 & \mathbb{F}_{p^2} \arrow[dr, dash, "2"'] & & \mathbb{F}_{p^3} \arrow[dl, dash, "3"] \\
 & & \mathbb{F}_{p} &
\end{tikzcd}$$

Example 25.2. One field of order $16 = 2^4$ is $\mathbb{F}_2[X]/\langle X^4 + X + 1\rangle$. All elements satisfy $t^{16} = t$. The solutions to $t^2 = t$ are the subfield $\{0, 1\}$ of order 2 and the solutions to $t^4 = t$ are the subfield $\{0, 1, X^2 + X, X^2 + X + 1\}$ of order 4.

25.2 Describing $\mathbb{F}_p$-Conjugates

Two elements in a finite field are called $\mathbb{F}_p$-**conjugate** if they share the same minimal polynomial over $\mathbb{F}_p$. We will show, after some lemmas about polynomials over $\mathbb{F}_p$, that all $\mathbb{F}_p$-conjugates can be obtained from each other by successively taking pth powers. This is in contrast to $\mathbb{Q}[X]$: all the roots of an irreducible polynomial in $\mathbb{Q}[X]$ are not generally expressible in terms of a particular root, with $X^3 - 2$ being a typical example. (The field $\mathbb{Q}(\sqrt[3]{2})$ contains only one root to this polynomial, not all 3 roots.)

25.2.1 Irreducible Polynomial in $\mathbb{F}_p[X]$ and $X^{p^n} - X$

Theorem 25.12. *Let $\pi(X)$ be irreducible of degree d in $\mathbb{F}_p[X]$.*

1. *In $\mathbb{F}_p[X]$, we have $\pi(X) \mid (X^{p^d} - X)$.*
2. *For $n \geq 0$, we have $\pi(X) \mid (X^{p^n} - X)$ if and only if $d \mid n$.*

Proof. This divisibility in 1 is the same as the congruence $X^{p^d} \equiv X \mod \pi(X)$, or equivalently the equation $\overline{X}^{p^d} = \overline{X}$ in $\mathbb{F}_p[X]/(\pi(X))$. Such an equation follows immediately from the Lemmas above, using the field $\mathbb{F}_p[X]/(\pi(X))$.

To prove ($\Longleftarrow$) in 2, write $n = kd$. Starting with $X \equiv X^{p^d} \mod \pi(X)$ and applying the p^dth power to both sides k times, we obtain

$$\begin{aligned} X &\equiv X^{p^d} \mod \pi(X) \\ &\equiv X^{p^{2d}} \mod \pi(X) \\ &\vdots \\ &\equiv X^{p^{kd}} \mod \pi(X) \\ &= X^{p^n} \mod \pi(X). \end{aligned}$$

Thus $\pi(X) \mid (X^{p^n} - X)$ in $\mathbb{F}_p[X]$.

Now we prove ($\Longrightarrow$) in 2. We assume

$$X^{p^n} \equiv X \mod \pi(X)$$

and we want to show $d \mid n$. Write $n = dq + r$ with $0 \leq r < d$. We will show $r = 0$. Observe that

$$\begin{aligned} X &\equiv X^{p^n} \mod \pi(X) \\ &\equiv (X^{p^{dq}})^{p^r} \mod \pi(X) \\ &\equiv X^{p^r} \mod \pi(X) \end{aligned}$$

This tells us that one particular element of $\mathbb{F}_p[X]/(\pi(X))$, the class of X, is equal to its own p^rth power. More generally, for any $f(X) \in \mathbb{F}_p[X]$, we have

$$\begin{aligned} f(X)^{p^r} &\equiv f(X^{p^r}) \mod \pi(X) \\ &\equiv f(X) \mod \pi(X). \end{aligned}$$

Therefore in $\mathbb{F}_p[X]/(\pi(X))$ the congruence class of $f(X)$ is equal to its own p^rth power. As $f(X)$ is a general polynomial in $\mathbb{F}_p[X]$, we have proved every element of $\mathbb{F}_p[X]/(\pi(X))$ is its own p^rth power (in $\mathbb{F}_p[X]/(\pi(X))$).

Consider now the polynomial $T^{p^r} - T$. When $r > 0$, this is a polynomial with degree $p^r > 1$, and we have found p^d different roots of this polynomial in $\mathbb{F}_p[X]/(\pi(X))$ (namely, every element of this field is a root). Therefore $p^d \leq p^r$, so $d \leq r$. But, recalling where r came from, $r < d$. This is a contradiction, so $r = 0$. This proves $d \mid n$. $\square$

25.2.2 Roots of an Irreducible $\pi(X)$ in $\mathbb{F}_p[X]$ are all Powers of a Root of $\pi(X)$

Theorem 25.13. *Let $\pi(X)$ be irreducible in $\mathbb{F}_p[X]$ with degree d and $F \supseteq \mathbb{F}_p$ be a field which $\pi(X)$ has a root, say α. Then $\pi(X)$ has roots $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}$. These d roots are distinct; more precisely, when i and j are nonnegative, then $\alpha^{p^i} = \alpha^{p^j}$ if and only if $i \equiv j \mod d$.*

Proof. Since $\pi(X)^p = \pi(X^p)$, we see α^p is also a root of $\pi(X)$, and likewise, $\alpha^{p^2}, \alpha^{p^3}$, and so on by iteration. Once we reach α^{p^d} we have cycled back to the start: $\alpha^{p^d} = \alpha$ by Theorem (25.12).

Now we will show for $i, j \geq 0$ that $\alpha^{p^i} = \alpha^{p^j}$ if and only if $i \equiv j \mod d$. Since $\alpha^{p^d} = \alpha$, the implication ($\Longleftarrow$) is straightforward. To argue in the other direction, we may suppose without loss of generality that $i \leq j$, so $j = i + k$ with $k \geq 0$. Then

$$\alpha^{p^i} = \alpha^{p^{i+k}} = (\alpha^{p^k})^{p^i}.$$

Applying Lemma (24.4) to this equality i times, with $A = F$, we have $\alpha = \alpha^{p^k}$. Therefore α is a root of $X^{p^k} - X$, so $\pi(X) \mid (X^{p^k} - X)$ in $\mathbb{F}_p[X]$. We conclude $d \mid k$ by the previous Theorem. □

Since $\pi(X)$ has at most $d = \deg \pi$ roots in any field, Theorem (25.13) tells us $\alpha, \alpha^p, \dots, \alpha^{p^{d-1}}$ are a complete set of roots of $\pi(X)$ and these roots are distinct.

Example 25.3. The polynomial $X^3 + X + 1$ is irreducible in $\mathbb{F}_2[X]$. In the field $F = \mathbb{F}_2[X]/(X^3 + X + 1)$, one root of the polynomial is $\overline{X}$. The other roots are $\overline{X}^2$ and $\overline{X}^4$. If we wish to write the third root without going beyond the second power of $\overline{X}$, note $X^4 \equiv X^2 + X \mod X^3 + X + 1$. Therefore, the roots of $X^3 + X + 1$ in F are $\overline{X}, \overline{X}^2$, and $\overline{X}^2 + \overline{X}$.

25.3 Galois Groups

Since $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}_p$ over $X^{p^n} - X$, which is separable, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois. It is a fundamental feature that the Galois group is cyclic, with a canonical generator.

25.3.1 $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F})$ is Cyclic with Canonical Generator

Theorem 25.14. *The pth power map $\varphi_p \colon t \mapsto t^p$ on $\mathbb{F}_{p^n}$ generates $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.*

Proof. Any $a \in \mathbb{F}_p$ satisfies $a^p = a$, so the function $\varphi_p \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ fixes $\mathbb{F}_p$ pointwise. Also φ_p is a field homomorphism and it is injective, so φ_p is surjective since $\mathbb{F}_{p^n}$ is finite. Therefore $\varphi_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

The size of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. We will show φ_p has order n in this group, so it generates the Galois group. For $r \geq 1$ and $t \in \mathbb{F}_{p^n}$, we have $\varphi_p^r(t) = t^{p^r}$. If φ_p^r is the identity then $t^{p^r} = t$ for all $t \in \mathbb{F}_{p^n}$, which can be rewritten as $t^{p^r} - t = 0$. The polynomial $X^{p^r} - X$ has degree p^r (since $r \geq 1$), so it has at most p^r roots in $\mathbb{F}_{p^n}$. Thus $p^n \leq p^r$, so $n \leq r$. Hence φ_p has order at least n in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, a group of order n, so φ_p generates the Galois group: every element of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is an iterate of φ_p. □

26 Field Extensions

Definition 26.1. Let K and L be a fields. If $L \supseteq K$, then we say L is a **field extension** of K. We denote such a field extension of L/K. A field K is an **extension field** of a field F if $F \subseteq K$. We denote such a field extension by K/F. In this case, K is an F-vector space. We denote the dimension of K as an F-vector space by $[K : F]$. Finally, if E is a field with

$$F \subseteq E \subseteq K,$$

we say E is an **intermediate** extension field.

Example 26.1. $\mathrm{ch}\mathbb{Q} = 0$ and $\mathrm{ch}\mathbb{F}_p = p$.

Proposition 26.1. *The characteristic of a field F is either 0 or a prime.*

Proof. If $\mathrm{ch}F = 0$ then we are done, so assume $\mathrm{ch}F = m$ and m is not prime. Then $m = ab$ where $a, b \in \mathbb{Z}$ such that $a, b > 1$. Then $m \cdot 1_F = (a \cdot 1_F)(b \cdot 1_F) = 0$ implies either $(a \cdot 1_F) = 0$ or $(b \cdot 1_F) = 0$. In either case, we get a contradiction since $\mathrm{ch}F \leq a, b < m$. So m is prime. □

Let F be a field and define $\varphi : \mathbb{Z} \to F$ by $\varphi(n) = n \cdot 1_F$. Then φ is a ring homomorphism. So $\mathbb{Z}/\mathrm{Ker}\varphi \cong \varphi(\mathbb{Z}) \subseteq F$. Since $\mathbb{Z}$ is a PID, $\mathrm{Ker}\varphi = m\mathbb{Z}$ for some $m \geq 0$. Let $p = \mathrm{ch}F$. Then $p \in m\mathbb{Z}$. So $m = 1$ or $m = p$ since p is prime. If $m = 1$, then $\varphi(1) = 0$ which is a contradiction, so $m = p$. Then $\mathrm{Ker}\varphi = p\mathbb{Z}$ and $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \subseteq F$. If $\mathrm{ch}F = 0$ then $\mathbb{Z} \cong \varphi(\mathbb{Z}) \subseteq F$ implies F contains an isomorphic copy of $\mathbb{Q}$. In either case, we call this the **prime subfield** of F.

Definition 26.2. (Field Extension) Let F and K be fields. If F is a subfield of K then we say K is a **field extension** of F, denoted $F \subset K$ or K/F.

Remark 42. If $F \subseteq K$ is a field extension, then K is a vector space over F. The **degree** of the extension K/F, denoted $[K : F]$, is the dimension of K as an F-vector space.

Example 26.2. $[\mathbb{R} : \mathbb{R}] = 1$ and $[\mathbb{C} : \mathbb{R}] = 2$.

If F is a field and $p(x) \in F[x]$ is an irreducible polynomial over F, can we find a field K containing F such that the equation $p(x) = 0$ has a solution in K? Yes.

Theorem 26.1. *Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial over F. Then there is a field K containing (an isomorphic copy of) F such that $p(x)$ has a root $\alpha \in K$. Identifying F with this isomorphic copy which is contained in K, we'll regard K as a field extension of F.*

Proof. Since $p(x)$ is irreducible in $F[x]$, which is a PID, $\langle p(x)\rangle$ is a maximal ideal in $F[x]$. So $K := F[x]/\langle p(x)\rangle$ is a field. Let $\pi : F[x] \to F[x]/\langle p(x)\rangle$ be the canonical projection map given by $\pi(a(x)) = \overline{a(x)}$. Then $\varphi := \pi_{|F}$ gives a ring homomorphism from F to $F[x]/\langle p(x)\rangle$. Since F is a field and since $\varphi(1) \neq 0$, $\mathrm{Ker}\varphi = 0$, so φ is injective. Finally, let $\alpha := \overline{x}$. Then

$$\begin{aligned} p(\alpha) &= p(\overline{x}) \\ &= \overline{p(x)} \\ &= \overline{0}. \end{aligned}$$

□

Theorem 26.2. *Let F be a field, $p(x)$ be an irreducible polynomial over F, $K := F[x]/\langle p(x)\rangle$, $\alpha := \bar{x}$, and $n = \deg p(x)$. Then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an F-basis of K. In particular, $[K : F] = n$.*

Proof. Let $\overline{g(x)} \in K$. Since F is a field, $F[x]$ is a Euclidean Domain, so there exists $q(x), r(x) \in F[x]$ such that $g(x) = q(x)p(x) + r(x)$ with either $r(x) = 0$ or $\deg r(x) \leq n-1$. If $r(x) = 0$, then $\overline{g(x)} = \bar{0}$. If $r(x) \neq 0$, then $r(x) = c_0 + c_1x + \cdots + c_\ell x^\ell$ where $\ell \leq n-1$. Therefore

$$\begin{aligned} \overline{g(x)} &= \overline{q(x)p(x) + r(x)} \\ &= \overline{r(x)} \\ &= \overline{c_0 + c_1x + \cdots + c_\ell x^\ell} \\ &= c_0 + c_1\alpha + \cdots + c_\ell \alpha^\ell \end{aligned}$$

implies $g(x) \in \mathrm{Span}\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Next we check that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is linearly independent over F. Let $b_0, b_1, \ldots, b_{n-1} \in F$ such that $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = \bar{0}$. Then $b_0 + b_1x + \cdots + b_{n-1}x^{n-1} = p(x)q(x)$ for some $q(x) \in F[x]$. But the degree of $p(x)$ is n, so we must have $q(x) = 0$, which implies $b_i = 0$ for $1 \leq i \leq n-1$. □

26.1 Algebraic Extensions

Definition 26.3. Let L/K be a field extension.

1. An element $\alpha \in L$ is said to be **algebraic** over K if there exists a nonzero polynomial $f(T) \in K[T]$ such that $f(\alpha) = 0$. If $\alpha \in L$ is not algebraic, then we say it is **transcendental** over K.
2. We say L/K is an **algebraic extension** if every $\alpha \in L$ is algebraic over K. We say L/K is a **transcendental extension** if there exists at least one $\alpha \in L$ which is transcendental over K.
3. We say L is **algebraically closed** if every irreducible polynomial in $L[X]$ splits completely in $L[X]$. We say L is an **algebraic closure** of K if L is algebraically closed and L/K is an algebraic extension.

Example 26.3. The number π is algebraic over $\mathbb{R}$ since $f(\pi) = 0$ where $f(T) = T - \pi$. On the other hand, it is a nontrivial theorem that π is transcendental over $\mathbb{Q}$.

Example 26.4. The imaginary number i is algebraic over $\mathbb{Q}$ since $f(i) = 0$ where $f(T) = T^2 + 1$.

Proposition 26.2. *Let K/F be a field extension. If $\alpha \in K$ is algebraic over F, then there is a unique monic irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. Moreover, if $f(x) \in F[x]$ has α as a root, then $p(x) \mid f(x)$.*

Proof. Let $p(x) \in F[x]$ be a polynomial of minimal degree having α as a root. We can assume, without loss of generality, that $p(x)$ is monic. We show that $p(x)$ is irreducible in $F[x]$. Suppose not. Then $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$ and $1 \leq \deg a(x) < \deg p(x)$ and $1 \leq \deg b(x) < \deg p(x)$. Then $0 = p(\alpha) = a(\alpha)b(\alpha)$ implies either $a(\alpha) = 0$ or $b(\alpha) = 0$ since K is a field. But this contradicts the minimality of the degree of $p(x)$. Next, suppose $f(x) \in F[x]$ such that $f(\alpha) = 0$. Since $F[x]$ is a Euclidean Domain, there exists $q(x), r(x) \in F[x]$ such that $f(x) = q(x)p(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg p(x)$. Suppose $r(x) \neq 0$. Then $r(\alpha) = f(\alpha) - q(\alpha)p(\alpha) = 0$. But this contradicts the minimality of the degree of $p(x)$. □

Recall that if K/F is a field extension, then α is algebraic over F if and only if $F \subseteq F(\alpha)$ is finite. In this case, the degree of the extension $[F(\alpha) : F]$ is the degree of the minimal polynomial of α.

Theorem 26.3. *If $F \subseteq K \subseteq L$ are field extensions, then $[L : F] = [L : K][K : F]$.*

Proof. Suppose $[K : F] = \ell$ and $[L : K] = m$ and let $\{\alpha_1, \dots, \alpha_m\}$ be a basis of L over K, and $\{\beta_1, \dots, \beta_\ell\}$ be a basis of K over F. Then $\{\alpha_1\beta_1, \dots, \alpha_m\beta_\ell\}$ is a basis for L over F. □

Recall that $p(x) = x^3 + 3x - 1$ is irreducible over $\mathbb{Q}$ since $p(\pm 1) \neq 0$. But there exists $\alpha \in (0, 1)$ such that $p(\alpha) = 0$. Let's show that $\sqrt{2} \notin \mathbb{Q}(\alpha)$. Suppose $\sqrt{2} \in \mathbb{Q}(\alpha)$, then $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$, so $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \cdot 2$ which is a contradiction.

Definition 26.4. Let $F \subseteq K$ be a field extension and let $\alpha_1, \dots, \alpha_\ell \in K$. Then

$$F(\alpha_1, \dots, \alpha_\ell) = F(\alpha_1)(\alpha_2, \dots, \alpha_\ell) = \cdots = F(\alpha_1)(\alpha_2)\cdots(\alpha_\ell).$$

Theorem 26.4. *Let $F \subseteq K$ be a field extension. If $\alpha_1, \dots, \alpha_\ell \in K$ are all algebraic over F, then $F \subseteq F(\alpha_1, \dots, \alpha_\ell)$ is finite.*

Proof. Let $n_i = \deg m_{\alpha_i, F}$. We have a sequence of field extensions

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F(\alpha_1, \alpha_2, \dots, \alpha_\ell).$$

Then

$$\begin{aligned}
[F(\alpha_1, \alpha_2, \dots, \alpha_\ell) : F] &= [F(\alpha_1, \alpha_2, \dots, \alpha_\ell) : F(\alpha_1)][F(\alpha_1) : F] \\
&= [F(\alpha_1, \alpha_2, \dots, \alpha_\ell) : F(\alpha_1, \alpha_2)][F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F] \\
&= [F(\alpha_1, \alpha_2, \dots, \alpha_\ell) : F(\alpha_1, \alpha_2, \dots \alpha_{\ell-1})] \cdots [F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F] \\
&\leq n_\ell \cdots n_2 n_1.
\end{aligned}$$

□

Theorem 26.5. *Let $F \subseteq K$ be a field extension. Then $F \subseteq K$ is finite if and only if $K = F(\alpha_1, \dots, \alpha_\ell)$.*

26.2 Constructing Algebraic Closures

Let K be a field. The purpose of this subsection is to construct an algebraic closure of K. Let us first introduce some notation. For each $k, n \in \mathbb{N}$ the k**th elementary symmetric polynomial in** n **variables** $X_1, \dots, X_n$, denoted $e_k(X_1, \dots, X_n)$, is defined by

$$e_k(X_1, \dots, X_n) = \begin{cases} 1 & \text{if } k = 0 \\ \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k} & \text{if } k \leq n \\ 0 & \text{if } k > n \end{cases}$$

For each nonconstant monic polynomial $f(X)$ in $K[X]$, write

$$f(X) = X^{n_f} + c_{f,1}X^{n_f - 1} + \cdots + c_{f,k}X^{n_f - k} + \cdots + c_{f,n_f}$$

where n_f is the degree of f and $c_{f,k} \in K$ for all $1 \leq k \leq n_f$, and let $t_{f,1}, \dots, t_{f,n_f}$ be independent variables. Throughout this section, whenever we write "$t_{f,k}$", it is understood that f is a nonconstant monic polynomial in $K[X]$ and that $1 \leq k \leq n_f$. For each nonconstant monic polynomial $f(X)$ in $K[X]$, choose a splitting field of $f(X)$ over K and let $\alpha_{f,1}, \dots, \alpha_{f,n_f}$ be the roots of $f(X)$ in this splitting field. Finally, let $A = K[\{t_{f,k}\}]$ be the polynomial ring generated over K by indepedent variables doubly indexed by every nonconstant monic $f \in K[X]$ and $1 \leq k \leq n_f$, and let I be the ideal in A generated by the coefficients of all the difference polynomials

$$f(X) - \prod_{i=1}^{n_f}(X - t_{f,k}) \in A[X].$$

In other words, $\mathfrak{a} = \langle \{u_{f,k}\} \rangle$ where

$$u_{f,k} := c_{f,k} - (-1)^k e_k(t_{f,1}, \dots, t_{f,n_f})$$

for each nonconstant monic polynomial f and for each $1 \leq k \leq n_f$. Observe that

$$u_{f,k}(\alpha_{f,1}, \dots, \alpha_{f,n_f}) = 0$$

for all nonconstant monic polynomials $f(X)$ in $K[X]$. Indeed, we can factor $f(X)$ over $K(\alpha_{f,1} \dots, \alpha_{f,n_f})$ as

$$(X - \alpha_{f,1}) \cdots (X - \alpha_{f,n_f}) - f(X) = X^{n_f} + c_{f,1}X^{n_f - 1} + \cdots + c_{f,n_f}. \tag{77}$$

Expanding the righthand side of (77) and comparing coefficients gives us the desired result.

Lemma 26.6. *The ideal* $\mathfrak{a}$ *is proper.*

Proof. Assume for a contradiction that I is not proper, so $1 \in \mathfrak{a}$. Then we can write 1 as a finite sum

$$1 = \sum_{i=1}^{m} v_i u_{f_i,k_i} \tag{78}$$

where $v_i \in A$ for all $1 \leq i \leq m$. Evaluating $t_{f_i,k_i} = \alpha_{f_i,k_i}$ for each $1 \leq i \leq m$ to both sides of (78) gives us $1 = 0$. This is a contradiction. □

Since I is a proper ideal, Zorn's Lemma guarantees that $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}$ in A. The quotient ring $A/\mathfrak{m}$ is a field and the natural composite homomorphism $K \to A \to A/\mathfrak{m}$ of rings lets us view the field $A/\mathfrak{m}$ as an extension of K since ring homomorphisms out of fields are always injective.

Theorem 26.7. *The field* $A/\mathfrak{m}$ *is an algebraic closure of* K.

Proof. For each indeterminate $t_{f,k}$, let $\bar{t}_{f,k}$ denote its coset in $A/\mathfrak{m}$. Observe that for each nonconstant monic polynomial $f(X)$ in $K[X]$, we have

$$\begin{aligned} f(X) &= X^{n_f} + \sum_{k=1}^{n_f} c_{f,k} X^{n_f - k} \\ &\equiv X^{n_f} + \sum_{k=1}^{n_f} (-1)^k e_k(t_{f,,1}, \dots, t_{f,n_f}) X^{n_f - k} \mod \mathfrak{m} \\ &= \prod_{k=1}^{n_f} (X - \bar{t}_{f,k}). \end{aligned}$$

since $u_{f,1}, \dots, u_{f,n_f} \in \mathfrak{m}$. Thus $f(X)$ splits completely in $(A/\mathfrak{m})[X]$, and since $\bar{t}_{f,k}$ is a root of $f(X)$, we see that each $\bar{t}_{f,k}$ is algebraic over K. It follows that $A/\mathfrak{m}$ is an algebraic extension field of K since $A/\mathfrak{m}$ is generated by the $\bar{t}_{f,k}$'s (as A is generated by the $t_{f,k}$'s) and that every nonconstant monic in $K[X]$ splits completely.

We will now show $A/\mathfrak{m}$ is algebraically closed, and thus it is an algebraic closure of K. Set $F = A/\mathfrak{m}$. It suffices to show every monic irreducible $\pi(X)$ in $F[X]$ has a root in F. We have already seen that any nonconstant monic polynomial in $K[X]$ splits completely in $F[X]$, so let's show $\pi(X)$ is a factor of some monic polynomial in $K[X]$. There is a root α of $\pi(X)$ in some extension of F. Since α is algebraic over F and F is algebraic over K, α is algebraic over K. That implies some monic $f(X)$ in $K[X]$ has α as a root. The polynomial $\pi(X)$ is the minimal polynomial of α in $F[X]$, so $\pi(X) \mid f(X)$ in $F[X]$. Since $f(X)$ splits completely in $F[X]$, we have $\alpha \in F$. □

26.2.1 Counting the Number of Maximal Ideals

In this section, let $f(X)$ to be a monic separable irreducible polynomial over a field K of degree n and express it as

$$f = X^n + \sum_{i=1}^{n} c_i X^{n-i}$$

where $c_i \in K$ for all $1 \leq i \leq n$. Let L be a splitting field of f over K and let $\alpha_1, \ldots, \alpha_n$ be the roots of f in L, so $L = K(\alpha_1, \ldots, \alpha_n)$. Let $T_1, \ldots, T_n$ be indeterminates, and let $R = K[T_1, \ldots, T_n]/\langle u_1, \ldots, u_n \rangle$ where

$$u_i = c_i - (-1)^i e_i(T_1, \ldots, T_n)$$

for each $1 \leq i \leq n$. We denote by t_i to be the image of T_i under the quotient map $K[T_1, \ldots, T_n] \to R$ for each $1 \leq i \leq n$.

Theorem 26.8. *The number of maximal ideals of R is given by*

$$\frac{n!}{|\mathrm{Gal}(L/K)|}$$

Proof. We first note that the maximal ideals of R are all of the form $\ker \psi$ where $\psi \colon R \to L$ is a nonzero K-algebra homomorphism. Indeed, let $\mathfrak{m}$ be a maximal ideal of R and let $\bar{t}_i$ be the image of t_i under the quotient map $\rho \colon R \to R/\mathfrak{m}$ for each $1 \leq i \leq n$. Note that f splits over R as

$$\begin{aligned} f(X) &= X^n + \sum_{i=1}^{n} c_i X^{n-i} \\ &= X^n + \sum_{i=1}^{n_i} (-1)^i e_i(t_1, \ldots, t_n) X^{n-i} \\ &= \prod_{i=1}^{n} (X - t_i). \end{aligned}$$

In particular $f(t_i) = 0$ for all $1 \leq i \leq n$. This implies $f(\bar{t}_i) = 0$ for each $1 \leq i \leq n$. Therefore $R/\mathfrak{m} = K(\bar{t}_1, \ldots, \bar{t}_n)$ is a splitting field of f over K. It follows that there exists a K-algebra isomorphism $\iota \colon R/\mathfrak{m} \to L$. Thus $\mathfrak{m}$ is the kernel of the K-algebra homomorphism $\iota\rho \colon R \to L$.

Thus in order to describe the maximal ideals of R, it suffices to describe the nonzero K-algebra homomorphisms $R \to L$. There is an obvious nonzero K-algebra homomorphism $\varphi \colon R \to L$ given by $\varphi(t_i) = \alpha_i$ for all $1 \leq i \leq n$. Furthermore, if $\pi \in S_n$, then we obtain another nonzero K-algebra homomorphism $\varphi\pi \colon R \to L$ given by $\varphi\pi(t_i) = \alpha_{\pi(i)}$ for all $1 \leq i \leq n$. We claim that this is all of them. Indeed, since $f(t_i) = 0$, we see that any K-algebra homomorphism $R \to L$ must send t_i to some root of f in L, say $\alpha_{\pi(i)}$, for each $1 \leq i \leq n$. Moreover, the $\alpha'_{\pi(i)}s$ must satisfy

$$f(X) = \prod_{i=1}^{n} (X - \alpha_{\pi(i)}).$$

Thus π must be a permutation of $\{1, \ldots, n\}$. It follows that every K-algebra has the form $\varphi\pi$ for some $\pi \in S_n$.

Finally, suppose $\psi_1 \colon R \to L$ and $\psi_2 \colon R \to L$ are two K-algebra homomorphisms. We claim that $\ker \psi_1 = \ker \psi_2$ if and only if there exists a $\sigma \in \mathrm{Gal}(L/K)$ such that $\psi_1 \sigma = \psi_2$ (where we view $\mathrm{Gal}(L/K)$ as a subgroup of S_n in the natural way). Indeed, one direction is clear. For the other direction, let $\rho \colon R \to R/\ker \psi_1$ be the quotient map and let $\overline{\psi}_1 \colon R/\ker \psi_1 \to L$ and $\overline{\psi}_2 = R/\ker \psi_1 \to L$ be the K-algebra isomorhpisms induced by ψ_1 and ψ_2 respectively (so $\overline{\psi}_1 \varrho = \psi_1$ and $\overline{\psi}_2 \pi = \psi_2$). If we define $\sigma = \overline{\psi}_2 \overline{\psi}_1^{-1}$, then it is easy to check that $\psi_1 \sigma = \psi_2$. □

26.3 Uniqueness of Algebraic Closures

Throughout this subsection, let k be a field and $\overline{k}/k$ be a choice of an algebraic closure.

Lemma 26.9. *Let L/k be an algebraic extension and let L'/L be another algebraic extension. There is a k-embedding $i \colon L \hookrightarrow \overline{k}$, and once i is picked there exists a k-embedding $L' \hookrightarrow \overline{k}$ extending i.*

Proof. Since an embedding $i \colon L \hookrightarrow \overline{k}$ realizes the algebraically closed $\overline{k}$ as an algebraic extension of L (and hence as an algebraic closure of L), by renaming the base field as L it suffices to just prove the first part: any algebraic extension admits an embedding into a specified algebraic closure.

Define Σ to be the set of pairs (k', i) where $k' \subseteq L$ is an intermediate extension over k and $i \colon k' \hookrightarrow \overline{k}$ is a k-embedding. Using the inclusion $i_0 \colon k \hookrightarrow \overline{k}$ that comes along with the data of how $\overline{k}$ is realized as an algebraic closure of k, we see that $(k, i_0) \in \Sigma$, so Σ is nonempty. We wish to apply Zorn's Lemma, where we define a partial ordering on Σ by the condition that $(k', i') \leq (k'', i'')$ if $k' \subseteq k''$ inside of L and $i''|_{k'} = i'$. It is a simple exercise in gluing set maps to see that the hypothesis of Zorn's Lemma is satisfied, so there exists a maximal element $(K, i) \in \Sigma$.

We just have to show $K = L$. Pick $x \in L$, so x is algebraic over K (as it is algebraic over k). If $f_x \in K[T]$ is the minimal polynomial of x, then $K(x) \cong K[T]/f_x$. Using $i\colon K \hookrightarrow \overline{k}$ realizes $\overline{k}$ as an algebraic closure of K, so $f_x \in K[T]$ has a root in $\overline{k}$. Pick such a root, say r, and then we define $K[T] \to \overline{k}$ by using i on the coefficients K and sending T to r. This map kills f_x, and hence factors through the quotient to define a map of fields $K[T]/f_x \hookrightarrow \overline{k}$ extending i. Composing this with the isomorphism $K(x) \cong K[T]/f_x$ therefore defines an element $(K(x), i') \in \Sigma$ which dominates (K, i). By maximality, this forces $(K(x), i') = (K, i)$, or in other words $K(x) = K$ as subfields of L. This holds for all $x \in L$ and says exactly $x \in K$. Thus $L = K$, as desired.

□

Theorem 26.10. *Let $\overline{k}_1$ and $\overline{k}_2$ be two algebraic closures of k. Then there exists an isomorphism $\overline{k}_1 \cong \overline{k}_2$ over k.*

Proof. By the lemma, applied to $L = \overline{k}_1$ (algebraic over k) and $\overline{k} = \overline{k}_2$ (an algebraically closed field equipped with a structure of algebraic extension of k), there exists a k-embedding $i\colon \overline{k}_1 \hookrightarrow \overline{k}_2$. Since $\overline{k}_1$ is algebraic over k and $\overline{k}_2$ is algebraically closed, it follows that the k-embedding i realizes $\overline{k}_2$ as an algebraic extension of $\overline{k}_1$. But an algebraically closed field (such as $\overline{k}_1$) admits no non-trivial algebraic extensions, so the map i is forced to be an isomorphism. More concretely, any $y \in \overline{k}_2$ is a root of an irreducible monic $f \in k[T]$, and $f = \prod(T - r_j)$ in $\overline{k}_1[T]$ since $\overline{k}_1$ is algebraically closed, so applying i shows that $i(r_j)$'s exhaust the roots of f in $\overline{k}_2$. Thus, $y = i(r_j)$ for some j, so indeed i is surjective. □

Remark 43. Beware that the isomorphism in the theorem is nearly always highly non-unique (it can be composed with any k-automorphism of $\overline{k}_2$, of which there are many in general). Thus, one should *never* write $\overline{k}_1 = \overline{k}_2$; *always* keep track of the choice of isomorphism. In particular, always speak of *an* algebraic closure rather than *the* algebraic closure; there is no "preferred" algebraic closure except in cases when there are no non-trivial automorphisms over k (which happens for fields which have the property of being "separably closed".

27 Splitting Fields

When K is a field and $f(T) \in K[T]$ is nonconstant, there is a field extension K'/K in which $f(T)$ picks up a root, say α. Then $f(T) = (T - \alpha)g(T)$ where $g(T) \in K'[T]$ and $\deg g = \deg f - 1$. By applying the same process to $g(T)$ and continuing in this way finitely many times, we reach an extension L/K in which $f(T)$ splits into linear factors: in $L[T]$,

$$f(T) = c(T - \alpha_1) \cdots (T - \alpha_n).$$

We call the field $K(\alpha_1, \ldots, \alpha_n)$ that is generated by the roots of $f(T)$ over K a **splitting field of** $f(T)$ **over** K. The idea is that in a splitting field we can find a full set of roots of $f(T)$ and *no smaller field extension of* K has that property. Let's look at some examples.

Example 27.1. The polynomials $T^2 + 3T - 2$ does not split over $\mathbb{Q}$, but it does split over $\mathbb{Q}(\sqrt{17})$. Indeed,

$$T^2 + 3T - 2 = \left(T - \frac{-3 + \sqrt{17}}{2}\right)\left(T - \frac{-3 - \sqrt{17}}{2}\right).$$

Since $\mathbb{Q}(\sqrt{17})$ is the smallest field which contains the roots $(-3 + \sqrt{17})/2$ and $(-3 - \sqrt{17})/2$, it must be a splitting field for $T^2 + 3T - 2$. The polynomial also splits over $\mathbb{R}$, but $\mathbb{R}$ is not a splitting field for $T^2 + 3T - 2$.

Example 27.2. A splitting field of $T^2 + 1$ over $\mathbb{R}$ is $\mathbb{R}(i, -i) = \mathbb{C}$.

Example 27.3. A splitting field of $T^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$, since we pick up two roots $\pm\sqrt{2}$ in the field generated by just one of the roots. A splitting field of $T^2 - 2$ over $\mathbb{R}$ is $\mathbb{R}$ since $T^2 - 2$ splits into linear factors in $\mathbb{R}[T]$.

Example 27.4. In $\mathbb{C}[T]$, a factorization of $T^4 - 2$ is $(T - \sqrt[4]{2})(T + \sqrt[4]{2})(T - i\sqrt[4]{2})(T + i\sqrt[4]{2})$. A splitting field of $T^4 - 2$ over $\mathbb{Q}$ is

$$\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i).$$

In the second description one of the field generators is not a root of the original polynomial $T^4 - 2$. This is a simpler way of writing the splitting field. A splitting field of $T^4 - 2$ over $\mathbb{R}$ is $\mathbb{R}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{C}$.

These examples illustrate that, as with irreducibility, the choice of base field is an important part of determining the splitting field. Over $\mathbb{Q}$, $T^4 - 2$ has a splitting field that is an extension of degree 8, while over $\mathbb{R}$ the splitting field of the same polynomial is an extension (of $\mathbb{R}$!) of degree 2.

Theorem 27.1. *Let K be a field and $f(T)$ be nonconstant in $K[T]$. If L and L' are splitting fields of $f(T)$ over K then $[L : K] = [L' : K]$, there is a field isomorphism $L \to L'$ fixing all of K, and the number of such isomorphisms $L \to L'$ is at most $[L : K]$.*

Proof. $\square$

Example 27.5. Every splitting field of $T^4 - 2$ over $\mathbb{Q}$ has degree 8 over $\mathbb{Q}$ and is isomorphism to $\mathbb{Q}(\sqrt[4]{2}, i)$.

Example 27.6. Every splitting field of $(T^2 - 2)(T^2 - 3)$ over $\mathbb{Q}$ has degree 4 over $\mathbb{Q}$ and is isomorphic to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

27.1 Homomorphisms on Polynomial Coefficients

To prove Theorem (27.1) we will use an inductive argument involving homomorphisms between polynomial rings. Any field homomorphism $\sigma\colon F \to F'$ extends to a ring homomorphism $\sigma\colon F[T] \to F'[T]$ as follows: for $f(T) = \sum_{i=0}^n c_i T^i \in F[T]$, set $(\sigma f)(T) = \sum_{i=0}^n \sigma(c_i) T^i \in F'[T]$. We call this map "applying σ to the coefficients." Writing $f(T) = c_n T^n + c_{n-1} T^{n-1} + \cdots + c_1 T + c_0$, with $c_i \in F$, for $\alpha \in F$, we have

$$\begin{aligned}
\sigma(f(\alpha)) &= \sigma(c_n \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1 \alpha + c_0) \\
&= \sigma(c_n)\sigma(\alpha)^n + \sigma(c_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(c_1)\sigma(\alpha) + \sigma(c_0) \\
&= (\sigma f)(\sigma(\alpha)).
\end{aligned}$$

In particular, if $f(\alpha) = 0$, then

$$\begin{aligned}
(\sigma f)(\sigma(\alpha)) &= \sigma(f(\alpha)) \\
&= \sigma(0) \\
&= 0,
\end{aligned}$$

so σ sends any root of $f(T)$ in F to a root of $(\sigma f)(T)$ in F'.

27.2 Proof of the Theorem

Rather than prove Theorem (27.1) directly, we formula a more general theorem.

Theorem 27.2. *Let $\sigma\colon K \to K'$ be an isomorphism of fields, $f(T) \in K[T]$, L be a splitting field of $f(T)$ over K and L' be a splitting field of $(\sigma f)(T)$ over K'. Then $[L : K] = [L' : K']$, σ extends to an isomorphism $L \to L'$ and the number of such extensions is at most $[L : K]$.*

$$\begin{tikzcd}
L \arrow[r, dashed] \arrow[d, dash] & L' \arrow[d, dash] \\
K \arrow[r, "\sigma"] & K'
\end{tikzcd}$$

Proof. We argue by induction on $[L : K]$. If $[L : K] = 1$, then $f(T)$ splits completely in $K[T]$ so $(\sigma f)(T)$ splits completely in $K'[T]$. Therefore $L' = K'$, so $[L' : K'] = 1$. The only extension of σ to L in this case is σ, so the number of extensions of σ to L is at most $1 = [L : K]$.

Suppose $[L : K] > 1$. Since L is generated as a field over K by the roots of $f(T)$, $f(T)$ has a root $\alpha \in L$ that is not in K. Fix this α for the rest of the proof. Let $\pi(T)$ be the minimal polynomial of α over K, so α is a root of $\pi(T)$ and $\pi(T) \mid f(T)$ in $K[T]$. If there's an isomorphism $\widetilde{\sigma}\colon L \to L'$ extending σ, then $\widetilde{\sigma}(\alpha)$ is a root of $(\sigma\pi)(T)$. Indeed, we have

$$\begin{aligned}
(\sigma\pi)(\widetilde{\sigma}(\alpha)) &= (\widetilde{\sigma}\pi)(\widetilde{\sigma}(\alpha)) \\
&= \widetilde{\sigma}(\pi(\alpha)) \\
&= \widetilde{\sigma}(0) \\
&= 0,
\end{aligned}$$

where the first equality comes from $\pi(T)$ having coefficients in K (so $\widetilde{\sigma} = \sigma$ on those coefficients). Therefore the values of $\widetilde{\sigma}(\alpha)$ - to be determined - must come from roots of $(\sigma\pi)(T)$.

Now we show $(\sigma\pi)(T)$ has a root in L'. Since $\sigma\colon K \to K'$ is an isomorphism, applying σ to coefficients is a ring isomorphism $K[T] \to K'[T]$ (the inverse applies σ^{-1} to coefficients in $K'[T]$), so $\pi(T) \mid f(T)$ implies $(\sigma\pi)(T) \mid (\sigma f)(T)$. Since $\pi(T)$ is monic irreducible, $(\sigma\pi)(T)$ is monic irreducible (ring isomorphisms preserve irreducibility). Since $(\sigma f)(T)$ splits completely in $L'[T]$ by the definition of L', its factor $(\sigma\pi)(T)$ splits completely in $L'[T]$. Pick a root $\alpha' \in L'$ of $(\sigma\pi)(T)$. Set $d = \deg \pi(T) = \deg(\sigma\pi)(T)$, so $d > 1$ (since $d = [K(\alpha) : K] > 1$). This information is in the diagram below, and there are at most d choices for α' in L'. The minimal polynomials of α and α' over K and K' (resp.) are $\pi(T)$ and $(\sigma\pi)(T)$.

$$\begin{tikzcd}
L \arrow[r, dashed] \arrow[d, no head] & L' \arrow[d, no head] \\
K(\alpha) \arrow[r, dashed] \arrow[d, no head, "d"'] & K'(\alpha') \arrow[d, no head, "d"] \\
K \arrow[r, "\sigma"] & K'
\end{tikzcd}$$

There is a *unique* extension of $\sigma\colon K \to K'$ to a field isomorphism $K(\alpha) \to K'(\alpha')$ such that $\alpha \mapsto \alpha'$. First we show uniqueness. If $\sigma'\colon K(\alpha) \to K'(\alpha')$ extends σ and $\sigma'(\alpha) = \alpha'$, then the value of σ' is determined everywhere on $K(\alpha)$ because $K(\alpha) = K[\alpha]$ and

$$\begin{aligned}
\sigma'\left(\sum_{i=0}^{m} c_i\alpha^i\right) &= \sum_{i=0}^{m} \sigma'(c_i)(\sigma'(\alpha))^i \\
&= \sum_{i=0}^{m} \sigma(c_i)\alpha'^i.
\end{aligned}$$

In other words, a K-polynomial in α goes to the corresponding K'-polynomial in α' where σ is applied to the coefficients. Thus there is at most one σ' extending σ with $\sigma'(\alpha) = \alpha'$.

To prove σ' exists, we will build an isomorphism from $K(\alpha)$ to $K'(\alpha')$ with the desired behavior on K and α. Any element of $K(\alpha)$ can be written as $f(\alpha)$ where $f(T) \in K[T]$. It can be like this for more than one polynomial: perhaps $f(\alpha) = g(\alpha)$ where $g(T) \in K[T]$. In that case $f(T) \equiv g(T) \bmod \pi(T)$, so $f(T) = g(T) + \pi(T)h(T)$. Applying σ to coefficients on both sides, which is a ring homomorphism $K[T] \to K'[T]$, we have $(\sigma f)(T) = (\sigma g)(T) + (\sigma\pi)(T)(\sigma h)(T)$, and setting $T = \alpha'$ kills off the second term, leaving us with $(\sigma f)(\alpha') = (\sigma g)(\alpha')$. Therefore it is *well-defined* to set $\sigma'\colon K(\alpha) \to K'(\alpha')$ by $f(\alpha) \mapsto (\sigma f)(\alpha')$. This function is σ on K and sends α to α'. Since applying σ to coefficients is a ring homomorphism $K[T] \to K'[T]$, σ' is a field homomorphism $K(\alpha) \to K'(\alpha')$. For example, if x and y in $K(\alpha)$ are written as $f(\alpha)$ and $g(\alpha)$, then $xy = f(\alpha)g(\alpha) = (fg)(\alpha)$ (evaluation at α is multiplicative) so

$$\begin{aligned}
\sigma'(xy) &= \sigma(fg)(\alpha') \\
&= ((\sigma f)(\sigma g))(\alpha') \\
&= (\sigma f)(\alpha')(\sigma g)(\alpha') \\
&= \sigma'(x)\sigma'(y).
\end{aligned}$$

Using $\sigma^{-1}\colon K' \to K$ to go the other way shows σ' is a field isomorphism.

Place σ' in the field diagram below

$$\begin{tikzcd}
L \arrow[r, dashed] \arrow[d, no head] & L' \arrow[d, no head] \\
K(\alpha) \arrow[r, "\sigma'"] \arrow[d, no head, "d"'] & K'(\alpha') \arrow[d, no head, "d"] \\
K \arrow[r, "\sigma"] & K'
\end{tikzcd}$$

Now we can finally induct on degrees of splitting fields. Take as new base fields $K(\alpha)$ and $K'(\alpha')$, which are isomorphic by σ'. Since L is a splitting field of $f(T)$ over K, it's also a splitting field of $f(T)$ over the larger field $K(\alpha)$. Similarly L' is a splitting field of $(\sigma f)(T)$ over K' and thus also over the larger field $K'(\alpha')$. Since $f(T)$ has its coefficients in K and $\sigma' = \sigma$ on K, we have $(\sigma' f)(T) = (\sigma f)(T)$. So the top square in the above diagram is like the square in the theorem itself, except the splitting field degrees dropped: since $d > 1$,

$$[L : K(\alpha)] = \frac{[L : K]}{d} < [L : K].$$

By induction, $[L : K(\alpha)] = [L' : K'(\alpha')]$ and σ' has an extension to a field isomorphism $L \to L'$. Since σ' extends σ, σ itself has an extension to an isomorphism $L \to L'$ and

$$\begin{aligned}[L : K] &= [L : K(\alpha)]d \\ &= [L' : K'(\alpha')]d \\ &= [L' : K'].\end{aligned}$$

(If the proof started with $K' = K$, it would usually be false that $K(\alpha) = K'(\alpha')$, so Theorem (27.1) is not directly accessible to our inductive proof.)

It remains to show σ has at most $[L : K]$ extensions to an isomorphism $L \to L'$. First we show every isomorphism $\widetilde{\sigma}\colon L \to L'$ extending σ is the extension of some intermediate isomorphism σ' of $K(\alpha)$ with a subfield of L'. From the start of the proof, $\widetilde{\sigma}(\alpha)$ must be a root of $(\sigma\pi)(T)$. Define $\alpha' := \widetilde{\sigma}(\alpha)$. Since $\widetilde{\sigma}|_K = \sigma$, the restriction $\widetilde{\sigma}|_{K(\alpha)}$ is a field homomorphism that is σ on K and sends α to α', so $\widetilde{\sigma}|_{K(\alpha)}$ is an isomorphism from $K(\alpha)$ to $K'(\widetilde{\sigma}(\alpha)) = K'(\alpha')$. Thus $\widetilde{\sigma}$ on L is a lift of the intermediate field isomorphism $\sigma' := \widetilde{\sigma}|_{K(\alpha)}$.

$$\begin{tikzcd}
L \arrow[r, "\widetilde{\sigma}"] \arrow[d, dash] & L' \arrow[d, dash] \\
K(\alpha) \arrow[r, "\sigma'"] \arrow[d, dash, "d"'] & K'(\alpha') \arrow[d, dash, "d"] \\
K \arrow[r, "\sigma"] & K'
\end{tikzcd}$$

By induction on degrees of splitting fields, σ' lifts to at most $[L : K(\alpha)]$ isomorphisms $L \to L'$. Since σ' is determined by $\sigma'(\alpha)$, which is a root of $(\sigma\pi)(T)$, the number of maps σ' is at most $\deg(\sigma\pi)(T) = d$. The number of isomorphisms $L \to L'$ that lift σ is the number of homomorphisms $\sigma'\colon K(\alpha) \to L'$ lifting σ times the number of extensions of each σ' to an isomoprhism $L \to L'$, and that total is at most $d[L : K(\alpha)] = [L : K]$. $\square$

Proposition 27.1. *Let L be a splitting field of a family of polynomials in $K[X]$. Then every irreducible polynomial of $K[X]$ which has a root in L splits into linear factors in L.*

Proof. Note that L has the form $L = K(\{b_\alpha\})$ where each b_α is a root of some polynomial in that family. Let π be an irreducible polynomial in $K[X]$ with a root $a \in L$. Then there is some polynomial f in $K[X_1, \ldots, X_n]$ such that $f(b_{\alpha_1}, \ldots, b_{\alpha_n}) = a$. To clean notation in what follows, write $b_i = b_{\alpha_i}$ for each $1 \le i \le n$. We claim that all of the other roots of π are in L and can be obtained by permuting the b_i in $f(b_1, \ldots, b_n)$. To do this, we work inside an algebraic closure M of L (and we may assume that we have inclusions $K \subset L \subset M$). Let a' be another root of π inside M. There there exists a K-automorphism σ of M which takes a to a'. Furthermore σ acts as a permutation of the b_i's, that is $\sigma(b_i) = b_{\rho(i)}$ for some $\rho \in S_n$ for each $1 \le i \le n$. In particular, when we apply σ to $f(b_1, \ldots, b_n) = a$, we obtain

$$f(b_{\rho(1)}, \ldots, b_{\rho(n)}) = \sigma f(b_1, \ldots, b_n) = \sigma a = a'.$$

Thus all of the roots of π belong to L, and it follows that π splits completely in L. $\square$

28 Separability

Definition 28.1. Let K be a field. We have the following definitions

1. Let $f(T)$ be a nonzero polynomial over K.

   (a) We say f is **separable** when it has distinct roots in a splitting field over K.

   (b) If f has a multiple root in a splitting field, then it is called **inseparable**.

   (c) We say f is **purely inseparable** if it has the form $X^{p^d} - a$ for some p positive prime, $d \geq 0$, and $a \in K$.

2. Let α be an algebraic number over K.

   (a) We say α is **separable over** K when its minimal polynomial over K is separable.

   (b) If the minimal polynomial of α is inseperable over K, then we say α is **inseperable over** K. Note that if $\alpha \in L$ where L/K is a field extension, then the minimal polynomial of α over L is simply $T - \alpha$, which is clearly separable. Thus we really do need the qualifier "over K" in this definition.

   (c) We say α is **purely inseperable over** K if its minimal polynomial over K is purely inseparable.

3. Let L/K be an algebraic field extension.

   (a) We say L/K is a **separable** field extension if every $\alpha \in L$ is separable over K.

   (b) We say L/K is an **inseparable** field extension if there exists one $\alpha \in L$ which is inseparable over K.

   (c) We say L/K is a **purely inseparable** field extension if every $\alpha \in L$ is purely inseperable over K.

Example 28.1. The polynomial $T^2 - T$ is separable over any field K since its roots are 0 and 1 (every field contains 0 and 1). The polynomial $T^3 - 2$ is separable over $\mathbb{Q}$ since it splits into distinct linear factors over the the field $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ of f over $\mathbb{Q}$ as

$$T^3 - 2 = (T - \sqrt[3]{2})(T - \zeta_3\sqrt[3]{2})(T - \zeta_3^2\sqrt[3]{2}).$$

Thus it has distinct roots in the splitting field $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ of f over $\mathbb{Q}$. On the other hand, $T^3 - 2$ is not separable over $\mathbb{F}_3$. Indeed, it factors over $\mathbb{F}_3$ into linear factors as

$$T^3 - 2 = (T + 1)^3.$$

Thus is has a triple root in $\mathbb{F}_3$.

28.1 Separable Polynomials

From Definition (28.1), checking a polynomial is separable requires building a splitting field to check the roots are distinct. It turns out however that there is a criterion for deciding a polynomial is separable (that is, having no multiple roots) without having to work in a splitting field. Indeed, we can use differentiation in $K[T]$ to describe the separability condition without leaving $K[T]$.

28.1.1 Criterion for Nonzero Polynomial to be Separable

Theorem 28.1. *A nonzero polynomial in $K[T]$ is separable if and only if it is relatively prime to its derivative in $K[T]$.*

Proof. Let f be a nonzero polynomial in $K[T]$ and let L be a splitting field of f over K.

Case 1: Suppose f is separable and let $b \in L$ be any root of f. We claim that b is not a root of f'. Indeed, write $f = (T - b)h$ where $h \in L[T]$ with $h(b) \neq 0$. Since $f'(b) = h(b) \neq 0$, we see that b is not a root of f'. In particular, this implies f and f' have no common roots, so they have no common factors in $K[T]$: they are relatively prime.

Case 2: Suppose f is inseparable. Then there exists a repeated root $b \in L$ of f. We claim that b is also a root of f'. Indeed, write $f = (T - b)^2 g$ where $g \in L[T]$. Then the product rule shows

$$f' = (T - b)^2 g' + 2(T - b)g,$$

so $f'(b) = 0$. In particular, since f and f' have b as a common root, they are both divisible by the minimal polynomial of b over K. Thus f and f' are not relatively prime in $K[T]$. Taking the contrapositive, if f and f' are relatively prime in $K[T]$, then f has no repeated root. $\square$

When we are given a specific $f(T)$, whether or not $f(T)$ and $f'(T)$ are relatively prime can be checked by Euclid's algorithm for polynomials.

Example 28.2. In $\mathbb{F}_3[T]$, let $f(T) = T^6 + T^5 + T^4 + 2T^3 + 2T^2 + T + 2$. Using Euclid's algorithm in $\mathbb{F}_3[T]$ on $f(T)$ and $f'(T)$,

$$\begin{aligned} f(T) &= f'(T)(2T^2 + T) + (2T^2 + 2) \\ f'(T) &= (2T^2 + 2)(T^2 + 2T + 2), \end{aligned}$$

so $(f(T), f'(T)) = 2T^2 + 2$. The greatest common divisor is nonconstant, so $f(T)$ is inseparable. In fact, $f(T) = (T^2 + 1)^2(T^2 + T + 2)$. Notice we were able to detect that $f(T)$ has a repeated root *before* we gave its factorization.

Example 28.3. Let $f(T) = T^n - a$ where $a \in K^\times$. The derivative of $f(T)$ is nT^{n-1}. If $n = 0$ in K, then $f'(T) = 0$ and $(f(T), f'(T)) = f(T)$ is nonconstant, so $T^n - a$ is inseparable. If $n \neq 0$ in K, then $f'(T) \neq 0$ and $(T^n - a, nT^{n-1}) = 1$ since T doesn't divide $T^n - a$. Therefore $T^n - a$ is separable in over K if and only if $n \neq 0$ in K.

28.1.2 Criterion for Irreducible Polynomial to be Separable

Theorem 28.2. *For any field K, an irreducible polynomial over K is separable if and only if its derivative if not 0. In particular, when K has characteristic 0 every irreducible over K is separable and when K has characteristic p, an irreducible over K is separable if and only if it is not a polynomial in T^p.*

Proof. Let $\pi(T)$ be irreducible over K. Separability is equivalent to $(\pi, \pi') = 1$ by Theorem (28.1). If π and π' are not relatively prime, then $\pi \mid \pi'$ since π is irreducible. Taking the derivative drops degrees, so having π' be divisible by π forces $\pi' = 0$. Conversely, if $\pi' = 0$, then $(\pi, \pi') = \pi$ is nonconstant, so π is inseparable by Theorem (28.1). Thus separability of π is equivalent to $\pi' \neq 0$.

When K has characteristic 0, every irreducible over K has nonzero derivative since any nonconstant polynomial has nonzero derivative. So all irreducibles over K are separable. Now suppose K has characteristic p. Let π be an irreducible in $K[T]$ such that π is inseperable, and express π as

$$\pi = a_n T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0,$$

where we may assume that $a_n \neq 0$ in K. The condition $\pi' = 0$ means $ia_i = 0$ in K for $0 \leq i \leq n$. This implies $p \mid i$ whenever $a_i \neq 0$, so the only nonzero terms in π occur in degrees divisible by p. In particular, $n = \deg \pi$ is a multiple of p, say $n = pm$. Write each exponent of a nonzero term in π as a multiple of p:

$$\pi = a_{pm}T^{pm} + a_{p(m-1)}T^{p(m-1)} + \cdots + a_p T^p + a_0 = \widetilde{\pi}(T^p)$$

where $\widetilde{\pi} \in K[T]$. So $\pi \in K[T^p]$. Conversely, if $\pi(T) = \widetilde{\pi}(T^p)$ is a polynomial in T^p, then c $\pi' = \widetilde{\pi}'(T^p)pT^{p-1} = 0$, so π is inseparable in $K[T]$. □

Example 28.4. Let $K = \mathbb{F}_3(u)$ be a rational function field over $\mathbb{F}_3$. The polynomial $T^{10} + u^2T^5 + u \in K[T]$ is irreducible by Eisenstein's criterion. It is also separable since it is irreducible and its derivative $T^9 + 2u^2T^4$ is nonzero.

Example 28.5. Let K be a field with positive characteristic p and let $f \in K[x]$ be an irreducible polynomial such that $\deg f = n$. If $p \nmid n$, then f is separable.

28.1.3 Multiplicities for Inseparable Irreducible Polynomials

When a polynomial is inseparable, at least one of its roots has multiplicity greater than 1. The multiplicities of all the roots need not agree. For example, $X^2(X-1)^3 = 0$ has 0 as a root with multiplicity 2 and 1 as a root with multiplicity 3. This polynomial is reducible, so it is a dull example. When an inseparable polynomial is *irreducible*, which can only happen in positive characteristic, it is natural to ask how the multiplicities of different roots are related to each other. In fact, the multiplicities are all the same:

Theorem 28.3. *Let $\pi \in K[T]$ be irreducible, where K has characteristic $p > 0$. Write $\pi = \pi_{\text{sep}}(T^{p^m})$ where $m \geq 0$ is as large as possible (if $m = 0$, then $\pi = \pi_{\text{sep}}$). Then π_{sep} is irreducible and separable in $K[T]$, and each root of π has multiplicity p^m.*

Proof. Since $\deg \pi = p^m \deg \pi_{\text{sep}}$, there is a largest possible m that can be used. Any nontrivial factorization of π_{sep} gives one for π (if $\pi_{\text{sep}} = fg$, then $\pi = f(T^{p^m})g(T^{p^m})$), so π_{sep} is irreducible in $K[X]$. By the maximality of

m, we see that π_{sep} is not a polynomial in T^p, which means its derivative is not 0, so it must be separable. Now factor π_{sep} in a splitting field over K, say

$$\pi_{\text{sep}} = a(T - b_1) \cdots (T - b_d),$$

where the b_i's are distinct since π_{sep} is separable. In a large enough field, we have $b_i = \beta_i^{p^m}$. Since the pth power map is injective in characteristic p, distinctness of the b_i's implies distinctness of the β_i's. Therefore

$$\begin{aligned}\pi &= \pi_{\text{sep}}(T^{p^m}) \\ &= a(T^{p^m} - b_1) \cdots (T^{p^m} - b_d) \\ &= a(T^{p^m} - \beta_1^{p^m}) \cdots (T^{p^m} - \beta_d^{p^m}), \\ &= a(T - \beta_1)^{p^m} \cdots (T - \beta_d)^{p^m},\end{aligned}$$

which shows the roots of π (the β_i's) are the p^mth roots of the roots of π_{sep} (the b_i's), and each root of π has multiplicity p^m. □

28.2 Separable Extensions

Theorem 28.4. *Let L/K be a finite extension of fields with $[L : K] = n$ and $\sigma \colon K \to F$ a field embedding.*

$$\begin{tikzcd} L \arrow[dr, dashed] \arrow[dd, dash, "n"'] & \\ & E \\ K \arrow[ur, "\sigma"'] & \end{tikzcd}$$

1. *The number of extensions of σ to an embedding $L \to E$ is at most n.*
2. *If L/K is inseparable then the number of extensions of σ to an embedding $L \to E$ is less than n.*
3. *If L/K is separable then there is a field F/E such that the number of extensions of σ to an embedding $L \to F$ is equal to n.*

Proof. 1. We argue by induction on $n = [L : K]$. If $n = 1$ then $L = K$ and the result is clear. Now suppose $n > 1$. Choose $b \in L$ such that $b \notin K$ and set $m := [K(b) : K]$ (so $m \leq n$). Our field diagram looks like the following.

$$\begin{tikzcd} L \arrow[d, dash] & \\ K(b) \arrow[d, dash] & E \\ K \arrow[ur, "\sigma"'] & \end{tikzcd}$$

To bound the number of extensions of σ to an embedding of L into E, we first bound the number of extensions of σ to an embedding $\tau \colon K(b) \to E$ and then bound the number of extensions of any such τ to an embedding $L \to E$.

$$\begin{tikzcd} L \arrow[d, dash] & \\ K(b) \arrow[r, "\tau"] \arrow[d, dash] & E \\ K \arrow[ur, "\sigma"'] & \end{tikzcd}$$

Let $\pi(T)$ be the minimal polynomial of b over K. From the proof that two splitting fields of a polynomial are isomorphic, the number of τ's extending σ is equal the number of roots in E of $\sigma\pi$. The number of these roots is *at most* the degree of $\sigma\pi$, which equals $\deg \pi = [K(b) : K] = m$. This upper bound could be strict for two reasons: $\sigma\pi$ might not split in $E[T]$ or it could split but be inseparable. Let F/E be a splitting field of $\sigma\pi$. Thus in F we can write

$$\sigma\pi = (T - \sigma b_1)^{p^k} \cdots (T - \sigma b_m)^{p^k},$$

where $k \geq 0$ is chosen as large as possible (if $k = 0$, then $\sigma\pi$ is separable) and where $\beta_i \in F$ are the roots of $\sigma\pi$ (where we set $\beta_1 = \sigma(b)$).

$$\sigma\pi = (T - \sigma(b))$$

Once we have extended σ to some τ on $K(b)$, we count how many ways τ extends to L. As in the proof that splitting fields are isomorphic, the trick is to consider $K(b)$ as the new base field, with τ playing the role of σ. Since $b \notin K$ we have

$$[L : K(b)] < [L : K],$$

so by induction on the field degree the number of extensions of $\tau \colon K(b) \to E$ to an embedding of L into E is at most $[L : K(b)]$. Multiplying the upper bounds on the number of extensions of σ to $K(b)$ and the number of further extensions up to L, the number of extensions of σ to L is at most

$$[L : K(b)][K(b) : K] = [L : K],$$

so by induction we're done.

2. When L/K is inseparable, some $b \in L$ is inseparable over K. Running through the first part of the proof of (1) with this b, its minimal polynomial π in $K[T]$ is inseparable, so $\sigma\pi$ is inseparable in $E[T]$. This inseparability forces the number of extensions of σ to $K(b)$ to be *less* than $[K(b) : K] = \deg \pi$. Indeed, we have

$$\pi(T)$$

By (1), the number of extensions up to L of any field embedding $K(\alpha) \to F$ is at most $[L : K(\alpha)]$, so the number of extensions of σ to L is strictly less than

$$[L : K(\alpha)][K(\alpha) : K] = [L : K].$$

3. Write $L = K(\alpha_1, \dots, \alpha_r)$ with each α_i separable over K. We want to construct a field $F' \supseteq F$ such that $\sigma \colon K \to F$ has $[L : K]$ extensions to embeddings of L into F'. We will argue in a similar way to (1), but replacing F with some larger F' will let the upper bound on the number of embeddings in the proof of (1) be reached. □

28.2.1 Transitivity of Separable Extensions

Proposition 28.1. *Let $M/L/K$ be an extension of fields. Then M/K is separable if and only if M/L and L/K are separable.*

Proof. First suppose M/L and L/K are seperable. We want to show that M/K is separable. Let $c \in M$. Note that if $c \in L$, then c is seperable since L/K is seperable, so we may assume that $c \in M \backslash L$. Let π_K be the minimal polynomial of c over K and let π_L be the minimal polynomial of c over L. We have $\pi_L g = \pi_K$ for some $g \in L[X]$. □

Proposition 28.2. *Let $F \subseteq K \subseteq L$ be an extension of fields and suppose L/F is algebraic. Then L/F is separable if and only if L/K and K/F are separable.*

Proof. Suppose that L/F is separable. Clearly K/F is separable since K is a subfield of L which contains F, so it remains to show that L/K is separable. Let $\alpha \in L$, let $\pi_{\alpha,K}(X)$ be the minimal polynomial of α over K, and let $\pi_{\alpha,F}(X)$ be the minimal polynomial of α over F. Then $\pi_{\alpha,K} \mid \pi_{\alpha,F}$ in $K[X]$, so

$$\pi_{\alpha,K}(X)g(X) = \pi_{\alpha,F}(X) \tag{79}$$

for some $g(X) \in K[X]$. Now differentiate both sides of (79) and set $X = \alpha$ to get

$$\pi'_{\alpha,K}(\alpha)g(\alpha) = \pi'_{\alpha,F}(\alpha).$$

Then $\pi'_{\alpha,F}(\alpha) \neq 0$ since otherwise this would imply $\pi_{\alpha,F} \mid \pi'_{\alpha,F}$ which would contradict separability of α over F. Similarly $g(\alpha) \neq 0$ since otherwise this would imply $\pi_{\alpha,K} \mid g$ which would imply $\pi^2_{\alpha,K} \mid \pi_{\alpha,F}$ which would again contradict separability of α over F.

Conversely, suppose that L/K and K/F are both separable. Let $\alpha \in L$, let $\pi_{\alpha,K}(X)$ be the minimal polynomial of α over K, and let $\pi_{\alpha,F}(X)$ be the minimal polynomial of α over F. If $\alpha \in K$, then α is separable over F since K/F is a separable extension, thus we may assume $\alpha \notin K$. Then $\pi_{\alpha,K} \mid \pi_{\alpha,F}$ in $K[X]$, so

$$\pi_{\alpha,K}(X)g_1(X) = \pi_{\alpha,F}(X) \tag{80}$$

for some $g_1(X) \in K[X]$. Now differentiate both sides of (79) and set $X = \alpha$ to get

$$\pi'_{\alpha,K}(\alpha)g_1(\alpha) = \pi'_{\alpha,F}(\alpha).$$

Then $\pi'_{\alpha,K}(\alpha) \neq 0$ since otherwise this would imply $\pi_{\alpha,K} \mid \pi'_{\alpha,K}$ which would contradict separability of α over K. If $g_1(\alpha) = 0$, then $\pi_{\alpha,K} \mid g$ which would imply $\pi^2_{\alpha,K} \mid \pi_{\alpha,F}$ which would again contradict separability of α over F. Let $\alpha \in L$ and let $\pi_{\alpha,K}(X)$ be its minimal polynomial of K and let $\pi_{\alpha,F}(X)$ be its minimal polynomial over F. If $\alpha \in K$, then the result is clear, so assume $\alpha \notin K$. Thus $\pi_{\alpha,K}(\alpha) \neq 0$. We wish to show that $\pi_{\alpha,F}$ is separable. Observe that $\pi_{\alpha,K} \mid \pi_{\alpha,F}$ in $F[X]$ implies $\pi_{\alpha,K} f = \pi_{\alpha,F}$ for some $f(X) \in F[X]$. Also, note that since $\pi_{\alpha,K}$ is separable and irreducible, we have

$$\begin{aligned}
\pi'_{\alpha,F}(X) &= \pi'_{\alpha,K}(X)f(X) + \pi_{\alpha,K}(X)f'(X) \\
&= \pi_{\alpha,K}(X)f'(X)
\end{aligned}$$

Note that $f'(\alpha) \neq 0$ since $\deg f' < \deg \pi_{\alpha,F}$, therefore $\pi'_{\alpha,F}(\alpha) \neq 0$. In particular, $\pi'_{\alpha,F}(X) \neq 0$. Therefore $\pi_{\alpha,F}$ is separable which implies α is separable. □

We have

$$\pi_L = T^m + b_{m-1}T^{m-1} + \cdots + b_1 T + b_0 = (T - c_1)(T - c_2) \cdots (T - c_m)$$

where $b_i \in L$ and where $c = c_1$. We also have

$$\pi_K = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0$$

where $a_i \in K$. In particular,

28.2.2 Classification of Finite Separable Extensions

Theorem 28.5. *Let L/K be a finite extension and write $L = K(b_1, \dots, b_n)$. Then L/K is separable if and only if each b_i is separable over K.*

Proof. If L/K is separable, then each b_i is separable over K by definition of separable extensions. Conversely, suppose each b_i is seperable over K. We have □

Proof. We prove by induction on n. The base case $n = 1$ says $K(b)/K$ is seperable if and only if b is seperable over K. If Let π be the minimal polynomial of b over K and let N/K be a splitting field of π. Then in N, we have

$$\pi = (T - b_1)(T - b_2) \cdots (T - b_d)$$

where we set $b = b_1$ and where the b_i are distinct. □

Let M/L be a finite extension such that M/K is Galois. Suppose $b \in L$ is separable over K, set $m = [K(b) : K]$, and let $\pi(T)$ be the minimal polynomial of b over K. Then π splits over M as

$$\pi = (T - b_1) \cdots (T - b_m)$$

where $b_1, \dots, b_m \in M$ are the *distinct* K-conjugates of b in M (say with $b_1 = b$). A K-embedding $\sigma\colon K(b) \hookrightarrow M$ is completely dermined by where it maps b.. Furthermore, σ must map b to a K-conjugate of b, so there are at most m K-embeddings. For each $1 \leq i \leq m$, let $\sigma_i\colon K(b) \hookrightarrow M$ be the K-embedding defined by $\sigma_i(b) = b_i$. For $i \neq j$, we have $b_i \neq b_j$ which implies $\sigma_i \neq \sigma_j$. Thus there are precisely m K-embeddings $K(b) \hookrightarrow M$ (namely $\sigma_1, \dots, \sigma_m$).

Theorem 28.6. *(Primitive Element Theorem) Any finite separable extension of K has the form $K(\gamma)$ for some γ.*

When K has characteristic 0, all of its finite extensions are separable, so the primitive element theorem says any finite extension of K has the form $K(\gamma)$ for some γ.

28.3 Separable and Inseparable Degree

Let K/k be a finite extension, and k'/k the separable closure of k in K, so K/k' is purely inseparable. This yields two refinements of the field degree: the **separable degree** $[K : k]_s := [k' : k]$ and the **inseparable degree** $[K : k]_i := [K : k']$ (so their product is $[K : k]$, and $[K : k]_i$ is always a p-power).

Example 28.6. Suppose $K = k(a)$, and $f \in k[x]$ is the minimal polynomial of a. Then we have $f = f_{\text{sep}}(x^{p^n})$ where $f_{\text{sep}} \in k[x]$ is the separable irreducible over k, and a^{p^n} is a root of f_{sep} (so the monic irreducible f_{sep} is the minimal polynomial of a^{p^n} over k). Thus, we get a tower of field extensions

$$k \subseteq k(a^{p^n}) \subseteq K$$

whose lower layer is separable and upper layer is purely inseparable (as $K = k(a)$ and the minimal polynomial of a over $k(a^{p^n})$ is $x^{p^n} - a^{p^n}$). Hence, $K/k(a^{p^n})$ has no subextension that is a nontrivial separable extension of k', so $k' = k(a^{p^n})$, which is to say

$$[k(a) : k]_s = [k' : k] = [k(a^{p^n}) : k] = \deg f_{\text{sep}}$$
$$[k(a) : k]_i = [K : k'] = [K : k]/[k' : k] = (\deg f)/(\deg f_{\text{sep}}) = p^n.$$

If one tries to prove directly that the separable and inseparable degrees are multiplicative in towers from the definitions, one runs into the problem that in general one cannot move all inseparability to the "bottom" of a finite extension (in contrast with separability). This is illustrated by:

Example 28.7. Let $k = \mathbb{F}_p(X, Y)$ be the fraction field of $\mathbb{F}_p[X, Y]$. Let $f = T^{p^2} + XT^p + Y \in k[T]$. Let $A = \mathbb{F}_p[X, T]$ (so A is a UFD with fraction field $\mathbb{F}_p(X, T)$. Then since f is irreducible in $A[Y]$, it must be irreducible in $A(Y)$ by Gauss' Lemma. Next let $R = \mathbb{F}_p(Y)[T]$. Then since f is irreducible in $R[X] = A(Y)$, it must be irreducible in $R(X) = k[T]$, again by Gauss' Lemma. Thus, it is well-posed to define $L = k(a)$ for a root a of f; this is an extension of k of degree p^2.

Clearly $f = h(T^p)$ with $h = T^p + XT + Y$ visibly separable, so the extension L/k is not separable yet contains the degree p subextension $E := k(a^p)$ that is separable of degree p over k. We claim that E is the unique field strictly between L and k, so L/k cannot be expressed as a tower of a separable extension on top of a purely inseparable one!

29 Trace and Norm

29.1 Definition of Trace, Norm, and Characteristic Polynomial

Let L/K be a finite field extension. We associate each element α of L the K-linear transformation $\mathrm{m}_\alpha : L \to L$, where m_α is multiplication by α, that is,

$$\mathrm{m}_\alpha(x) = \alpha x$$

for all $x \in L$. Suppose $\mathbf{e} = (e_1, \dots, e_n)$ is an ordered K-basis of L. The matrix representation of m_α with respect to the basis $\mathbf{e}$ will be denoted by $[\mathrm{m}_\alpha]_{\mathbf{e}}$. If the basis $\mathbf{e}$ is clear from context, then will will simplify this notation to just $[\mathrm{m}_\alpha]$. If $\mathbf{e}' = (e_1', \dots, e_n')$ is another ordered K-basis of L and C is a change of basis matrix from $\mathbf{e}$ to $\mathbf{e}'$, then $\mathbf{e}' = \mathbf{e}C$ and

$$[\mathrm{m}_\alpha]_{\mathbf{e}'} = C^{-1}[\mathrm{m}_\alpha]_{\mathbf{e}}C.$$

In particular, the trace and norm of the matrix represenation of α does not depend on the basis. Now let us define the trace and norm.

Definition 29.1. Let L/K be a finite field extension and let $\alpha \in L$. We define the **trace function** $\mathrm{Tr}_{L/K} : L \to K$ and **norm function** $\mathrm{N}_{L/K} : L \to K$ as follows: choose any ordered K-basis $\mathbf{e} = (e_1, \dots, e_n)$ of L and for each $\alpha \in K$ let $[\mathrm{m}_\alpha]$ be the matrix representation of m_α with respect to this basis. Then we set

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}[\mathrm{m}_\alpha] \quad \text{and} \quad \mathrm{N}_{L/K}(\alpha) = \det[\mathrm{m}_\alpha]$$

We also define the **characteristic polynomial** of α relative to the extension L/K to be the polynomial

$$\chi_{\alpha,L/K}(X) = \det(X \cdot I_n - [\mathrm{m}_\alpha]) \in K[X],$$

where $n = [L : K]$.

Let L/K be a finite extension of fields and let $\alpha \in L$. If we build a K-basis of L by first picking a basis of $K(\alpha)$ and then picking a basis of L over $K(\alpha)$, we get a 'block' matrix for m_α consisting of $[L : K(\alpha)]$ copies of the smaller square matrix for m_α along the main diagonal. In particular, we have

$$\mathrm{Tr}_{L/K}(\alpha) = [L : K(\alpha)]\mathrm{Tr}_{K(\alpha)/K}(\alpha) \quad \text{and} \quad \mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{K(\alpha)/K}(\alpha)^{[L:K(\alpha)]}.$$

This shows that $\mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha)$ essentially only depend on the field extension $K(\alpha)/K$ (which is intrinsic to α, or the minimal polynomial of α). In fact, if $\pi_{\alpha,K}(X)$ denotes the minimal polynomial of α over K, then we also have

$$\pi_{\alpha,K}^{[L:K(\alpha)]} = \chi_{\alpha,L/K}$$

by the same reasoning as above.

Example 29.1. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\gamma)$ for γ a root of $X^3 - X - 1$. Then $\gamma^3 = 1 + \gamma$. Use the basis $\{1, \gamma, \gamma^2\}$. For $\alpha = a + b\gamma + c\gamma^3$ with a, b,and c rational, multiply α by $1, \gamma$, and γ^2:

$$\begin{aligned}\alpha \cdot 1 &= a + b\gamma + c\gamma^2 \\ \alpha \cdot \gamma &= a\gamma + b\gamma^2 + c\gamma^3 = c + (a+c)\gamma + b\gamma^2 \\ \alpha \cdot \gamma^2 &= c\gamma + (a+c)\gamma^2 + b\gamma^3 = b + (b+c)\gamma + (a+c)\gamma^2.\end{aligned}$$

Therefore $[\mathrm{m}_\alpha]$ equals

$$\begin{pmatrix} a & c & b \\ b & a+c & b+c \\ c & b & a+c \end{pmatrix}.$$

Thus we have

$$\begin{aligned}\mathrm{Tr}_{L/K}(\alpha) &= 3a + 2c \\ \mathrm{N}_{L/K}(\alpha) &= a^3 + 2a^2c - ab^2 - 3abc + ac^2 + b^3 - bc^2 + c^3 \\ \chi_{\alpha,L/K}(X) &= X^3 - (3a+2c)X^2 + (b^2 + 3bc - c^2 - 4ac - 3a^2)X - (a^3 + 2a^2c - ab^2 - 3abc + ac^2 + b^3 - bc^2 + c^3)\end{aligned}$$

For any $n \times n$ square matrix A, its trace and determinant appear up to sign as coefficients in its characteristic polynomial:

$$\det(XI_n - A) = X^n - \mathrm{tr}(A)X^{n-1} + \cdots + (-1)^n \det A.$$

Thus

$$\chi_{\alpha,L/K}(X) = X^n - \mathrm{Tr}_{L/K}(\alpha)X^{n-1} + \cdots + (-1)^n \mathrm{N}_{L/K}(\alpha).$$

This tells us the trace and norm of α are, up to sign, coefficients of the characteristic polynomial of α, which can been seen in Example (29.1). Unlike the minimal polynomial of α over K, whose degree $[K(\alpha) : K]$ varies with K, the degree of $\chi_{\alpha,L/K}(X)$ is always n, which is independent of the choice of α in L.

Theorem 29.1. *Every α in L is a root of its own characteristic polynomial $\chi_{\alpha,L/K}(X)$.*

Proof. This is a consequence of the Cayley-Hamilton theorem in linear algebra. □

29.1.1 Properties of Trace and Norm

Proposition 29.1. *Let L/K be a finite field extension. The trace $\mathrm{Tr}_{L/K} \colon L \to K$ is K-linear and the norm $\mathrm{N}_{L/K} : L \to K$ is multiplicative. Moreover, $\mathrm{N}_{L/K}(L^\times) \subseteq K^\times$.*

Proof. Let $\alpha, \beta \in L$ and let $a, b \in K$. Choose any basis of L over K. Then we have

$$\begin{aligned}\mathrm{Tr}_{L/K}(a\alpha + b\beta) &= \mathrm{tr}[\mathrm{m}_{a\alpha+b\beta}] \\ &= \mathrm{tr}[a\mathrm{m}_\alpha + b\mathrm{m}_\beta] \\ &= a\mathrm{tr}[\mathrm{m}_\alpha] + b\mathrm{tr}[\mathrm{m}_\beta] \\ &= a\mathrm{Tr}_{L/K}(\alpha) + b\mathrm{Tr}_{L/K}(\beta).\end{aligned}$$

Similarly we have

$$\begin{aligned}\mathrm{N}_{L/K}(\alpha\beta) &= \det[m_{\alpha\beta}] \\ &= \det[\mathrm{m}_\alpha \mathrm{m}_\beta] \\ &= \det[\mathrm{m}_\alpha]\det[\mathrm{m}_\beta] \\ &= \mathrm{N}_{L/K}(\alpha)\mathrm{N}_{L/K}(\beta).\end{aligned}$$

Thus $\mathrm{Tr}_{L/K}$ is K-linear and $\mathrm{N}_{L/K}$ is multiplicative. For the last statement, let $\alpha \in L^\times$. Then

$$\begin{aligned}1 &= \mathrm{N}_{L/K}(1) \\ &= \mathrm{N}_{L/K}(\alpha\alpha^{-1}) \\ &= \mathrm{N}_{L/K}(\alpha)\mathrm{N}_{L/K}(\alpha^{-1}).\end{aligned}$$

It follows that $\mathrm{N}_{L/K}(\alpha) \in K^\times$. □

Lemma 29.2. *Assume that L/K is not separable. Then $\mathrm{Tr}_{L/K} = 0$.*

Proof. Let $\alpha \in L$. Since L/K is not separable, then $p = \mathrm{char}(K) > 0$ and either $L/K(\alpha)$ is not separable or else $K(\alpha)/K$ is not separable. In the first case, $[L : K(\alpha)]$ is divisible by the inseparability degree $[L : K(\alpha)]_i > 1$ in $\mathbb{Z}$ and so is divisible by p, whence $[L : K(\alpha)] = 0$ in K. In the second case, the minimal polynomial $\pi_{\alpha,K}$ of α over K is a polynomial in X^p, so no monomials of consecutive positive degrees appear in $\pi_{\alpha,K}$. Since $\pi_{\alpha,K} = \chi_{\alpha,K(\alpha)/K}$ and $\mathrm{Tr}_{K(\alpha)/K}(\alpha)$ is the second highest coefficient of $\chi_{\alpha,K(\alpha)/K}$ (up to sign), we see that $\mathrm{Tr}_{L/K}(\alpha) = 0$. Since α was arbitrary, it follows that $\mathrm{Tr}_{L/K} = 0$. □

29.2 Trace and Norm For a Galois Extension

Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. We can express characteristic polynomials, traces, and norms for the extension L/K in terms of G.

Theorem 29.3. *When L/K is a finite Galois extension with Galois group G and $\alpha \in L$, then*

$$\chi_{\alpha,L/K}(X) = \prod_{\sigma \in G}(X - \sigma(\alpha)).$$

In particular,

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha), \quad \textit{and} \quad \mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Proof. Let $\pi_{\alpha,K}(X)$ be the minimal polynomial of α over K, so $\chi_{\alpha,L/K} = \pi_{\alpha,K}^{n/d}$, where $n = [L : K]$ and $d = [K(\alpha) : K] = \deg \pi_{\alpha,K}$. From Galois theory,

$$\pi_{\alpha,K}(X) = \prod_{i=1}^{d}(X - \sigma_i(\alpha))$$

where $\sigma_1(\alpha), \dots, \sigma_d(\alpha)$ are all the distinct values of $\sigma(\alpha)$ as σ runs over the Galois group. For each $\sigma \in G$, we have $\sigma(\alpha) = \sigma_i(\alpha)$ for a unique i from 1 to d. Moreover, $\sigma(\alpha) = \sigma_i(\alpha)$ if and only if $\sigma \in \sigma_i H$, where

$$H = \{\tau \in G \mid \tau(\alpha) = \alpha\} = \mathrm{Gal}(L/K(\alpha)).$$

Therefore as σ runs over G, the number $\sigma_i(\alpha)$ appears as $\sigma(\alpha)$ whenever σ is in the left coset $\sigma_i H$, so $\sigma_i(\alpha)$ occurs $|H|$ times, and

$$\begin{aligned} |H| &= [L : K(\alpha)] \\ &= [L : K]/[K(\alpha) : K] \\ &= n/d. \end{aligned}$$

Therefore

$$\begin{aligned} \prod_{\sigma \in G}(X - \sigma(\alpha)) &= \prod_{i=1}^{d}(X - \sigma_i(\alpha))^{n/d} \\ &= \left(\prod_{i=1}^{d}(X - \sigma_i(\alpha))\right)^{n/d} \\ &= \pi_{\alpha,K}(X)^{n/d} \\ &= \chi_{\alpha,L/K}(X). \end{aligned}$$

□

29.2.1 Trace Sum Formula

Theorem 29.4. *Suppose L/K is separable and M/L is a finite extension such that M/K is Galois. If $b \in L$, then we have*

$$\mathrm{Tr}_{L/K}(b) = \sum_{\sigma : L \hookrightarrow M} \sigma(b)$$

where the sum in M is taken over all K-embeddings $\sigma\colon L \hookrightarrow F$.

Proof. We first focus on $\mathrm{Tr}_{K(b)/K}(b)$ and then use this to get our hands on $\mathrm{Tr}_{L/K}(b)$ (since $K(b)$ may be a proper subfield of L). Recall that $\mathrm{Tr}_{K(b)/K}(b)$ is the negative of the second-highest coefficient of the minimal polynomial of b over K. By factoring this polynomial over the Galois exension M/K (where it splits completely!) we can identify this second-highest coefficient with the negative of the sum of the roots of the polynomial in M, which is to say the negative sum of the K-conjugates of b. In other words, $\mathrm{Tr}_{K(b)/K}(b) \in K$ is the sum of the K-conjugates of b in M, which is to say the sum of the images of b under the K-embeddings of $K(b)$ into M.

Consider the various K-embeddings of L into M. Such an embedding can be built up in two stages: first we figure out what to do on $K(b)$, and then the chosen K-embedding $j\colon K(b) \to M$ is lifted to an embedding $L \to M$. Those choices for j are easy to describe: we simply send b to one of its K-conjugates, and we can use whatever such K-conjugate we wish. Since there is an embedding of L into M over K, once we have fixed a choice of j, say with $j(b) = b'$, the number of liftings of to embeddings $L \to M$ is $[L : K(b)]$. Hence, in the proposed summation formula each $\sigma(b) = b'$ really appears $[L\colon K(b)]$ times, and so the proposed formula is just

$$[L : K(b)] \sum_{j\colon K(b) \hookrightarrow M} j(b) = [L : K(b)]\mathrm{Tr}_{K(b)/K}(b) = \mathrm{Tr}_{L/K}(b).$$

□

Theorem 29.5. *Suppose L/K is separable and M/L is a finite extension such that M/K is Galois. If $b \in L$, then we have*

$$\mathrm{N}_{L/K}(b) = \prod_{\sigma: L \hookrightarrow M} \sigma(b)$$

where the product in M is taken over all K-embeddings $\sigma\colon L \hookrightarrow F$.

Proof. Proved in an analagous way as in the trace case. □

29.2.2 Transitivity of Trace

Theorem 29.6. *Let $M/L/K$ be a tower of finite extensions. Then*

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}.$$

Proof. If M/K is not separable, then either M/L is not seperable or L/K is not seperable. In this case, both sides of the 'transitivity formula' are 0. Now suppose M/K is separable, so that both M/L and L/K are separable too. Choose N/M finite such that N/K is Galois. Let $G_K = \mathrm{Gal}(N/K)$, let $G_L = \mathrm{Gal}(N/L)$, and let $G_M = \mathrm{Gal}(N/M)$. By the trace sum formula, for $c \in M$ we have

$$\mathrm{Tr}_{M/K}(c) = \sum_{\substack{K\text{-embeddings} \\ \sigma\colon M \hookrightarrow N}} \sigma(c) = \sum_{g \in G_K/G_M} g(c)$$

where G_K/G_M is the left coset space of G_M in G_K and g is really running through a set of representatives for these cosets. Meanwhile,

$$\mathrm{Tr}_{M/L}(c) = \sum_{\substack{L\text{-embeddings} \\ \sigma\colon M \hookrightarrow N}} \sigma(c) = \sum_{g \in G_L/G_M} g(c).$$

Therefore, we have

$$\begin{aligned} \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(c)) &= \sum_{\gamma \in G_K/G_L} \gamma \left(\sum_{g \in G_L/G_M} g(c) \right) \\ &= \sum_{\gamma \in G_K/G_L} \sum_{g \in G_L/G_M} \gamma g(c) \\ &= \sum_{\gamma g \in G_K/G_M} \gamma g(c), \end{aligned}$$

where we use the fact that as g runs through a set of left coset representatives of G_L/G_M and γ runs through a set of left coset representatives of G_K/G_L, clearly γg runs through a set of left coset representatives for G_K/G_M. This yields the formula. □

30 Galois Extensions

Proposition 30.1. *Let L/K be a Galois extension of degree n with Galois group $G = \mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$. Then we have an isomorphism of K-algebras*

$$L \otimes_K L \simeq \prod_{\sigma \in G} L,$$

given by $b_1 \otimes b_2 \mapsto (b_1 \sigma(b_2))_\sigma$.

Proof. Suppose $L \simeq K[x]/f$ where f is a monic irreducible polynomial in $K[x]$ which factors in L as

$$f(x) = (x - \sigma_1 b)(x - \sigma_1 b) \cdots (x - \beta_n)$$

. Then $L\otimes$ □

31 Perfect Fields

Definition 31.1. A field K is called **perfect** if every irreducible polynomial in $K[X]$ is separable.

Every field of characteristic 0 is perfect. We will see that finite fields are perfect too. The simplest example of a nonperfect field is the rational function field $\mathbb{F}_p(u)$, since $X^p - u$ is irreducible in $\mathbb{F}_p(u)[X]$ but not separable.

Recall that for an irreducible $\pi(X)$, it is inseparable if and only if $\pi'(X) = 0$. Here is the standard way to check a field is perfect:

Theorem 31.1. *A field K is perfect if and only if it has characteristic 0, or it has characteristic p and $K^p = K$.*

Proof. When K has characteristic 0, any irreducible $\pi(X)$ in $K[X]$ is separable since $\pi'(X) \neq 0$. It remains to show when K has characteristic p that every irreducible in $K[X]$ is separable if and only if $K^p = K$. To do this, we will show the *negations* are equivalent: An inseparable irreducible exists in $K[X]$ if and only if $K^p \neq K$.

If $K^p \neq K$, choose $a \in K \backslash K^p$. Then $X^p - a$ has only one root in a splitting field: If $\alpha^p = a$, then $X^p - a = X^p - \alpha^p = (X - \alpha)^p$ since we are working in characteristic p. The polynomial $X^p - a$ is irreducible in $K[X]$ too: any nontrivial proper monic factor of $X^p - a$ is $(X - \alpha)^m$ where $1 \leq m \leq p - 1$. The coefficient of X^{m-1} in $(X - \alpha)^m$ is $-m\alpha$, so if $X^p - a$ has a nontrivial proper factor in $K[X]$, then $-m\alpha \in K$ for some m from 1 to $p - 1$. Then $m \in \mathbb{F}_p^\times \subset K^\times$, so $\alpha \in K$, which means $a = \alpha^p \in K^p$, a contradiction. Thus, $X^p - a$ is irreducible and inseparable in $K[X]$.

Now suppose there is an inseparable irreducible $\pi(X) \in K[X]$. Then $\pi'(X) = 0$, so $\pi(X)$ is a polynomial in X^p, say

$$\pi(X) = a_m X^{pm} + a_{m-1} X^{p(m-1)} + \cdots + a_1 X^p + a_0 \in K[X^p].$$

If $K^p = K$, then we can write $a_i = b_i^p$ for some $b_i \in K$, so

$$\pi(X) = (b_m X^m + b_{m-1} X^{(m-1)} + \cdots + b_1 X + b_0)^p.$$

Since $\pi(X)$ is irreducible, we have a contradiction, which shows $K^p \neq K$. □

Corollary 28. *Fields of characteristic 0 and finite fields are perfect.*

Proof. By Theorem (31.1), fields of characteristic 0 are perfect. It remains to show a finite field K of characteristic p satisfies $K^p = K$. The pth power map $K \to K$ is injective, and therefore surjective because K is finite, so we are done. □

Theorem 31.2. *A field K is perfect if and only if every finite extension of K is a separable extension.*

Proof. Suppose K is perfect: every irreducible in $K[X]$ is separable. If L/K is a finite extension, then the minimal polynomial in $K[X]$ of every element of L is irreducible, and therefore separble, so L/K is a separable extension.

Now suppose every finite field extension of K is a separable extension. To show K is perfect, let $\pi(X) \in K[X]$ be irreducible. Consider the field $L = K(\alpha)$, where $\pi(\alpha) = 0$. This field is a finite extension of K, so a separable extension by hypothesis, so α is separable over K. Since $\pi(X)$ is the minimal polynomial of α in $K[X]$, it is a separable polynomial. □

Proposition 31.1. *Let $\Bbbk$ be a perfect field of positive characteristic p and let $f \in \Bbbk[\![x, y]\!]$. Suppose that $\partial_x f = 0 = \partial_y f$. Then there exists a $\widetilde{f} \in \Bbbk[x, y]$ such that $\widetilde{f}^p = f$.*

Proof. Note that $\partial_x f = 0 = \partial_y f$ implies f has the form

$$f = \sum_{i,j \geq 0} c_{ij} x^{pi} y^{pj} = c_{00} + c_{10} x^p + c_{01} y^p + c_{20} x^{2p} + c_{11} x^p y^p + c_{02} y^{2p} + \cdots$$

where $c_{ij} \in \Bbbk$. Since $\Bbbk$ is perfect, we have $c_{ij} = \widetilde{c}_{ij}^p$ for some $\widetilde{c}_{ij} \in \Bbbk$ for all i, j. In particular we see that $f = \widetilde{f}^p$ where

$$\widetilde{f} = \sum_{i,j \geq 0} \widetilde{c}_{ij} x^i y^j = \widetilde{c}_{00} + \widetilde{c}_{10} x + \widetilde{c}_{01} y + \widetilde{c}_{20} x^2 + \widetilde{c}_{11} xy + \widetilde{c}_{02} y^2 + \cdots.$$

□

32 Artin-Schreier

Let K be a field with characteristic $p > 0$. For each $a \in K$ we set $f_a = t^p - t - a \in K[t]$. Clearly f_a is inseparable since $f_a' = -1$. Also note that if α is a root of f_a in a splitting field, then the other roots are $\alpha + 1, \alpha + 2, \dots, \alpha + p - 1$. It follows that either f_a is irreducible or splits completely. Thus reducibility of f_a is equivalent to $a = b^p - b$ for some $b \in K$, and in the irreducible case a Galois splitting field K_a/K is of degree p and we have $K_a \simeq K_{a'}$ over K if and only if $a - a' = b^p - b$ for some $b \in K$. Indeed, if α is a root of f_a and α' is a root of $f_{a'}$, then $\alpha + \alpha'$ is a root of $f_{a+a'}$. If $K_a \simeq K_{a'}$ over K, then there is an automorphism which fixes $\alpha + \alpha'$ and thus $f_{a+a'}$ must split completely. All cyclic p-extensions K'/K are K-isomorphic to K_a for some $a \in K$ not of the form $b^p - b$ with $b \in K$.

Definition 32.1. A field K is called a (non-Archimedean) **local field** if it is complete with respect to a topology induced by a discrete valuation v and if its residue field is finite. Equivalently, a local field is a locally compact topological field with respect to a non-discrete topology. The real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ are called (Archimedean) local fields.

33 Valuations

33.1 Definitions Corresponding to Valuations

Definition 33.1. Let K be a field and let $(\Gamma, \geq)$ be a totally ordered abelian group. We extend the ordering and group law on Γ to the set $\Gamma \cup \{\infty\}$ by the rules $\infty \geq \gamma$ and $\infty + \gamma = \infty = \gamma + \infty$ for all $\gamma \in \Gamma$. A **valuation** on K is a map $v\colon K \to \Gamma \cup \{\infty\}$ which satisfies the following properties for all $a, b \in K$:

1. $v(a) = \infty$ if and only if $a = 0$,
2. $v(ab) = v(a) + v(b)$,
3. $v(a + b) \geq \min(v(a), v(b))$ with equality if $v(a) \neq v(b)$.

The second property says that $v|_{K^\times}$ is a group homomorphism. One can interpret the valuation as the order of the leading-order term. Thus the third property corresponds to the order of a sum being the order of the larger term, unless the two terms have the same order, in which case they may cancel, in which case the sum may have smaller order. We also want to point out that the equality part in the third property can already be derived from the fact that $v|_{K^\times}$ is a group homomoprhism and the fact that $v(a + b) \geq \min(v(a), v(b))$. Indeed, first note that the second property implies $v(\pm 1) = 0$. In particular, $v(\pm x) = v(x)$ for all $x \in K$. Thus assuming that $v(a) > v(b)$, then $v(-a + b) \geq v(b)$. Setting $b = a + b$ gives us

$$v(b) \geq v(a + b) \geq v(b),$$

from which it follows that $v(a + b) = v(b)$.

Usually we define a valuation on K by first definining it on $K^\times$ and showing that the second and third properties hold for all $a, b \in K^\times$. Then we may extend it to all of K by setting $v(0) = \infty$. Thus we may write "let $v\colon K^\times \to \Gamma$ be a valuation" with the understanding that v is defined on all of K by setting $v(0) = \infty$. Also, when we write "let $v\colon K^\times \to \Gamma$ be a valuation on K", then it is understood that K is a field and Γ is a totally ordered abelian group. There are several objects associatied to a given valuation:

Definition 33.2. Let $v\colon K^\times \to \Gamma$ be a valuation on K.

1. The **value group** of v is the subgroup of Γ given by $\Gamma_v = v(K^\times)$. Usually v is surjective, so that $\Gamma_v = \Gamma$.

2. The **valuation domain** of v is the subring of K given by $R_v = \{a \in K \mid v(a) \geq 0\}$. To see that this is in fact a subring of K, note that $v(1) = 0$ since $v|_{K^\times}$ is a group homomorphism, so $1 \in R_v$. Also if $a, b \in R_v$, then properties 2 and 3 in Definition (33.1) shows $a + b \in R_v$ and $ab \in R_v$. Furthermore, R_v is in fact a domain since if $ab = 0$ for $a, b \in R$, then $\infty = v(a) + v(b)$ implies either $v(a) = \infty$ or $v(b) = \infty$, that is, either $a = 0$ or $b = 0$.

3. The **maximal ideal associated** to v is the maximal ideal in R_v given by $\mathfrak{m}_v = \{a \in K \mid v(a) > 0\}$. To see that this is in fact a maximal ideal, suppose $a \in R_v \backslash \mathfrak{m}_v$, so $v(a) = 0$. Then

$$\begin{aligned} 0 &= v(1) \\ &= v(aa^{-1}) \\ &= v(a) + v(a^{-1}) \\ &= v(a^{-1}). \end{aligned}$$

   Thus $a^{-1} \in R_v$, which shows that a is a unit. Note that we've also shown that $R_v^\times = \{a \in K \mid v(a) = 0\}$. Also note that $\mathfrak{m}_v$ is the unique maximal ideal in R_v. In particular, R_v is a local ring.

4. The **residue field associated** to v is the field $k_v = R_v/\mathfrak{m}_v$.

33.1.1 Equivalence of Valuations

Definition 33.3. Let $v_1\colon K^\times \to \Gamma_1$ and $v_2\colon K^\times \to \Gamma_2$ be two valuations on K. We say v_1 is **equivalent** to v_2, denoted $v_1 \sim v_2$, if there is an order preserving group isomorphism $\varphi\colon \Gamma_1 \to \Gamma_2$ such that

$$v_2(a) = \varphi(v_1(a))$$

for all $a \in K^\times$. It is straightforward to check that $\sim$ is in fact an equivalence relation. Given a valuation $v\colon K \to \Gamma$, we shall denote its equivalence class by $[v]$. It is also straightforward to check that two valuations on K are equivalent if and only if they have the same valuation ring. An equivalence class of valuations is called a **place of** K.

Remark 44. Ostrowski's theorem gives a complete classification of places of the field of rational numbers $\mathbb{Q}$: these are precisely the equivalence classes of valuations for the p-adic completions of $\mathbb{Q}$.

33.1.2 Examples and Nonexamples of Valuations

Example 33.1. Consider the field $\mathbb{C}(X)$ of rational polynomials over the complex numbers in the variable X. Suppose we define $v\colon \mathbb{C}(X)^\times \to \mathbb{Z}$ by

$$v(f/g) = \deg f - \deg g$$

for all $f/g \in \mathbb{C}(X)^\times$. It is easy to check that v is well-defined and that it is a group homomorphism. However v is not a valuation since otherwise we'd have

$$\begin{aligned} -2 &= v\left(\frac{2}{1-X^2}\right) \\ &= v\left(\frac{1}{1-X} + \frac{1}{1+X}\right) \\ &\geq \min\left\{v\left(\frac{1}{1-X}\right), v\left(\frac{1}{1+X}\right)\right\} \\ &= \min\{-1,-1\} \\ &= -1, \end{aligned}$$

which is a contradiction.

On the other hand, suppose we define $v_\pi\colon \mathbb{C}(X)^\times \to \mathbb{Z}$ as follows: if $f/g \in \mathbb{C}(X)^\times$. then we can express it as $f/g = \pi^n(\widetilde{f}/\widetilde{g})$ where $n \in \mathbb{Z}$, π is an irreducible polynomial in $\mathbb{C}[X]$, and $\widetilde{f}, \widetilde{g} \in \mathbb{C}[X]\backslash\{0\}$ such that π is not a factor of neither $\widetilde{f}$ nor $\widetilde{g}$, then we set $v_\pi(f/g) = n$. Again one can check that v_π is a well-defined group homomorphism. Additionally, it also satisfies the third criterion in Definition (33.1). Thus v_π is a valuation on $\mathbb{C}(X)^\times$. More generally, suppose R is a unique factorization domain with fraction field K. Given an irreducible element $\pi \in R$, we can define a valuation $v_\pi\colon K^\times \to \mathbb{Z}$ as follows: if $a/b \in K^\times$, then we can express it as

$a/b = \pi^n(\widetilde{a}/\widetilde{b})$ where $n \in \mathbb{Z}$ and $\widetilde{a}, \widetilde{b} \in R \backslash \{0\}$ such that π is not a factor of neither $\widetilde{a}$ nor $\widetilde{b}$, then we set $v_\pi(a/b) = n$. Note that if π' is another irreducible element in R such that $\pi' = u\pi$ for some unit $u \in R$, then $v_\pi = v_{\pi'}$. Indee, given $\gamma \in K^\times$, express it as $\gamma = \pi^n(a/b)$ where $a, b \in R$ and where π is not factor of neither a nor b, then we also have the expression $\gamma = (u\pi)^n(a/(u^n b))$ where $\pi' = u\pi$ is not a factor of neither a nor $u^n b$. Thus $v_\pi(\gamma) = n = v_{\pi'}(\gamma)$ and since $\gamma \in K^\times$ was arbitrary, we see that $v_\pi = v_{\pi'}$. We call v_π the **π-adic valuation**. An important special case of this is where $R = \mathbb{Z}$, $K = \mathbb{Q}$, and $\pi = p$ where p is a positive prime.

Example 33.2. Consider the field $K((X))$ of formal power series over a field K:

$$K((X)) = \left\{ \sum_{n > -\infty}^{\infty} a_n X^n \mid a_n \in K \right\}.$$

Define $v\colon K((X))^\times \to \mathbb{Z}$ as follows: given $f(X) \in K((X))^\times$, express it as

$$f(X) = \sum_{n=N}^{\infty} a_n X^n$$

where $N \in \mathbb{Z}$ and $a_N \neq 0$, and set $v(f) = N$. It is easy to check that v is in fact a valuation. Indeed, the only nontrivial thing to check is that

33.2 Valuation Rings

Let $v\colon K \to \Gamma$ be a valuation on K. It is easy to check that the valuation domain R_v satisfies the following property that for all $x \in K^\times$, either $x \in R_v$ or $x^{-1} \in R_v$. Integral domains which satisfy this property have a name:

Definition 33.4. Let A be an integral domain and let K denote its fraction field. We say A is a **valuation domain** if it satisfies the property that for all $x \in K$, either $x \in A$ or $x^{-1} \in A$.

Thus R_v is a valuation domain in the sense of Definition (33.4), so our terminology in Definition (33.2) is justified. In the next proposition, we show that there is a converse to this. Namely, any valuation domain is the valuation domain of a valuation! In the theorem that follows, we show that this valuation is unique up to equivalence.

Proposition 33.1. *Let A be a domain and let K be its fraction field. The following conditions are equivalent*

1. *For all nonzero $a, b \in A$, either $a \mid b$ or $b \mid a$;*
2. *A is a valuation domain;*
3. *There is a valuation π on K such that $A = \{x \in K \mid \pi(x) \geq 0\} \cup \{0\}$. This valuation is called the **standard valuation** of A.*

Proof. ($1 \implies 2$): Let $x \in K^\times$. Write $x = a/b$ where $a, b \in A \backslash \{0\}$. Then either $a \mid b$ or $b \mid a$. If $b \mid a$, then we can write $a = bc$ for some nonzero $c \in A$. In this case, we have

$$\begin{aligned} x &= a/b \\ &= bc/b \\ &= c, \end{aligned}$$

and hence $x \in A$. On the other hand, if $a \mid b$, then we can write $b = ad$ for some nonzero $d \in A$. In this case, we have

$$\begin{aligned} x^{-1} &= b/a \\ &= ad/a \\ &= d, \end{aligned}$$

and hence $x^{-1} \in A$.

($2 \implies 3$): Note that $K^\times/A^\times$ is an abelian group. We can turn it into a totally ordered abelian group by defining a total ordering on $K^\times/A^\times$ as follows: Let $\overline{x}, \overline{y} \in K^\times/A^\times$. Then we say

$$\overline{x} \geq \overline{y} \text{ if and only if } xy^{-1} \in A. \tag{81}$$

Let us check that (81) is well-defined. Suppose xa and yb are two different representatives of the cosets $\overline{x}$ and $\overline{y}$ respectively, where $a, b \in A^\times$. Then

$$\begin{aligned}(xa)(yb)^{-1} &= (xa)(y^{-1}b^{-1}) \\ &= (xy^{-1})(ab^{-1}) \\ &\in A\end{aligned}$$

implies $\overline{xa} \geq \overline{yb}$. Thus (81) is well-defined. Next, observe that the relation given in (81) is antisymmetric: if $\overline{x} \geq \overline{y}$ and $\overline{y} \geq \overline{x}$, then $xy^{-1} \in A$ and $yx^{-1} \in A$, which implies $xy^{-1} \in A^\times$, and hence

$$\begin{aligned}\overline{x} &= \overline{x(yy^{-1})} \\ &= \overline{(xy^{-1})y} \\ &= \overline{y}.\end{aligned}$$

It is also transitive: if $\overline{x} \geq \overline{y}$ and $\overline{y} \geq \overline{z}$ implies

$$\begin{aligned}xz^{-1} &= x(y^{-1}y)z^{-1} \\ &= (xy^{-1})(yz^{-1}) \\ &\in A\end{aligned}$$

which implies $\overline{x} \geq \overline{z}$). It is also a total relation since either $\overline{x} \geq \overline{y}$ or $\overline{y} \geq \overline{x}$ (since either $xy^{-1} \in A$ or $yx^{-1} \in A$). Thus (81) gives us a total ordering on $K^\times / A^\times$.

Now we define $\pi \colon K^\times \to \Gamma$ to be the natural quotient map. Clearly π is a surjective homomorphism. We also have

$$\pi(x+y) \geq \min\{\pi(x), \pi(y)\} \text{ with equality if } \pi(x) \neq \pi(y).$$

Indeed, assume without loss of generality that $\pi(y) \geq \pi(x)$. Then $(x+y)x^{-1} = 1 + yx^{-1} \in A$ implies $\pi(x+y) \geq \pi(x)$. Now assume $\pi(x) \neq \pi(y)$, so $yx^{-1} \notin A$. Then $x^{-1}(x+y) = 1 + yx^{-1} \notin A$. This implies $x(x+y)^{-1} \in A$ (by 2). Thus $\pi(x) \geq \pi(x+y)$, which implies $\pi(x) = \pi(x+y)$ by antisymmetry of $\geq$. Finally, we observe that

$$A^\times = \{x \in K \mid \pi(x) = 0\}$$

by construction. Moreover, we have

$$A = \{x \in K \mid \pi(x) \geq 0\} \cup \{0\},$$

since $\pi(x) \geq 0$ if and only if $\pi(x) \geq \pi(1)$ if and only if $x \in A$.

($3 \implies 1$): Let $(\Gamma, \geq)$ be a totally ordered abelian group and let $v \colon K^\times \to \Gamma$ be such a valuation. Suppose $a, b \in A \backslash \{0\}$, and without loss of generality, assume that $v(b) \geq v(a)$. Then

$$\begin{aligned}v(ba^{-1}) &= v(b) - v(a) \\ &\geq 0\end{aligned}$$

implies $ba^{-1} \in A$. In particular, this implies $a \mid b$. □

Theorem 33.1. *Let K be a field and let $v \colon K^\times \to \Gamma$ be a valuation on K. Assume that v is surjective so that $\Gamma = \Gamma_v$. Let R_v be the valuation ring of v and let $\pi \colon K^\times \to K^\times / R_v^\times$ be the standard valuation of R_v. Then π is equivalent to v. Conversely, suppose R is a valuation domain with fraction field K and let $\pi \colon K^\times \to K^\times / R^\times$ be the standard valuation of R. Then $A = A_\pi = \{x \in K \mid \pi(x) \geq 0\} \cup \{0\}$.*

Proof. We define $\varphi \colon K^\times / R_v^\times \to \Gamma$ by $\varphi(\overline{x}) = v(x)$ for all $\overline{x} \in K^\times$. Note that the map φ is well-defined since $R_v^\times = \{a \in K \mid v(a) = 0\}$. It is straightforward to check that φ is an order preserving group isomoprhism which satisfies $\varphi\pi = v$. Thus π is equivalent to v. The converse statement was proved in Proposition (33.1). □

33.2.1 Every Valuation Ring is Integrally Closed

Proposition 33.2. *Every Valuation Ring is Integrally Closed.*

Proof. Let A be a valuation ring with fraction field K and let $\alpha \in K$ be integral over A. Then

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

for some $a_0, \dots, a_{n-1} \in A$. Suppose $\alpha \notin A$. Then $\alpha^{-1} \in A$, since A is a valuation ring. Multiplying the equation above by $\alpha^{-(n-1)} \in A$ and moving all but the first term on the LHS to the RHS yields

$$\alpha = -a_{n-1} - \cdots - a_0\alpha^{-n-1} \in A,$$

contradicting our assumption that $\alpha \notin A$. It follows that A is integrally closed. □

33.3 Discrete Valuation Rings

Definition 33.5. A ring A is called a **discrete valuation ring** if it is a principal ideal domain that has a unique non-zero prime ideal $\mathfrak{m}$. The field $A/\mathfrak{m}$ is called the **residue field** of A.

In a principal ideal domain, the non-zero prime ideals are the ideals of the form πA where π is an irreducible element. The definition above comes down to saying that A has one and only one irreducible element, up to multiplication by an invertible element; such an element is called a **uniformizing element** of A (or **uniformizer**). The non-zero ideals of A are of the form $\pi^n A$. If $a \neq 0$ is any element of A, then one can write $a = u\pi^n$ where $n \in \mathbb{N}$ and u is a unit. The integer n is called the **valuation** of a and is denoted $\nu(a)$; it does not depend on the choice of π. Let K be the field of fractions of A. If γ is any element of $K^\times$, one can again write γ in the form $u\pi^n$ where $n \in \mathbb{Z}$ this time, and set $\nu(\gamma) = n$. It is easy to check that ν gives rise to a valuation on $K^\times$.

Definition 33.6. A **valuation** on a field K is a group homomorphism $K^\times \to \mathbb{R}$ such that for all $x, y \in K$ we have

$$v(x+y) \geq \min(v(x), v(y)).$$

We may extend v to a map $K \to \mathbb{R} \cup \{\infty\}$ by defining $v(0) := \infty$. For any $0 < c < 1$, defining

$$|x|_v := c^{v(x)}$$

yields a nonarchimedean absolute value. The image of v in $\mathbb{R}$ is the **value group** of v. We say that v is a **discrete valuation** if its value group is equal to $\mathbb{Z}$. The set

$$A := \{x \in K \mid v(x) \geq 0\}$$

is called the **valutation ring** of K (with respect to v). A **discrete valuation ring** (DVR) is an integral domain that is the valuation ring of its fraction field with respect to a discrete valuation.

It is easy to verify that every valuation ring A is in fact a ring, and even an integral domain (if x and y are nonzero, then $v(xy) = v(x) + v(y) \neq \infty$, so $xy \neq 0$), with K as its fraction field. Notice that for any $x \in K^\times$ we have $v(1/x) = v(1) - v(x) - -v(x)$, so at least one of x and $1/x$ has nonnegative valuation and lies in A. It follows that $x \in A$ is invertible (in A) if and only if $v(x) = 0$, hence the unit group of A is

$$A^\times = \{x \in K \mid v(x) = 0\}.$$

We can partition the nonzero elements of K according to the sign of their valuation. Elements with valuation zero are units in A, elements with positive valuation are nonunits in A, and elements with negative valuation do not lie in A, but their multiplicative inverses are nonunits in A. This leads to a more general notion of a valuation ring:

Definition 33.7. A **valuation ring** is an integral domain A with fraction field K with the property that for every $x \in K$, either $x \in A$ or $x^{-1} \in A$.

Let us now suppose that the integral domain A is the valuation ring of its fraction field with respect to some discrete valuation v (which we shall see is uniquely determined). Any element $\pi \in A$ for which $v(\pi) = 1$ is called a **uniformizer**. Uniformizers exist, since $v(A) = \mathbb{Z}_{\geq 0}$. If we fix a uniformizer π, then every $x \in K^\times$ can be written uniquely as

$$x = u\pi^n$$

where $n = v(x)$ and $u = x/\pi^n \in A^\times$ and uniquely determined. It follows that A is a unique factorization domain (UFD), and in fact A is a principal ideal domain (PID). Indeed, every nonzero ideal of A is equal to

$$(\pi^n) = \{a \in A \mid v(a) \geq n\},$$

for some integer $n \geq 0$. Moreover,

Example 33.3. Let V be a normal algebraic variety (i.e. the local ring at every point is an integrally closed domain) of dimension n and let W be an irreducible subvariety of V of dimension $n-1$. Let $A_{V/W}$ be the local ring of V along W (i.e. the set of rational functions f on V which are defined on at least one point of W). By the normality hypothesis, we see that $A_{V/W}$ is integrally closed; the dimension hypothesis shows that it is a one-dimensional local ring; therefore it is a discrete valuation ring; its residue field is the field of rational functions on W. If v_W denotes the associated valuation, and if f is a rational function on V, then integer $v_W(f)$ is called the **order** of f along W; it is the multiplicity of W in the divisor of zeros and poles of f.

Example 33.4. Let S be a Riemann surface (i.e. a one-dimensional complex manifold), and let $P \in S$. The ring $\mathfrak{H}_P$ of functions holomorphic in a neighborhood of P is a discrete valutation ring, isomorphic to the subring of convergent power series in $\mathbb{C}[\![T]\!]$; its residue field is $\mathbb{C}$.

33.3.1 Characterizations of Discrete Valuation Rings

Proposition 33.3. *Let A be a commutative ring. Then A is a discrete valuation ring if and only if A is a Noetherian local ring and its maximal ideal is generated by a non-nilpotent element.*

Proof. It is clear that a discrete valuation ring has the stated properties. Conversely, suppose that A has these properties. Let π be a generator of the maximal ideal $\mathfrak{m}$ of A. Let $\mathfrak{a}$ be the ideal of the ring formed by the elements x such that $x\pi^n = 0$ for n sufficiently large. Since A is Noetherian, we see that $\mathfrak{a}$ is finitely generated. Thus there exists a fixed N such that $x\pi^N = 0$ for all $x \in \mathfrak{a}$.

We will now show that the intersection of the powers $\mathfrak{m}^n$ are zero (this is in fact true in any Noetherian local ring). Let $x \in \bigcap_{n=1}^{\infty} \mathfrak{m}^n$. For each $n \in \mathbb{N}$, write $x = a_n\pi^n$ where $a_n \in A$. We will show that $a_n \in \mathfrak{a}$ for n sufficiently large, which will imply $x = 0$. Observe that

$$\begin{aligned} 0 &= x - x \\ &= a_n\pi^n - a_{n+1}\pi^{n+1} \\ &= (a_n - a_{n+1}\pi)\pi^n. \end{aligned}$$

In particular we have $a_n - \pi a_{n+1} \in \mathfrak{a}$. This implies the sequence $(\mathfrak{a} + Aa_n)$ of ideals is increasing. Since A is Noetherian, the sequence $(\mathfrak{a} + Aa_n)$ must stabilize, say at $n \in \mathbb{N}$. Thus $\mathfrak{a} + Aa_n = \mathfrak{a} + Aa_{n+1}$, which implies $a_{n+1} \in \mathfrak{a} + Aa_n$. Write

$$a_n - \pi a_{n+1} = y \quad \text{and} \quad a_{n+1} = z + aa_n$$

where $y, z \in \mathfrak{a}$ and $a \in A$. Then note that

$$\begin{aligned} (1 - \pi a)a_{n+1} &= a_{n+1} - a\pi a_{n+1} \\ &= z + aa_n - a(a_n - y) \\ &= z + ay \\ &\in \mathfrak{a}. \end{aligned}$$

Now $1 - \pi a$ is a unit since A is local, thus it follows that $a_{n+1} \in \mathfrak{a}$ for n sufficiently large, and taking $n + 1 \geq N$, we see that $x = \pi^{n+1}a_{n+1}$ is zero, which proves

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0.$$

By hypothesis none of the $\mathfrak{m}^n$ is zero. If a is a nonzero element of A, then a can therefore be written in the form $\pi^n u$, with u invertible. This writing is clearly unique; it shows that A is an integral domain. Furthermore, if one sets $n = \nu(a)$, one checks easily that the function ν extends to a discrete valuation of the field of fractions of A with A as its valuation ring. □

Proposition 33.4. *Let A be a Noetherian integral domain. Then A is a discrete valuation ring if and only it is integrally closed and has a unique nonzero prime ideal.*

Proof. Suppose A is a discrete valuation ring. By definition, A has a unique nonzero prime ideal. Furthermore, A is a valuation ring. All valuation rings are integrally closed by Proposition (33.2).

Now we show the converse. Suppose A is integrally closed and has a unique nonzero prime ideal, say $\mathfrak{m}$. In particular, A is a local ring. Let

$$\widetilde{\mathfrak{m}} = A :_K \mathfrak{m} = \{x \in K \mid x\mathfrak{m} \subseteq A\}.$$

Then $\widetilde{\mathfrak{m}}$ is an A-submodule of K which contains A. If $y \in \mathfrak{m}\backslash\{0\}$, then it is clear that $\widetilde{\mathfrak{m}} \subset y^{-1}A$, and as A is Noetherian, this shows that $\widetilde{\mathfrak{m}}$ is a finitely generated A-module (we call $\widetilde{\mathfrak{m}}$ a **fractional ideal** of K with respect to A). Now observe that $\mathfrak{m}\widetilde{\mathfrak{m}}$ is contained in A, and so must be an ideal in A. Since $\mathfrak{m} \subseteq A$ we also have $\mathfrak{m} \subseteq \mathfrak{m}\widetilde{\mathfrak{m}}$. Thus

$$\mathfrak{m} \subseteq \widetilde{\mathfrak{m}}\mathfrak{m} \subseteq A.$$

Since $\mathfrak{m}$ is maximal, this means either $\mathfrak{m} = \widetilde{\mathfrak{m}}\mathfrak{m}$ or $\widetilde{\mathfrak{m}}\mathfrak{m} = A$.

Assume for a contradiction that $\mathfrak{m} = \widetilde{\mathfrak{m}}\mathfrak{m}$. First we will show that A being integrally closed implies $\widetilde{\mathfrak{m}} = A$. Let $x \in \widetilde{\mathfrak{m}}$. Then $x^n\mathfrak{m} \subset \mathfrak{m}$ for all $n \in \mathbb{N}$. Let $\mathfrak{a}_n$ be the A-submodule of K generated by $\{1, x, \dots, x^n\}$. Then observe that $(\mathfrak{a}_n)$ is an ascending sequence of A-submodules of $\widetilde{\mathfrak{m}}$. Since A is Noetherian, we must have $\mathfrak{a}_n = \mathfrak{a}_{n-1}$ for n large, so $x^n \in \mathfrak{a}_{n-1}$. One can write

$$x^n = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

where each $a_i \in A$. This shows that x is integral over A. Thus $x \in A$ since A is integrally closed.

Thus, assuming $\mathfrak{m} = \widetilde{\mathfrak{m}}\mathfrak{m}$, we see that A being integrally closed forces $\widetilde{\mathfrak{m}} = A$. Now we will show that A having a unique nonzero prime ideal will imply $\widetilde{\mathfrak{m}} \neq A$, which will give us our desired contradiction. Let x be a nonzero element of $\mathfrak{m}$, and consider the ring A_x of fractions of the type a/x^n with $a \in A$ and $n \geq 0$. Then since A has a unique nonzero prime ideal, we must have $A_x = K$. Indeed, if $A_x \neq K$, then there would exist a nonzero prime ideal $\mathfrak{p}_x$ in A_x. Then $\mathfrak{p}_x = A \cap \mathfrak{p}_x$ would be a prime ideal in A which would not contain x, but $\mathfrak{m}$ contains x and $\mathfrak{m} = \mathfrak{p}_x$ as $\mathfrak{m}$ is unique.

Thus every element of K can be written in the form a/x^n; let us apply this to $1/b$ with $b \neq 0$ in A. We get $1/b = a/x^n$, and thus $x^n = ab \in \langle b \rangle$. Therefore every element of $\mathfrak{m}$ has a power belonging to the ideal $\langle b \rangle$. In fact, since $\mathfrak{m}$ is finitely generated, we can find an $N \in \mathbb{N}$ such every element of $\mathfrak{m}$ raised to the N belongs to $\langle b \rangle$. We choose $N \in \mathbb{N}$ to be the smallest integer such that $\mathfrak{m}^N \subseteq \langle b \rangle$. Then choosing $y \in \mathfrak{m}^{N-1}$ such that $y \notin \langle b \rangle$, we see that $\mathfrak{m}y \subseteq \langle b \rangle$, and thus $y/b \in \widetilde{\mathfrak{m}}$ and $y/z \notin A$. Thus $\widetilde{\mathfrak{m}} \neq A$, and we have our contradiction.

Finally, we see that $\mathfrak{m}\widetilde{\mathfrak{m}} = A$. We will now show that $\mathfrak{m}$ is a principal ideal. Since $\mathfrak{m}\widetilde{\mathfrak{m}} = A$, we have

$$\sum_{i=1}^{n} x_i y_i = 1$$

where $x_i \in \mathfrak{m}$ and $y_i \in \widetilde{\mathfrak{m}}$. The products $x_i y_i$ all belong to A; at least one of them, say xy, does not belong to $\mathfrak{m}$, there is an invertible element u. Replacing x by xu^{-1}, one obtains a relation $xy = 1$, with $x \in \mathfrak{m}$ and $y \in \widetilde{\mathfrak{m}}$. If $z \in \mathfrak{m}$, one has $x(yz)$ with $yz \in A$ since $y \in \widetilde{\mathfrak{m}}$. Therefore z is a multiple of x, which shows that $\mathfrak{m}$ is indeed a principal ideal, generated by x. □

Proposition 33.5. *Let A be a Noetherian integral domain. The following two properties are equivalent:*

1. *$A_\mathfrak{p}$ is a discrete valuation ring for every nonzero prime ideal $\mathfrak{p}$ in A.*

2. *A is integrally closed and of dimension ≤ 1.*

Proof. First let us show 1 implies 2. Suppose $A_\mathfrak{p}$ is a discrete valuation ring for every nonzero prime ideal $\mathfrak{p}$ in A and suppose $\mathfrak{p}, \mathfrak{p}'$ are prime ideals in A such that $\mathfrak{p} \subset \mathfrak{p}'$. Then $A_{\mathfrak{p}'}$ contains the prime ideal $\mathfrak{p}A_{\mathfrak{p}'}$. In particular we must have either $\mathfrak{p}A_{\mathfrak{p}'} = 0$ or $\mathfrak{p}A_{\mathfrak{p}'} = \mathfrak{p}'A_{\mathfrak{p}'}$ as $\mathfrak{p}'A_{\mathfrak{p}'}$ is unique. This implies either $0 = \mathfrak{p}$ or $\mathfrak{p} = \mathfrak{p}'$. Indeed if, say $\mathfrak{p}A_{\mathfrak{p}'} = \mathfrak{p}'A_{\mathfrak{p}'}$, then for any $x \in \mathfrak{p}'$, we would have $x/1 = z/y$ where $z \in \mathfrak{p}$ and $y \notin \mathfrak{p}'$. Thus $xy = z$ which would imply $x \in \mathfrak{p}$ as $\mathfrak{p}$ is prime. Thus $\dim A \leq 1$.

On the other hand, suppose $\gamma \in K$ is integral over A. Then γ is integral over $A_\mathfrak{p}$ for each prime ideal $\mathfrak{p}$ of A. Thus $\gamma \in A_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of A. This implies $\gamma \in A$. Indeed, write $\gamma = a/b$ where $a, b \in A$ with $b \neq 0$. Then the ideal

$$b : a = \{d \in A \mid da = bc \text{ for some } c \in A\}$$

is not contained in any prime ideal $\mathfrak{p}$ of A. Indeed, since $a/b \in A_\mathfrak{p}$, we can write $a/b = c/d$ with $d \notin \mathfrak{p}$, and clearly $d \in b : a$. Therefore $b : a = A$ which implies $a = bc$ for some $c \in A$ which implies $\gamma = c \in A$.

Now we will show 2 implies 1. Suppose A is integrally closed and of dimension ≤ 1 and let $\mathfrak{p}$ be a nonzero prime ideal of A. It is clear that $A_\mathfrak{p}$ has a unique nonzero prime ideal, namely $\mathfrak{p}A_\mathfrak{p}$, so it suffices to show that $A_\mathfrak{p}$ is integrally closed. A is integrally closed and of dimension ≤ 1. This follows from Proposition (15.10).

□

Definition 33.8. A Noetherian integral domain which has the two equivalent properties of Proposition (33.5) is called a **Dedekind domain**.

Proposition 33.6. *Let A be a Dedekind domain. Then every nonzero fractional ideal of A is invertible.*

Proof. Let $\mathfrak{a}$ be a fractional ideal in A. Define

$$\widetilde{\mathfrak{a}} = A :_K \mathfrak{a} = \{\gamma \in K \mid \gamma\mathfrak{a} \subseteq A\}.$$

Then observe that for each prime ideal $\mathfrak{p}$ of A we have

$$\begin{aligned}(\widetilde{\mathfrak{a}}\mathfrak{a})_\mathfrak{p} &= \widetilde{\mathfrak{a}}_\mathfrak{p}\mathfrak{a}_\mathfrak{p} \\ &= (A_\mathfrak{p} :_K \mathfrak{a}_\mathfrak{p})\mathfrak{a}_\mathfrak{p} \\ &= A_\mathfrak{p},\end{aligned}$$

where we used the fact that $\mathfrak{a}_\mathfrak{p}$ is invertible in $A_\mathfrak{p}$. It follows that $\widetilde{\mathfrak{a}}\mathfrak{a} = A$, hence $\mathfrak{a}$ is invertible. □

33.4 Domination

Definition 33.9. Let K be a field. We define a preordered set $(\mathcal{D}_K, \geq_{\mathrm{d}})$ as follows: the underlying set is defined to be

$$\mathcal{D}_K := \{A \mid A \text{ is a local domain such that } A \subseteq K\}.$$

The preorder $\leq_{\mathrm{d}}$ is defined as follows: let $A, B \in \mathcal{D}_K$. We write $B \geq_{\mathrm{d}} A$ if $B \supseteq A$ and $\mathfrak{m}_A = A \cap \mathfrak{m}_B$. In this case, we also say B **dominates** A.

More generally, if R is a subring of K (so necessarily a domain), then we define a preordered set $(\mathcal{D}_{K/R}, \geq_{\mathrm{d}})$ as follows: the underlying set is defined to be

$$\mathcal{D}_{K/R} := \{A \mid A \text{ is a local domain such that } R \subseteq A \subseteq K\}.$$

The preorder $\leq_{\mathrm{d}}$ is defined as above. If $A \in \mathcal{D}_{K/R}$, then we say A is **centered** on R.

Proposition 33.7. *Let K be a field and let $A \in \mathcal{D}_K$. A maximal element in $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$ exists. Furthemore, any such maximal element is a valuation ring with K as its fraction field.*

Proof. We appeal to Zorn's Lemma. First note that $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$ is nonempty since $A \in (\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$. Let $(A_\lambda)_{\lambda \in \Lambda}$ be a totally ordered collection of local subrings of K (so $A_\mu \geq_{\mathrm{d}} A_\lambda$ for each $\mu \geq \lambda$, which means $A_\mu \supseteq A_\lambda$ and $\mathfrak{m}_\lambda = A_\lambda \cap \mathfrak{m}_\mu$ for each $\mu \geq \lambda$). Then $\bigcup_{\lambda \in \Lambda} A_\lambda$ is a local subring of K which dominates all of the A_λ. Indeed, it is straightforward to check that $\bigcup_{\lambda \in \Lambda} A_\lambda$ is a subring of K and $\bigcup_{\lambda \in \Lambda} \mathfrak{m}_\lambda$ is an ideal in $\bigcup_{\lambda \in \Lambda} A_\lambda$. To see that $\bigcup_{\lambda \in \Lambda} \mathfrak{m}_\lambda$ is the unique maximal ideal in $\bigcup_{\lambda \in \Lambda} A_\lambda$, we will show that its complement consists of units. Let $x \in \bigcup_{\lambda \in \Lambda} A_\lambda$ and suppose $x \notin \bigcup_{\lambda \in \Lambda} \mathfrak{m}_\lambda$. Since $x \in \bigcup_{\lambda \in \Lambda} A_\lambda$, there exists some λ such that $x \in A_\lambda$. Since $x \notin \bigcup_{\lambda \in \Lambda} \mathfrak{m}_\lambda$, we see that $x \notin \mathfrak{m}_\lambda$. Thus x is a unit in A_λ since $(A_\lambda, \mathfrak{m}_\lambda)$ is a local ring. It follows that x is a unit in $\bigcup_{\lambda \in \Lambda} A_\lambda$ since $A_\lambda \subseteq \bigcup_{\lambda \in \Lambda} A_\lambda$. Thus $\bigcup_{\lambda \in \Lambda} \mathfrak{m}_\lambda$ is the unique maximal ideal in $\bigcup_{\lambda \in \Lambda} A_\lambda$. Thus every totally ordered subset of $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$ has an upper bound. It follows from Zorn's Lemma that $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$ has a maximal element.

Now we prove the latter part of the proposition. Let $(B, \mathfrak{m})$ be a maximal element in $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$. First we show B has K as its fraction field. Assume for a contradiction that K is not the fraction field of B. Choose $x \in K$ which is not in the fraction field of B. If x is transcendental over B, then $B[x]_{(x,\mathfrak{m})} \in (\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$, which contradicts maximality of B. If x is algebraic over B, then for some $b \in B$, the element bx is integral over B. In this case, the subring $B' \subseteq K$ generated by B and bx is finite over B. In particular, there exists a prime ideal $\mathfrak{m}' \subseteq B'$ lying over $\mathfrak{m}$. Then $B'_{\mathfrak{m}'}$ dominates B. In particular, this implies $B = B'_{\mathfrak{m}'}$ by maximality of B, and then x is in the fraction field of B which is a contradiction.

Finally, we show that B is a valuation ring. Let $x \in K$ and assume that $x \notin B$. Let B' denote the subring of K generated by B and x. Since B is maximal in $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$, there is no prime of B' lying over $\mathfrak{m}$. Since $\mathfrak{m}$ is maximal we see that $\mathrm{V}(\mathfrak{m}B') = \emptyset$. Then $\mathfrak{m}B' = B'$, hence we can write

$$1 = \sum_{i=0}^{d} t_i x^i$$

with $t_i \in \mathfrak{m}$. This implies

$$(1 - t_0)(x^{-1})^d - \sum t_i (x^{-1})^{d-i} = 0.$$

In particular we see that x^{-1} is integral over B. Thus the subring B'' of K generated by B and x^{-1} is finite over B and we see that there exists a prime ideal $\mathfrak{m}'' \subseteq B''$ lying over $\mathfrak{m}$. By maximality of B, we conclude that $B = (B'')_{\mathfrak{m}''}$, and hence $x^{-1} \in B$. □

33.5 Absolute Values

Definition 33.10. An **absolute value** on a field K is a map $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in K$ the following hold:

1. $|x| = 0$ if and only if $x = 0$;
2. $|xy| = |x||y|$;
3. $|x + y| \leq |x| + |y|$.

If the stronger condition $|x + y| \leq \max(|x|, |y|)$ also holds, then the absolute value is **nonarchimedean**; otherwise it is **archimedean**.

The second property tells us that $|\cdot|_{|K^\times}$ is a group homomorphism. In particular, if $\zeta \in K^\times$ is a root of unity, then we have $|\zeta| = 1$. It is clear that $\mathrm{d}(x, y) = |x - y|$ gives K the structure of a metric space, and the resulting topology is the discrete topology if and only if $|x| = 1$ for all $x \neq 0$. We shall call $|\cdot|$ a **trivial** absolute value if $|x| = 1$ for all $x \neq 0$. The usual absolute value on the set of real numbers is denoted $|\cdot|_{\mathbb{R}}$. We denote

$$\mathrm{B}_{\varepsilon}^{|\cdot|}(x) = \{y \in K \mid |x - y| < \varepsilon\}$$

to be the open ball of radius ε centered at x with respect to the metric induced by $|\cdot|$. If the absolute value is clear from context, then we supress $|\cdot|$ and the superscript and just write $\mathrm{B}_{\varepsilon}(x)$. Similarly, we denote

$$\mathrm{B}_{\varepsilon}^{|\cdot|}[x] = \{y \in K \mid |x - y| \leq \varepsilon\}$$

to be the closed ball of radius ε centered at x with respect to the metric induced by $|\cdot|$. It is straightforward to check that $\mathrm{B}_{\varepsilon}^{|\cdot|}[x]$ is the closure of $\mathrm{B}_{\varepsilon}^{|\cdot|}(x)$.

33.5.1 Topological Equivalence

Proposition 33.8. *Let $|\cdot|$ be an absolute value on K and let $e \in (0,1]$. Then $|\cdot|^e$ is another absolute value on K. Furthermore, $|\cdot|$ and $|\cdot|^e$ induce the same topology.*

Proof. Clearly we have $|x|^e = 0$ if and only if $x = 0$. Also for $x, y \in K$, we have

$$\begin{aligned} |xy|^e &= (|x||y|)^e \\ &= |x|^e|y|^e, \end{aligned}$$

and similarly

$$\begin{aligned} |x+y|^e &\leq (|x| + |y|)^e \\ &\leq |x|^e + |y|^e, \end{aligned}$$

where we needed to use the fact that $-^e$ is monotone increasing to the get the first inequality and where we needed to use the fact that $0 < e \leq 1$ to get the second inequality. To see that they induce the same topology, observe that

$$\begin{aligned} \mathrm{B}_{\varepsilon}^{|\cdot|}(x) &= \{y \in K \mid |x - y| < \varepsilon\} \\ &= \{y \in K \mid |x - y|^e < \varepsilon^e\} \\ &= \mathrm{B}_{\varepsilon^e}^{|\cdot|^e}(x). \end{aligned}$$

□

Remark 45. It is straightforward to check that $|\cdot|_{\mathbb{R}}^e$ does not satisfy the triangle inequality whenever $e > 1$. On the other hand, we shall see many examples of non-trivial absolute values $|\cdot|$ on $\mathbb{Q}$ such that $|\cdot|^e$ is an absolute value for all $e > 0$.

Theorem 33.2. *Let $|\cdot|$ and $|\cdot|'$ be two absolute values on K that induce the same topology on K. Then there exists $e > 0$ such that $|\cdot|' = |\cdot|^e$.*

Proof. Since the trivial absolute value is the unique one giving rise to the discrete topology, we may assume that the topology is non-discrete and hence that both absolute values are non-trivial. Pick $c \in K^{\times}$ such that $0 < |c| < 1$. Hence (c^n) converges to 0 with respect to the common topology, so $|c^n|' \to 0$ and thus $0 < |c|' < 1$. There is a unique $e > 0$ such that $|c|' = |c|^e$. By switching the roles of $|\cdot|$ and $|\cdot|'$ and replacing e with $1/e$ if necessary, we may assume that $0 < e \leq 1$. Hence, $|\cdot|^e$ is an absolute value and our goal is to prove that it is equal to $|\cdot|'$. Since $|\cdot|^e$ defines the same topology as $|\cdot|$, we may replace $|\cdot|$ with $|\cdot|^e$ to reduce to the case $e = 1$. That is, we have $0 < |c| = |c|' < 1$ for some $c \in K^{\times}$. Under this condition, we want to prove $|x| = |x|'$ for all $x \in K$, and we may certainly restrict attention to $x \in K^{\times}$.

Assume for a contradiction that $|x|' \neq |x|$ for some $x \in K^{\times}$. By replacing x with $1/x$ if neccessary, we may assume that $|x| < |x|' \leq 1$. We can find an $m, n \in \mathbb{N}$ such that

$$0 < |x^m| < |c^n| = |c^n|' < |x^m|' \leq 1.$$

By replacing x with x^m and c with c^n if necessary, we may assume that

$$1 < |x| < |c| = |c|' < |x|' \leq 1.$$

Thus $|x/c| < 1 < |x/c|'$. Hence $((x/c)^n)$ converges to zero with respect to the metric topology of $|\cdot|$ but not with respect to the metric topology of $|\cdot|'$. This is a contradiction since the two topologies are assumed to coincide. □

33.5.2 Non-Archimedean Absolute Values

An absolute value $|\cdot|$ on a field is **non-archimedean** if its restriction to the image of $\mathbb{Z}$ in K is bounded, and otherwise (that is, if $\mathbb{Z}$ is unbounded for the metric structure) we say $|\cdot|$ is **archimedean**. The non-archimedean property is inherited by any absolute value of the form $|\cdot|^e$ with $e > 0$, and so Theorem (33.2) implies that this condition is intrinsic to the underlying topology associated to the absolute value. Obviously the trivial absolute value is non-archimedean, and any absolute value on a field K with positive characteristic must be non-archimedean (as the image of $\mathbb{Z}$ in K consists of 0 and the set $K_p^\times$ of $(p-1)$th roots of unity in K). Of course, the usual absolute value on $\mathbb{Q}$ is archimedean.

The **non-archimedean triangle inequality** (also called the **ultrametric triangle inequality**) is

$$|x+y| \leq \max(|x|, |y|).$$

This is clearly much stronger than the usual triangle inequality, and it forces $|k| \leq 1$ for all $k \in \mathbb{Z}$, so $|\cdot|$ is forced to be non-archimedean in such cases. Interestingly, the stronger form of the triangle inequality is also necessary of $|\cdot|$ to be non-archimedean, and so the following theorem is often taken as the definition of a non-archimedean absolute value.

Theorem 33.3. *An absolute value $|\cdot|$ on a field K is non-archimedean if and only if it satisfies the non-archimedean triangle inequality. In particular, any absolute value on a field with positive characteristic must satisfy the non-archimedean triangle inequality.*

Proof. The sufficiency has already been noted, so the only issue is necessity. Consider the binomial theorem

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$$

in K for $n \geq 1$. Applying the absolute value to both sides and using the hypothesis that $|\cdot|$ is bounded on the image of $\mathbb{Z}$ in K, say with $|k| \leq C$ for all $k \in \mathbb{Z}$, we get

$$\begin{aligned} |x+y|^n &\leq \sum_{j=0}^{n} C|x|^{n-j}|y| \\ &\leq (n+1)C \max(|x|, |y|)^n \end{aligned}$$

for all $n \geq 1$. Extracting the nth roots gives

$$|x+y| \leq ((n+1)C)^{1/n} \max(|x|, |y|)$$

for all $n \geq 1$. As $n \to \infty$ clearly $((n+1)C)^{1/n} \to 1$, so we obtain the non-archimedean triangle inequality. □

Corollary 29. *If $|\cdot|$ is a non-archimedean absolute value on a field K, then so is $|\cdot|^e$ for all $e > 0$. In particular, $|\cdot|^e$ is an absolute value for all $e > 0$.*

Proof. By the theorem, $|x+y| \leq \max(|x|, |y|)$ for all $x, y \in K$. Raising both sides to the eth power gives the same for $|\cdot|^e$ for any $e > 0$, so in particular $|\cdot|^e$ satisfies the triangle inequality. The rest follows immediately. □

Here is an important refinement of the non-archimedean triangle inequality. Suppose that $|\cdot|$ is non-archimedean. We claim that the inequality $|x+y| \leq \max(|x|, |y|)$ is an equality if $|x| \neq |y|$. Indeed, suppose $|x| < |y|$. We then want to prove $|x+y| = |y|$. Suppose not, so $|x+y| < |y|$. Hence $|x|, |x+y| < |y|$, so

$$\begin{aligned} |y| &= |(y+x) - x| \\ &\leq \max(|y+x|, |-x|) \\ &= \max(|x+y|, |y|) \\ &< |y|, \end{aligned}$$

a contradiction. This has drastic consequences for the topology on K. For example, if $r > 0$ and $a, a' \in K$ satisfy $|a - a'| \leq r$, then $|x - a| \leq r$ if and only if $|x - a'| \leq r$. Hence any point in the disc $B_r[a]$ serves as a "center". More drastically, whereas $B_r[a]$ is a trivially closed set in K, it is in fact also open! Indeed, if $|x_0 - a| \leq r$ then the non-archimedean triangle inequality implies that

$$|x - x_0| < r \implies |x - a| \leq r.$$

Thus $B_r[a]$ contains an open disc around any of its points.

Theorem 33.4. *The topological space K is totally disconnected. That is, its only non-empty connected subsets are one-point sets.*

33.5.3 Obtaining a Valuation form a Non-Archimedean Absolute Value

Let K be a field and let $v\colon K^\times \to \mathbb{R}$ be a valuation. Recall that we obtain a non-archimedean absolute value on K as follows: choose $c \in (0,1)$ and define $|\cdot|_{c,v}\colon K \to \mathbb{R}_{\geq 0}$ by

$$|x|_{c,v} = c^{v(x)}$$

for all $x \in K$. Notice that if we had chose a different number in $(0,1)$, say $d \in (0,1)$, then

$$\begin{aligned}
|x|_{d,v} &= d^{v(x)} \\
&= (c^{\log_c(d)})^{v(x)} \\
&= c^{\log_c(d)v(x)} \\
&= \left(c^{v(x)}\right)^{\log_c(d)} \\
&= |x|_{c,v}^{\log_c(d)}
\end{aligned}$$

for all $x \in K$ where $\log_c(d) > 0$. In particular $|\cdot|_{c,v}$ and $|\cdot|_{d,v}$ induce the same underlying topology.

We can also go backwards. In particular, suppose $|\cdot|$ is an absolute value on K. Then we obtain a valuation on K as follows: choose $c \in (0,1)$ and define $v_{c,|\cdot|}\colon K^\times \to \mathbb{R}$ by

$$v_{c,|\cdot|}(x) = \log_c |x|. \tag{82}$$

for all $x \in K^\times$. As above, a different choice $d \in (0,1)$ would yield an equivalent valuation $v_{d,|\cdot|}$. Indeed, order preserving isomorphisms from $\mathbb{R}$ to itself are of the form $\mathrm{m}_a\colon \mathbb{R} \to \mathbb{R}$

$$\mathrm{m}_a(r) = ar$$

for all $r \in \mathbb{R}$ where $a > 0$. As noted above, there is an $a > 0$ such that $c^a = d$. Then

$$\begin{aligned}
v_{d,|\cdot|}(x) &= \log_d |x| \\
&= \log_{c^a} |x| \\
&= \log_c |ax| \\
&= v_{c,|\cdot|}(ax).
\end{aligned}$$

In any case, all of the definitions corresponding to valuation can also be carried over for non-archimedean absolute values. For instance, the valuation domain with respect to $|\cdot|$ is the subring of K given by

$$R_{|\cdot|} = \{x \in K \mid |x| \geq 1\}.$$

Similarly the maximal ideal associated to $|\cdot|$ is the maximal ideal in $R_{|\cdot|}$ given by

$$\mathfrak{m}_{|\cdot|} = \{x \in K \mid |x| > 1\}.$$

Technically speaking, (82) is only a valuation on K when $|\cdot|$ is a non-archimedean absolute value. Indeed, valuations on K must satisfy $v(x+y) \geq \min(v(x), v(y))$ for all $x, y \in K$, and we only get this if $|\cdot|$ is a non-archimedean absolute value (so $|\cdot|$ satisfies the dual axiom: $|x+y| \leq \max(|x|, |y|)$. On the other hand, it's still interesting to consider what properties $v_{c,|\cdot|}$ satisfies whenever $|\cdot|$ is an archimedean absolute value. For instance, consider the case where $|\cdot|$ is the usual archimedean absolute value on $K = \mathbb{Q}$. It seems natural in this case to set $c = 1/e$, thus our "valuation" would be defined by

$$v(x) = -\log|x|$$

for all $x \in \mathbb{Q}$. In particular, v still satisfies properties 1 and 2 in Definition (33.1), however it does fail property 3. Even though $|\cdot|$ doesn't satisfy the non-archimedean triangle inequality, it still satisfies the usual triangle inequality, so this should translate to some property that v has. Using the fact that $v(x) = -\log|x|$, we see that this property is:

$$\begin{aligned}
v(x+y) &= -\log|x+y| \\
&\geq -\log(|x| + |y|) \\
&\geq -\log|x| - \log|y| \\
&= v(x) + v(y).
\end{aligned}$$

Thus we might say v is an **archimedean** valuation where we replace the stronger property 3 in Definition (33.1) with the weaker property that $v(x+y) \geq v(x) + v(y)$ for all $x, y \in K$.

Let's see what the objects associated to v should look like in this case. The "valuation domain" of v is given by

$$R_v = \{x \in \mathbb{Q} \mid v(x) \geq 0\} = [-1,1] \cap \mathbb{Q} = \mathrm{B}_1[0].$$

Clearly this is not a domain (not even a ring), but let's consider what properties are still left over. First of all, note that the only reason this is not a ring is that given $x, y \in R_v$, it may not be the case that $x + y \in R_v$. On the other hand, if x, y are sufficiently small, then we do have $x + y \in R_v$. Furthermore, all of the ring axioms are satisfied for suffciently small elements of R_v.

The "maximal ideal" of v is given by

$$\mathfrak{m}_v = \{x \in \mathbb{Q} \mid v(x) > 0\} = (-1,1) \cap \mathbb{Q} = \mathrm{B}_1(0).$$

The "residue field" of v is given by

$$R_v/\mathfrak{m}_v = [-1,1] \cap \mathbb{Q}/(-1,1) \cap \mathbb{Q} = \{-\overline{1}, \overline{0}, \overline{1}\}.$$

Here $\overline{0}$ should represent "sufficiently small" elements of R_v. The "unit group" of R_v is given by

$$U_v = \{x \in \mathbb{Q} \mid v(x) = 0\} = \{-1, 1\}.$$

Notice that "uniformizers" exists in R_v in the sense that every element in R_v can be expressed uniquely as

$$x = \pm \left(\frac{1}{e}\right)^{v(x)}.$$

Thus $1/e$ is a uniformizer for v.

Proposition 33.9. *Let $a_0, \dots, a_{n-1}, \alpha \in \mathbb{R}$ with $|a_i| \leq 1$ for all $0 \leq i \leq n-1$ and $a_0 \neq 0$. Suppose we have*

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0.$$

Then $|\alpha| \leq 1$.

Proof. Assume for a contradiction that $|\alpha| > 1$. Then

$$\begin{aligned} |a_0| &= |\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha| \\ &= |\alpha||a_{n-1}\alpha^{n-1} + \cdots + a_1| \\ &= |\alpha||a_{n-1}\alpha^{n-1} + \cdots + a_1| \\ &> 1, \end{aligned}$$

which is a contradiction. □

33.5.4 Ostrowski's Theorem

We now wish to determine all non-trivial absolute values on $\mathbb{Q}$. We shall write $|\cdot|_\infty$ to denote the usual absolute value on $\mathbb{Q}$. For each prime p, let v_p be the valuation on $\mathbb{Q}$ defined as in Example (33.1). In particular, given $a/b \in \mathbb{Q}^\times$, we write $a/b = p^n\widetilde{a}/\widetilde{b}$ where $n \in \mathbb{Z}$ and $\widetilde{a}, \widetilde{b} \in \mathbb{Z}$ such that p is not a factor of neither $\widetilde{a}$ nor $\widetilde{b}$, and we set $v(a/b) = n$. Next, let $|\cdot|_p := |\cdot|_{1/p, v_p}$ be the corresponding absolute value with $c = 1/p$.

Theorem 33.5. *The absolute values on $\mathbb{Q}$ are one of the following:*

1. *The trivial one;*
2. *The ones of the form $|\cdot|_\infty^e$ where $0 < e \leq 1$;*
3. *The ones of the form $|\cdot|_p^e$ where $0 < e < \infty$ and p prime.*

These families for each varying exponent e also form the topological equivalence classes of such absolute values.

Proof. By Theorem (33.2), there are no unexpected topological equivalences. Thus it remains to prove that the only archimedean absolute values are powers of $|\cdot|_\infty$ and the only non-trivial non-archimedean absolute values are powers of $|\cdot|_p$ for some prime p. Let us first consider a non-trivial non-archimedean absolute value $|\cdot|$ on $\mathbb{Q}$. Note that necessarily we have $|n| \leq 1$ for all $n \in \mathbb{Z}$. If $|p| = 1$ for all primes p, then since $\mathbb{Q}^\times$ is multiplicatively generated by the primes and ± 1 we conclude that $|\cdot|$ is trivial on $\mathbb{Q}$. Thus $|p| < 1$ for some prime p. Such a prime is unique because if $|q| < 1$ for some other prime q then we have $ap + bq = 1$ for some $a, b \in \mathbb{Z}$ with $a, b \neq 0$, in which case

$$\begin{aligned}1 &= |1| \\ &= |ap + bq| \\ &\leq \max(|a||p|, |b||q|) \\ &< \max(|a|, |b|) \\ &\leq 1\end{aligned}$$

gives a contradiction. Hence $|q| = 1$ for all primes $q \neq p$. Since $|\cdot|$ is non-archimedean, $|\cdot|^e$ is an absolute value for all $e > 0$. Thus since $|p| \in (0,1)$ by the choice of p, by replacing $|\cdot|$ with $|\cdot|^3$ for some $e > 0$ we may arrange that $|p| = 1/p$. Hence $|\cdot|$ and $|\cdot|_p$ agree on all primes, and since these together with -1 generated $\mathbb{Q}^\times$ multiplicatively, we conclude $|\cdot| = |\cdot|_p$.

Now we suppose $|\cdot|$ is archimedean and we seek to prove $|\cdot| = |\cdot|_\infty^e$ for some $e \in (0,1]$. Since $|\cdot|$ is archimedean, it is unbounded on $\mathbb{Z}$, we must have $|b| > 1$ for some $b \in \mathbb{Z}$. Switching signs if necessary, we can assume $b > 0$ and hence $b > 1$. We take $b \in \mathbb{Z}^+$ to be minimal with $|b| > 1$; at the end of the proof it will follow that $b = 2$, but right now we do not know this to be the case. Choose the unique $e > 0$ such that $|b| = b^e$. Consider the base-b expansion of an integer $n \geq 1$: write

$$n = a_0 + a_1 b + \cdots + a_s b^s$$

with $0 \leq a_j < b$, $s \geq 0$, and $a_s \geq 1$. By minimality of b we have $|a_j| \leq 1$ for all j, so

$$\begin{aligned}|n| &\leq \sum_{j=0}^{s} |a_j||b|^j \\ &\leq \sum_{j=0}^{s} |b|^j \\ &= |b|^s(1 + 1/|b| + \cdots 1/|b|^s) \\ &= \frac{|b|^s}{1 - 1/|b|}.\end{aligned}$$

If we let $C = 1/(1 - 1/|b|) > 0$ we have

$$|n| \leq Cb^{es} \leq Cn^e$$

because $b^s \leq n$ and $C > 0$. This says $|k| \leq Ck^e$ for all $k \geq 1$, so by fixing k we have $|k^r| \leq Ck^{re}$ for all $r \geq 1$. Extracting rth roots gives $|k| \leq C^{1/r}k^e$, and taking $r \to \infty$ gives $|k| \leq k^e = |k|_\infty^e$ for all $k \geq 1$. Hence, passing to $-k$ gives $|k| \leq |k|_\infty^e$ for all $k \in \mathbb{Z}$.

We now prove the reverse inequality $|k| \geq |k|_\infty^e$ for all $k \in \mathbb{Z}$, and so $|k| = |k|_\infty^e$ holds for all $k \in \mathbb{Z}$, which in turn gives the identity $|\cdot| = |\cdot|_\infty^e$ on $\mathbb{Q}$ as desired. As above, it suffices to prove $|n| \geq C'n^e$ for some $C' > 0$ and all $n > 0$ (as then we can specialize to rth power, extract rth roots, and take $r \to \infty$). Using notation as above with base-b expansion of n, we have $b^{s+1} > n \geq b^s$, so

$$\begin{aligned}b^{e(s+1)} &= |b|^{s+1} \\ &= |b^{s+1}| \\ &= |b^{s+1} - n + n| \\ &\leq |b^{s+1} - n| + |n| \\ &\leq (b^{s+1} - n)^e + |n|,\end{aligned}$$

where the final step uses the proved inequality $|k| \leq k^e$ for $k = b^{s+1} - n > 0$. Hence

$$\begin{aligned}|n| &\geq b^{(s+1)e} - (b^{s+1} - n)^e \\ &= b^{(s+1)e}(1 - (1 - n/b^{s+1})^e) \\ &\geq n^e(1 - (1 - 1/b)^e),\end{aligned}$$

so taking $C' = 1 - (1 - 1/b)^e > 0$ gives $|n| \geq C'n^e$ for all $n \geq 1$, as required. $\square$

33.5.5 Variants of Ostrowski's Theorem

We shall use a similar method to determine all non-trivial absolute values up to topological equivalence on the rational function field $F = k(T)$ when k is a finite field, and we will also study fraction fields of more general Dedekind domains. We first focus on $F = k(T)$ with k finite. Observe that if $|\cdot|$ is a non-trivial absolute value on F then its restriction to k is trivial because $k^\times$ consists of roots of unity. Hence, we shall now abandon the finiteness restriction on k and will instead let k be an arbitrary field, but we will only classify (up to topological equivalence) those absolute values on $F = k(T)$ whose restriction to k is trivial; it is equivalent to say that the absolute value is bounded on k. Since the image of $\mathbb{Z}$ in F lands in k, all such absolute values must be non-archimedean. (If k has characteristic 0, then one can construct archimedean absolute values on $k(T)$, necessarily nontrivial on k, if and only if the underlying set for k does not exceed the cardinality of the continuum).

33.5.6 Completion of Algebraic Closure

Let K be a field complete with respect to a non-trivial non-archimedean absolute value $|\cdot|$. It is natural to seek a "smallest" extension of K that is both complete and algebraically closed. To this end, let $\overline{K}$ be an algebraic closure of K. Note that $\overline{K}$ is endowed with a unique absolute value extending that on K. Indeed, define $|\cdot|'$ on $\overline{K}$ as follows: if $b \in \overline{K}$, then we set

$$\begin{aligned}
|b|' &= \left|\mathrm{N}_{K(b)/K}(b)\right| \\
&= \left|\left(\prod_{\sigma\colon K(b)\hookrightarrow\overline{K}} \sigma(b)\right)^{[K(b):K]_{\mathrm{i}}}\right| \\
&= \left(\prod_{\sigma\colon K(b)\hookrightarrow\overline{K}} |\sigma(b)|\right)^{[K(b):K]_{\mathrm{i}}}
\end{aligned}$$

where σ runs through the distinct K-embeddings of $K(b)$ in $\overline{K}$. In particular, if $\sigma\colon K(b) \hookrightarrow \overline{K}$ is a K-embedding, then we have $|\sigma(b)|' = |b|'$. Let $\mathbb{C}_K$ be the completion of $\overline{K}$ with respect to this absolute value. The field $\mathbb{C}_K$ is to be considered as an analogue of the complex numbers relative to K, and for $K = \mathbb{Q}_p$ it is usually denoted $\mathbb{C}_p$.

Theorem 33.6. *$\mathbb{C}_K$ is algebraically closed.*

Proof. Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a polynomial in $\mathbb{C}_K[X]$. Since $\overline{K}$ is dense in $\mathbb{C}_K$, there exists polynomials

$$f_j = X^n + a_{n-1,j}X^{n-1} + \cdots + a_{0,j}$$

in $\overline{K}[X]$ with $a_{ij} \to a_i$ in $\mathbb{C}_K$ as $j \to \infty$. If $a_i \neq 0$, then we may arrange that $|a_{ij} - a_i| < \min(|a_i|, 1/j)$ for all j. Note that in this case, we have $|a_{ij}| = |a_i|$ for all j. Indeed, $|a_{ij}| \leq \max(|a_i|, |a_{ij} - a_i|) = |a_i|$, where in fact we have equality $|a_{ij}| = |a_i|$ since $|a_i| \neq |a_{ij} - a_i|$. If $a_i = 0$ then we may take $a_{ij} = 0$ for all j. Hence, for all $0 \leq i \leq n-1$ we have $|a_{ij}| = |a_i|$ and $|a_{ij} - a_i| < 1/j$ for all j. Of course, we have no control over the finite extensions $K(a_{ij}) \subseteq \overline{K}$ as j varies for a fixed i.

Since $\overline{K}$ is algebraically closed, we can pick a root $r_j \in \overline{K}$ for f_j for all j. The idea is to find a subsequence of the r_j's that is Cauchy, so it has a limit r in the *complete* field $\mathbb{C}_K$, and clearly $f(r) = \lim f_j(r_j) = 0$. This gives a root of f in $\mathbb{C}_K$. Since $f_j(r_j) = 0$ for all j, we have

$$\begin{aligned}
|r_j^n| &= \left|-\sum_{i=0}^{n-1} a_{ij} r_j^i\right| \\
&= \left|\sum_{i=0}^{n-1} a_{ij} r_j^i\right| \\
&\leq \max_i |a_{ij}||r_j|^i \\
&= \max_i |a_i||r_j|^i.
\end{aligned}$$

Hence, for each j there exists $0 \leq i(j) \leq n-1$ such that $|r_j|^n \leq |a_{i(j)}||r_j|^{i(j)}$, so $|r_j| \leq |a_{i(j)}|^{1/(n-i(j))}$. Thus if we set

$$C = \max(|a_0|^{1/n}, |a_1|^{1/(n-1)}, \ldots, |a_{n-1}|),$$

Then we have $|r_j| \leq C$ for all j. Note that C only depends on the coefficients a_i of f. Since f and f_j are monic with the same degree, we have

$$\begin{aligned}
|f(r_j)| &= |f(r_j) - f_j(r_j)| \\
&= \left|\sum_{i=0}^{n-1}(a_i - a_{ij})r_j^i\right| \\
&\leq \max_i |a_i - a_{ij}||r_j|^i \\
&\leq \max_i |a_i - a_{ij}| \cdot \max(1, C^{n-1}) \\
&\leq \frac{\max(1, C^{n-1})}{j}
\end{aligned}$$

for all j. Hence, $f(r_j) \to 0$ as $j \to \infty$. We shall now use this fact to infer that (r_j) has a Cauchy subsequence in $\mathbb{C}_K$, which in turn will complete the proof.

Let L be a finite extension of $\mathbb{C}_K$ in which the monic f splits, say $f(X) = \prod_k (X - \rho_k)$. We (uniquely) extend the absolute value on the (complete) field $\mathbb{C}_K$ to one on L, so we may rewrite the condition $f(r_j) \to 0$ as

$$\lim_{j\to\infty} \prod_{k=1}^{n} (r_j - \rho_k) = 0$$

in L. In other words, $\prod_{k=1}^n |r_j - \rho_k| \to 0$ in $\mathbb{R}$. Hence, by the pigeonhole principle, since there are only finitely many k's we must have that for some $1 \leq k_0 \leq n$ the sequence $(|r_j - \rho_{k_0}|)_j$ has a subsequence converging to 0. Some subsequence of the r_j's must therefore converge to ρ_{k_0} in L, so this subsequence is Cauchy in $\mathbb{C}_K$. □

Let $f = \sum a_i X^i \in K[X]$ be monic of degree $n > 0$, so the roots of f in $\mathbb{C}_K$ lie in $\overline{K}$. An inspection of the proof of Theorem (33.6) shows that the argument yields the following general result:

Lemma 33.7. *Let (f_j) be a sequence of monic polynomials $f_j = \sum a_{ij} X^j$ of degree n in $K[X]$ such that $a_{ij} \to a_i$ as $j \to \infty$ for all $0 \leq i \leq n-1$. Let $r_j \in \overline{K}$ be a root of f_j for each j. There exists a subsequence of (r_j) that converges to a root of $f = \sum a_i X^i$ in $\overline{K}$.*

We many now deduce the following general result that is usually called "continuity of roots" (in terms of their dependence on the coefficents of f).

Theorem 33.8. *Let $r \in \overline{K}$ be a root of a degree n monic polynomial $f = \sum a_i X^i \in K[X]$ with $\mathrm{ord}_r(f) = \mu > 0$. Fix $\varepsilon_0 > 0$ such that all roots of f in $\overline{K}$ distinct from r have distance at least ε_0 from r (if there are no other roots, we may use any $\varepsilon_0 > 0$). For all $0 < \varepsilon < \varepsilon_0$ there exists $\delta = \delta_{\varepsilon,f} > 0$ such that if $g = \sum b_i X^i \in K[X]$ is monic with degree n and $|a_i - b_i| < \delta$ for all i then g has exactly μ roots (with multiplicity) in the open disc $\mathrm{B}_\varepsilon(r) = \{x \in \overline{K} \mid |x - r| < \varepsilon\}$.*

Proof. We argue by contradiction. Fix a choice of ε. If there exists no corresponding δ, then we would get a sequence of monic polynomials $f_j = \sum a_{ij} X^i \in K[X]$ with degree n such that $a_{ij} \to a_i$ as $j \to \infty$ for each i and each f_j does not have exactly μ roots on $\mathrm{B}_\varepsilon(r)$. Pick factorizations $f_j = \prod_{k=1}^n (X - \rho_{jk})$ upon enumerating the n roots (with multiplicity) for each f_j in $\overline{K}$. By Lemma (33.7) applied to (ρ_{j1}), we can pass to a subsequence of the f_j's so $\rho_{j1} \to \rho_1$ with ρ_1 some root of f in $\overline{K}$. Successively working with $(\rho_{jk})_j$ for $k = 2, \ldots, n$ and passing through successive subsequence of subsequences, etc., we may suppose that there exist limits $\rho_{jk} \to \rho_k$ in $\overline{K}$ as $j \to \infty$ for each fixed $1 \leq k \leq n$.

Each ρ_k must be a root of f, but we claim more: every root of f arises in the form ρ_k for exactly as many k's as the multiplicity of the root. Working in the finite-dimensional $\overline{K}$-vector space of polynomials of degree $\leq n$ (given the sup-norm with respect to an arbitrary $\overline{K}$-basis, the choice of which does not affect the topology), we have

$$f_j = \prod_{k=1}^{n} (X - \rho_{jk}) \to \prod_{k=1}^{n} (X - \rho_k),$$

yet also $f_j \to f$. Hence, $f = \prod_{k=1}^n (X - \rho_k)$ in $\overline{K}[X]$. That is, $\{\rho_k\}$ is indeed the set of roots of f in $\overline{K}$ counted with multiplicities. Hence, $r = \rho_k$ for exactly μ values of k, say for $1 \leq k \leq \mu$ by relabelling.

By passing to a subsequence we may arrange that for each $1 \leq k \leq n$, we have $|\rho_{jk} - \rho_k| < \varepsilon$ for all j. In particular, if $1 \leq k \leq \mu$ we have $|\rho_{jk} - r| < \varepsilon$. Since all roots r' of f distinct from r have distance $\geq \varepsilon_0 > \varepsilon$ from r, by the non-archimedean triangle inequality we have $|\rho_{jk} - r'| \geq \varepsilon_0 > \varepsilon$ for all $1 \leq k \leq \mu$ and any j. However, if $k > \mu$ then ρ_k is such an r', yet $|\rho_{jk} - \rho_k| < \varepsilon$ for all j and all k, so for each fixed j we must have $|\rho_{jk} - r| \geq \varepsilon_0 > \varepsilon$ for all $k > \mu$. Thus, for the j's that remain (as we have passed to some subsequence of the original sequence), $\rho_{j1}, \ldots, \rho_{j\mu}$ are precisely the roots of f_j (with multiplicity) that are within a distinct $< \varepsilon$ from the root r of f. This contradicts the assumption on the f_j's. □

Here is an important corollary that is widely used.

Corollary 30. *Let $f \in K[X]$ be a separable monic polynomial with degree n. Choose $\varepsilon > 0$ as in Theorem (33.8). For each monic $g \in K[X]$ with degree n and coefficients sufficiently close to those of f, g is separable and each root of g in K_{sep} is within a distance $< \varepsilon$ from a unique root of f in K_{sep}. Moreover, if f is irreducible, then g is irreducible.*

Proof. We apply Theorem (33.8) with $\mu = 1$ to conclude that if such a g is coefficientwise sufficiently close to f then each of the n roots of g (with multiplicity) is within a distance $< \varepsilon$ from a unique root of f. In particular, g has n distinct roots and hence is separable. Thus all roots under consideration lie in K_{sep}. The uniqueness aspect, together with the fact that $\mathrm{Gal}(K_{\mathrm{sep}}/K)$ acts on K_{sep} by isometries, implies that the $\mathrm{Gal}(K_{\mathrm{sep}}/K)$-orbit of a root of g has the same size as the $\mathrm{Gal}(K_{\mathrm{sep}}/K)$-orbit of the corresponding nearest root of f. Hence, the degree-labelling of the irreducible factorization of g over K "matches" that of the separable f, and in particular if f is irreducible, then g is irreducible. □

33.6 Local Fields

33.6.1 Local Conductor

Definition 33.11. Let L/K be a finite extension of local non-archimedean fields. For each $n \in \mathbb{N}$ we set

$$U_K^{(n)} := 1 + \mathfrak{m}_K^n = \{u \in \mathcal{O}_K^\times \mid u \equiv 1 \bmod \mathfrak{m}_K^n\},$$

where $\mathcal{O}_K$ is the valuation ring of K and where $\mathfrak{m}_K$ is the maximal ideal of K. We call $U_K^{(n)}$ the n**th higher unit group** of K. Note that $U_K^{(0)} = \mathcal{O}_K$ and $U_K^{(1)} = \mathcal{O}_K^\times$. The **conductor** of L/K, denoted $n = \mathfrak{f}(L/K)$, is defined to be the smallest integer n such that

$$\mathrm{N}_{L/K}(L^\times) \supseteq U_K^{(n)}$$

where $\mathrm{N}_{L/K}$ is the field norm map. Equivalently, n is the smallest integer such that the local Artin map is trivial on $U_K^{(n)}$.

The conductor $n = \mathfrak{f}(L/K)$ measures the ramification of the extension L/K. For instance, the extension is unramified if and only if $n = 0$ and it is tamely ramified if and only if $n = 1$.

33.7 p-adic fields

Throughout this subsection we fix a positive prime p.

Definition 33.12. A p**-adic field** K of **degree** n is a finite extension $K/\mathbb{Q}_p$ such that $[K : \mathbb{Q}_p] = n$.

Let K be a p-adic field of degree n. The absolute value $|\cdot| = |\cdot|_p$ of $\mathbb{Q}_p$ extends to a unique absolute value (which we denote again by $|\cdot|$) on K by setting

$$|x| = |\mathrm{N}(x)|^{1/n}$$

for all $x \in K$ where $\mathrm{N}\colon K^\times \to \mathbb{Q}_p^\times$ is the norm function.
Throughout this subsection, let K be a finite extension of $\mathbb{Q}_p$ and let L be a finite extension of K. Then $\mathcal{O}_K$ and $\mathcal{O}_L$, the ring of integers of K and L are discrete valuation domains, so they have unique maximal ideals $\mathfrak{p}_K = (\pi_K)$ and $\mathfrak{p}_L = (\pi_L)$ where π_K and π_L are called **uniformizers**.

Definition 33.13. Let L/K be a finite extension of p-adic fields.

1. The **ramification index** of L/K is the positive integer e such that

$$\mathfrak{p}_K \mathcal{O}_L = \mathfrak{p}_L^e.$$

   (a) We say L/K is **unramified** if $e = 1$.
   (b) We say L/K is **totally ramified** if $e = [L : K]$.
   (c) We say L/K is **tamely ramified** if e is prime to p.
   (d) We say L/K is **wildly ramified** if it is not tamely ramified.

2. The **residue field degree** of L/K is the positive integer f such that

$$[\Bbbk_L : \Bbbk_K] = f.$$

3. The **discriminant** of L/K is the square of the determinant of the matrix

$$\begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{pmatrix},$$

   where $\sigma_1, \dots, \sigma_n$ are embeddings of L in an algebraic closure $\overline{K}$ and $\{\beta_1, \dots, \beta_n\}$ forms a basis of $\mathcal{O}_L$ as a free $\mathcal{O}_K$-modules. The discriminant of L/K is an element of $\mathcal{O}_K$ which is well-defined up to the square of a unit. In particular, it is of the form $\pi_K^c u$ where u is a unit. The value c is called the **discriminant exponent** of L/K.

Example 33.5. We describe all quadratic extensions of $\mathbb{Q}_p$. First assume p is odd. Let u be a unit in $\mathbb{Z}_p$ which is not a square modulo p. Then the quadratic extensions of $\mathbb{Q}_p$ are $\mathbb{Q}_p(\sqrt{u})$ (which is the unramified extension), $\mathbb{Q}_p(\sqrt{p})$, and $\mathbb{Q}_p(\sqrt{pu})$. Now consider the case where $p = 2$. Let u be any value in $\mathbb{Z}_2$ which is congruent to 5 modulo 8. Then again we have the three quadratic extensions $\mathbb{Q}_2(\sqrt{u})$ (which is the unramified extension), $\mathbb{Q}_2(\sqrt{2})$, and $\mathbb{Q}_2(\sqrt{2u})$. However we also have four other quadratic extensions, namely $\mathbb{Q}_2(i)$, $\mathbb{Q}_2(i\sqrt{u})$, $\mathbb{Q}_2(i\sqrt{2})$, and $\mathbb{Q}_2(i\sqrt{2u})$, where $i = \sqrt{-1}$.

Example 33.6. Let $K = \mathbb{Q}_2(\alpha)$ where α is a root of

$$f = x^8 + x^4 + x^3 + x^2 + 1.$$

This is a degree 8 extension of $\mathbb{Q}_2$ with Galois group C_8. What's interesting about this field (called the octic field) is that it's not the 2-completion of an octic extension of $\mathbb{Q}$ with Galois group C_8. It has minimal degree for this phenomenom.

Part IV
Linear Algebra

34 Matrix Representation of a Linear Map

Throughout this section, let K be a field, let V be a K-vector space with basis $\boldsymbol{\beta} = \{\beta_1, \dots, \beta_m\}$, and let W be a K-vector space with basis $\boldsymbol{\gamma} = \{\gamma_1, \dots, \gamma_n\}$. On a first encounter in linear algebra, one typically studies *concrete* vector spaces like $\mathbb{R}^2$ and *concrete* matrices like $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : \mathbb{R}^2 \to \mathbb{R}^2$. In a more abstract setting, one studies *abstract* vectors spaces like V, W and *abstract* linear maps between them like $T \colon V \to W$. However, this abstract setting is not as abstract as it may first seem. Indeed, it turns out that we can translate everything in the abstract setting to the more concrete setting. We will describe this translation in this note.

34.1 From the Abstract Setting to the Concrete Setting

34.1.1 Column Representation of a Vector

Let $v \in V$. Then for each $1 \le i \le m$, there exists unique $a_i \in K$ such that

$$v = \sum_{i=1}^m a_i \beta_i.$$

Since the a_i are uniquely determined, we are justified in making the following definition:

Definition 34.1. The **column representation of v with respect to the basis β**, denoted $[v]_\beta$, is defined by

$$[v]_\beta := \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}.$$

Proposition 34.1. *Let $[\cdot]_\beta \colon V \to K^m$ be given by*

$$[\cdot]_\beta(v) = [v]_\beta$$

for all $v \in V$. Then $[\cdot]_\beta$ is an isomorphism.

Proof. We first show that $[\cdot]_\beta$ is linear. Let $v_1, v_2 \in V$ and $c_1, c_2 \in K$. Then for each $1 \leq i \leq m$, there exists unique $a_{i1}, a_{i2} \in K$ such that

$$v_1 = \sum_{i=1}^m a_{i1}\beta_i \quad \text{and} \quad v_2 = \sum_{i=1}^m a_{i2}\beta_i.$$

Therefore we have

$$\begin{aligned} a_1 v_1 + a_2 v_2 &= a_1 \sum_{i=1}^m a_{i1}\beta_i + a_2 \sum_{i=1}^m a_{i2}\beta_i \\ &= \sum_{i=1}^m (a_1 a_{i1} + a_2 a_{i2})\beta_i. \end{aligned}$$

This implies

$$\begin{aligned} [a_1 v_1 + a_2 v_2]_\beta &= \begin{pmatrix} a_1 a_{11} + a_2 a_{12} \\ \vdots \\ a_1 a_{m1} + a_2 a_{m2} \end{pmatrix} \\ &= a_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + a_2 \begin{pmatrix} a_{12} \\ \vdots \\ a_{m2} \end{pmatrix} \\ &= a_1 [v_1]_\beta + a_2 [v_2]_\beta. \end{aligned}$$

Therefore $[\cdot]_\beta$ is linear. To see that $[\cdot]_\beta$ is an isomorphism, note that $[\beta_i] = e_i$, where e_i is the column vector in K^n whose i-th entry is 1 and whose entry everywhere else is 0. Thus, $[\cdot]_\beta$ restricts to a bijection on basis sets

$$[\cdot]_\beta \colon \{\beta_1, \dots, \beta_m\} \to \{e_1, \dots, e_n\},$$

and so it must be an isomorphism. □

34.1.2 Matrix Representation of a Linear Map

Let T be a linear map from V to W. Then for each $1 \leq i \leq m$ and $1 \leq j \leq n$, there exists unique elements $a_{ji} \in K$ such that

$$T(\beta_i) = \sum_{j=1}^n a_{ji}\gamma_j \tag{83}$$

for all $1 \leq i \leq m$. Since the a_{ji} are uniquely determined, we are justified in making the following definition:

Definition 34.2. The **matrix representation of T with respect to the bases β and γ**, denoted $[T]_\beta^\gamma$, is defined to be the $n \times m$ matrix

$$[T]_\beta^\gamma := \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}.$$

Proposition 34.2. *Let T be a linear map from V to W. Then*

$$[T]_\beta^\gamma [v]_\beta = [T(v)]_\gamma$$

for all $v \in V$.

Remark 46. In terms of diagrams, this proposition says that the following diagram is commutative

$$\begin{tikzcd} K^m \arrow[r, "{[T]_\beta^\gamma}"] & K^n \\ V \arrow[u, "{[\cdot]_\beta}"] \arrow[r, "T"'] & W \arrow[u, "{[\cdot]_\gamma}"'] \end{tikzcd}$$

Proof. Let $v \in V$ and let $a_i, a_{ji} \in K$ be the unique elements such that

$$v = \sum_{i=1}^{m} a_i \beta_i \quad \text{and} \quad T(\beta_i) = \sum_{j=1}^{n} a_{ji} \gamma_j$$

for all $1 \leq i \leq m$. Then

$$\begin{aligned} [T]_\beta^\gamma [v]_\beta &= \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=1}^m a_{1i} a_i \\ \vdots \\ \sum_{i=1}^m a_{ni} a_i \end{pmatrix} \\ &= [T(v)]_\gamma. \end{aligned}$$

Where the last equality follows from

$$\begin{aligned} T(v) &= T\left(\sum_{i=1}^{m} a_i \beta_i \right) \\ &= \sum_{i=1}^{m} a_i T(\beta_i) \\ &= \sum_{i=1}^{m} a_i \sum_{j=1}^{n} a_{ji} \gamma_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ji} a_i \right) \gamma_j. \end{aligned}$$

□

Theorem 34.1. *Let V, V', and V'' be K-vector spaces with bases $\boldsymbol{\beta}$, $\boldsymbol{\beta}'$, and $\boldsymbol{\beta}''$ respectively and let $T \colon V \to V'$ and $T' \colon V' \to V''$ be two K-linear maps. Then*

$$[T' \circ T]_{\boldsymbol{\beta}}^{\boldsymbol{\beta}''} = [T']_{\boldsymbol{\beta}'}^{\boldsymbol{\beta}''} [T]_{\boldsymbol{\beta}}^{\boldsymbol{\beta}'}.$$

Proof. Let $[v]_{\boldsymbol{\beta}} \in K^n$. Then we have

$$\begin{aligned} [T' \circ T]_{\boldsymbol{\beta}}^{\boldsymbol{\beta}''} [v]_{\boldsymbol{\beta}} &= [(T' \circ T)(v)]_{\boldsymbol{\beta}''} \\ &= [T'(T(v))]_{\boldsymbol{\beta}''} \\ &= [T']_{\boldsymbol{\beta}'}^{\boldsymbol{\beta}''} [T(v)]_{\boldsymbol{\beta}'} \\ &= [T']_{\boldsymbol{\beta}'}^{\boldsymbol{\beta}''} [T]_{\boldsymbol{\beta}}^{\boldsymbol{\beta}'} [v]_{\boldsymbol{\beta}}. \end{aligned}$$

Therefore $[T' \circ T]_{\boldsymbol{\beta}}^{\boldsymbol{\beta}''} = [T']_{\boldsymbol{\beta}'}^{\boldsymbol{\beta}''} [T]_{\boldsymbol{\beta}}^{\boldsymbol{\beta}'}$. □

34.2 Change of Basis Matrix

In this subsection, let $\boldsymbol{\alpha}$ be another basis for V and let δ be another basis for W.

Definition 34.3. Let $1_V \colon V \to V$ denote the identity map. The **change of basis matrix from $\boldsymbol{\beta}$ to $\boldsymbol{\alpha}$** is defined to be the matrix $[1_V]_{\boldsymbol{\alpha}}^{\boldsymbol{\beta}}$.

Remark 47.

1. The reason why we say from $\boldsymbol{\beta}$ to $\boldsymbol{\alpha}$ and not from $\boldsymbol{\alpha}$ to $\boldsymbol{\beta}$ is because we want to express the new basis $\boldsymbol{\alpha}$ in terms of the old basis $\boldsymbol{\beta}$.

2. Observe that the change of basis matrix from $\boldsymbol{\beta}$ to $\boldsymbol{\alpha}$ is invertible, with inverse being $[1_V]^{\boldsymbol{\alpha}}_{\boldsymbol{\beta}}$. Indeed, we have

$$\begin{aligned}[1_V]^{\boldsymbol{\beta}}_{\boldsymbol{\alpha}}[1_V]^{\boldsymbol{\alpha}}_{\boldsymbol{\beta}} &= [1_V \circ 1_V]^{\boldsymbol{\beta}}_{\boldsymbol{\beta}} \\ &= [1_V]^{\boldsymbol{\beta}}_{\boldsymbol{\beta}} \\ &= \mathrm{I}_m,\end{aligned}$$

   where I_m is the $m \times m$ identity matrix.

In applications, we often describe a change of basis from $\boldsymbol{\beta}$ to $\boldsymbol{\alpha}$ as a concrete matrix like

$$C = \begin{pmatrix} c_{11} & \cdots & c_{1m} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mm} \end{pmatrix}.$$

Let us show how to work with C in terms of our notation.

Proposition 34.3. *Let C be the change of basis matrix from $\boldsymbol{\beta}$ to $\boldsymbol{\alpha}$. Then*

$$C[v]_{\boldsymbol{\alpha}} = [v]_{\boldsymbol{\beta}}$$

for all $v \in V$.

Proof. Let $v \in V$. Then

$$\begin{aligned}C[v]_{\boldsymbol{\alpha}} &= [1_V]^{\boldsymbol{\beta}}_{\boldsymbol{\alpha}}[v]_{\boldsymbol{\alpha}} \\ &= [1_V(v)]_{\boldsymbol{\beta}} \\ &= [v]_{\boldsymbol{\beta}}.\end{aligned}$$

□

Proposition 34.4. *Let $T\colon V \to W$ be a linear map, let C be the change of basis matrix from $\boldsymbol{\beta}$ to $\boldsymbol{\alpha}$, and let D be the change of basis matrix from $\boldsymbol{\gamma}$ to $\boldsymbol{\delta}$. Then*

$$[T]^{\boldsymbol{\delta}}_{\boldsymbol{\alpha}} = D^{-1}[T]^{\boldsymbol{\gamma}}_{\boldsymbol{\beta}}C.$$

In particular, if $U\colon V \to V$ is an endomorphism, then

$$[U]^{\boldsymbol{\alpha}}_{\boldsymbol{\alpha}} = C^{-1}[U]^{\boldsymbol{\beta}}_{\boldsymbol{\beta}}C.$$

Proof. We have

$$\begin{aligned}[T]^{\boldsymbol{\delta}}_{\boldsymbol{\alpha}} &= [1_W \circ T \circ 1_V]^{\boldsymbol{\delta}}_{\boldsymbol{\alpha}} \\ &= [1_W]^{\boldsymbol{\delta}}_{\boldsymbol{\gamma}}[T]^{\boldsymbol{\gamma}}_{\boldsymbol{\beta}}[1_V]^{\boldsymbol{\beta}}_{\boldsymbol{\alpha}} \\ &= D^{-1}[T]^{\boldsymbol{\gamma}}_{\boldsymbol{\beta}}C.\end{aligned}$$

□

Example 34.1. Let $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ be an orthogonal transformation. Recall that this means T is a linear map which preserves the (usual) inner-product: for all $v, w \in \mathbb{R}^2$, we have

$$\langle Tv, Tw \rangle = \langle v, w \rangle.$$

Let $\boldsymbol{e} = e_1, e_2$ be the standard unit vectors in $\mathbb{R}^2$ and denote $A = [T]^{\boldsymbol{e}}_{\boldsymbol{e}}$. Then observe that

$$\begin{aligned}v^\top A^\top A w &= (Av)^\top (Aw) \\ &= \langle Tv, Tw \rangle \\ &= \langle v, w \rangle \\ &= v^\top w\end{aligned}$$

for all $v, w \in \mathbb{R}^2$. In particular, this implies $A^\top A = 1$, thus A is an orthogonal matrix. Generally speaking, an orthogonal matrix is a matrix whose inverse is its transpose. Suppose we represent T using a different basis. Then its matrix representation would have the form $C^{-1}AC$ for some $C \in \mathrm{GL}_n(\mathbb{R}^2)$. Now T is still an orthogonal transformation, but is $C^{-1}AC$ an orthogonal matrix still? The answer is no! Indeed, suppose that $C^{-1}AC$ is orthogonal. Then

$$\begin{aligned} 1 &= (C^{-1}AC)(C^{-1}AC)^\top \\ &= C^{-1}ACC^\top A^\top C^{\top -1}. \end{aligned}$$

Since A is orthogonal, this implies $CC^\top A = ACC^\top$. Therefore it is a necessary condition that $CC^\top \in \mathrm{Z}_{\mathrm{GL}_n}(A)$. In fact, this condition is also sufficient, however there are many cases where $CC^\top \notin \mathrm{Z}_{\mathrm{GL}_n}(A)$. For instance, consider $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $C = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then

$$\begin{aligned} CC^\top A - ACC^\top &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix} - \begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & -1 \\ -1 & -2 \end{pmatrix} \\ &\neq 0. \end{aligned}$$

34.2.1 Matrix Notation

Let $T\colon V \to W$ be a linear. A useful way to keep track of (111) for each i is to write it using matrix notation:

$$(T(\beta_1), \dots, T(\beta_m)) = (\gamma_1, \cdots, \gamma_n)[T]^\gamma_{\boldsymbol{\beta}}.$$

Using matrix notation, we obtain another proof of Proposition (34.4):

Proof. As matrix equations, we have

$$(\beta_1, \cdots, \beta_m)C = (\alpha_1, \dots, \alpha_m) \quad \text{and} \quad (\gamma_1, \cdots, \gamma_n)D = (\delta_1, \dots, \delta_n).$$

Thus, we have

$$\begin{aligned} (T(\beta_1), \dots, T(\beta_m)) &= (\gamma_1, \cdots, \gamma_n)[T]^\gamma_{\boldsymbol{\beta}} \\ (T(\beta_1), \dots, T(\beta_m))C \cdot C^{-1} &= (\gamma_1, \cdots, \gamma_n)D \cdot D^{-1}[T]^\gamma_{\boldsymbol{\beta}} \\ (T(\alpha_1), \dots, T(\alpha_m)) &= (\delta_1, \dots, \delta_n)D^{-1}[T]^\gamma_{\boldsymbol{\beta}}C, \end{aligned}$$

where $(T(\beta_1), \dots, T(\beta_m))C = (T(\alpha_1), \dots, T(\alpha_m))$ follows from linearity of T. It follows that

$$[T]^\delta_{\boldsymbol{\alpha}} = D^{-1}[T]^\gamma_{\boldsymbol{\beta}}C.$$

□

Example 34.2. Suppose V and W are 3-dimensional K-vector spaces with basis $\boldsymbol{\beta} = (\beta_1, \beta_2, \beta_3)$ for V and basis $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \gamma_3)$ for W. Suppose $T\colon V \to W$ is a linear transformation such that the matrix representation of T with respect to $\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ is

$$[T]^\gamma_{\boldsymbol{\beta}} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

So $T(\beta_1) = \gamma_1$, $T(\beta_2) = \gamma_1 + \gamma_3$, and $T(\beta_3) = \gamma_2$. We summarize in the table below how to convert this matrix into a diagonal matrix using elementary row and column operations. We also show what effect each operation has on the basis elements.

Basis for V	Basis for W	Matrix Representation
$(\beta_1, \beta_2, \beta_3)$	$(\gamma_1, \gamma_2, \gamma_3)$	$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$
$(\beta_1, \beta_2 - \beta_1, \beta_3)$	$(\gamma_1, \gamma_2, \gamma_3)$	$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} e_{12}(-1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$
$(\beta_1, \beta_2 - \beta_1 + \beta_3, \beta_3)$	$(\gamma_1, \gamma_2, \gamma_3)$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} e_{32}(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$
$(\beta_1, \beta_2 - \beta_1 + \beta_3, \beta_1 - \beta_2)$	$(\gamma_1, \gamma_2, \gamma_3)$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} e_{23}(-1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$
$(\beta_1, \beta_2 - \beta_1 + \beta_3, \beta_1 - \beta_2)$	$(\gamma_1, \gamma_2 + \gamma_3, \gamma_3)$	$e_{32}(-1) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

34.3 Linear Isomorphism from $\mathbf{Hom}_K(V, W)$ to $\mathbf{M}_{n\times m}(K)$

So far, we have shown how to obtain a column vector $[v]_\beta$ from an abstract vector v, and we have shown how to obtain a matrix $[T]_\beta^\gamma$ from an abstract linear map $T\colon V \to W$. We've also shown that the column represenation map $[\cdot]_\beta\colon V \to K^m$ is a *linear* map. This means, for example, that $[v_1 + v_2]_\beta = [v_1]_\beta + [v_2]_\beta$ for any two vectors $v_1, v_2 \in V$. Can we view the matrix representation map $[\cdot]_\beta^\gamma$ as a linear map? Indeed we can. To see how this works, we first need to describe the domain of $[\cdot]_\beta^\gamma$.

We denote by $\mathrm{Hom}_K(V, W)$ to be the set of all K-linear maps from V to W. We give $\mathrm{Hom}_K(V, W)$ the structure of a K-vector space as follows: If $T, U \in \mathrm{Hom}_K(V, W)$ and $a \in K$, then we define addition of T and U, denoted $T + U$, and scalar multiplication of a with T, denoted aT, by

$$(T + U)(v) = T(v) + U(v) \quad \text{and} \quad (aT)(v) = T(av)$$

for all $v \in V$.

Exercise 4. Check that the addition and scalar multiplication as defined above gives $\mathrm{Hom}_K(V, W)$ the structure of a K-vector space.

Exercise 5. For each $1 \leq i \leq m$ and $1 \leq j \leq n$, let $T_{ji}\colon V \to W$ be unique the linear map such that

$$T_{ji}(\beta_k) = \begin{cases} \gamma_j & \text{if } k = i \\ 0 & \text{if } k \neq i \end{cases}$$

for all $1 \leq k \leq m$. Check that the set $\{T_{ji} \mid 1 \leq i \leq m \text{ and } 1 \leq j \leq n\}$ is a basis for $\mathscr{L}(V, W)$.

Theorem 34.2. *Let V and W be K-vector spaces with basis $\beta = \{\beta_1, \dots, \beta_m\}$ for V and basis $\gamma = \{\gamma_1, \dots \gamma_n\}$ for W. Then we have an isomorphism of K-vector spaces*

$$[\cdot]_\beta^\gamma\colon Hom_K(V, W) \cong M_{n\times m}(K)$$

where the map $[\cdot]_\beta^\gamma$ is defined by

$$[\cdot]_\beta^\gamma(T) = [T]_\beta^\gamma$$

for all $T \in Hom_K(V, W)$.

Proof. We first show that the map $[\cdot]_\beta^\gamma$ is linear. Let $T, U \in \mathrm{Hom}_K(V, W)$ and let $a, b \in K$. Then it follows from Proposition (41.2) and Proposition (41.1) that

$$\begin{aligned} [aT + bU]_\beta^\gamma [v]_\beta &= [(aT + bU)(v)]_\gamma \\ &= [aT(v) + bU(v)]_\gamma \\ &= a[T(v)]_\gamma + b[U(v)]_\gamma \\ &= a[T]_\gamma [v]_\beta + b[U]_\gamma [v]_\beta. \end{aligned}$$

Therefore $[\cdot]_\beta^\gamma$ is a linear map. To see that $[\cdot]_\beta^\gamma$ is an isomorphism, note that $[T_{ji}]_\beta^\gamma = E_{ji}$, where E_{ji} is the matrix in K^n whose (j,i)-th entry is 1 and whose entry everywhere else is 0. Thus, $[\cdot]_\beta^\gamma$ restricts to a bijection on basis sets

$$[\cdot]_\beta^\gamma \colon \{T_{ji} \mid 1 \leq i \leq m \text{ and } 1 \leq j \leq n\} \to \{E_{ji} \mid 1 \leq i \leq m \text{ and } 1 \leq j \leq n\},$$

and so it must be an isomorphism. □

34.3.1 K-Algebra Isomorphism from $\mathrm{End}(V)$ to $\mathrm{M}_n(K)$

We write $\mathrm{End}_K(V)$ instead of $\mathrm{Hom}_K(V,V)$ to denote the set of all K-linear maps from V to itself. Simmilarly we write $\mathrm{M}_n(K)$ instead of $\mathrm{M}_{n\times n}(K)$ to denote the set of all $n \times n$ matrices. There is extra structure present in $\mathrm{End}_K(V)$ and $\mathrm{M}_n(K)$ that is not necessarily present in $\mathrm{Hom}_K(V,W)$ and $\mathrm{M}_{n\times m}(K)$; namely, $\mathrm{End}_K(V)$ and $\mathrm{M}_n(K)$ have K-algebra structures. Composition gives $\mathrm{End}_K(V)$ a K-algebra structure and matrix multiplication gives $\mathrm{M}_n(K)$ a K-algebra structure. It's reasonable to suspect that the matrix representation map $[\cdot]_\beta^\beta$ is a K-algebra isomorphism. In fact, this is indeed the case: Theorem (34.2) tells us that the matrix representation map $[\cdot]_\beta^\beta$ can be viewed as an isomorphism from $\mathrm{End}_K(V)$ to $\mathrm{M}_n(K)$ as K-vector spaces, and Theorem (34.1) tells us that the matrix representation map preserves the K-algebra structures (it takes composition to matrix multiplication). Combining these two theorems together tells us that the matrix representation map $[\cdot]_\beta^\beta$ can be viewed as an isomorphism from $\mathrm{End}_K(V)$ to $\mathrm{M}_n(K)$ as K-algebras.

34.4 Duality

Definition 34.4. The **dual** of V is defined to be the K-vector space

$$V^\star := \{\varphi \colon V \to K \mid \varphi \text{ is linear}\}.$$

where addition and scalar multiplication are defined by

$$(\varphi + \psi)(v) = \varphi(v) + \psi(v) \quad \text{and} \quad (\lambda\varphi)(v) = \varphi(\lambda v)$$

for all $\varphi, \psi \in V^\star$, $\lambda \in \mathbb{C}$, and $v \in V$. The **dual** of β is defined to be the basis of $V^\star$ given by $\beta^\star := \{\beta_1^\star, \dots, \beta_m^\star\}$, where each $\beta_i^\star$ is uniquely determined by

$$\beta_i^\star(\beta_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases}$$

Exercise 6. Check that $V^\star$ is indeed a K-vector space and that $\beta^\star$ is indeed a basis for $V^\star$.

Definition 34.5. Let $T \colon V \to W$ be a linear map. The **dual** of T is defined to be the map $T^\star \colon W^\star \to V^\star$ given by

$$T^\star(\varphi) = \varphi \circ T$$

for all $\varphi \in W^\star$.

Proposition 34.5. *The map $T^\star$ defined above is linear.*

Proof. Let $\varphi, \psi \in W^\star$ and let $a, b \in K$. Then

$$\begin{aligned} T^\star(a\varphi + b\psi)(v) &= (a\varphi + b\psi)(T(v)) \\ &= a\varphi(T(v)) + b\psi(T(v)) \\ &= aT^\star(\varphi)(v) + bT^\star(\psi)(v) \end{aligned}$$

for all $v \in V$. Thus $T^\star(a\varphi + b\psi)$ and $aT^\star(\varphi) + bT^\star(\psi)$ agree on all of V, and so they must be equal. □

Remark 48. An important remark here is that to determine whether two linear maps out of V are equal, we do *not* need to check that they agree on all of V as we did in the proof above. In fact, we just need to show that they agree on the basis β.

34.4.1 Matrix Representation of the Dual of a Linear Map

Proposition 34.6. *Let $T\colon V \to W$ be a linear map. Then*

$$[T^\star]_{\gamma^\star}^{\beta^\star} = ([T]_\beta^\gamma)^\top,$$

where $([T]_\beta^\gamma)^\top$ is the transpose of $[T]_\beta^\gamma$.

Proof. Suppose that

$$T(\beta_i) = \sum_{j=1}^n a_{ji}\gamma_j \tag{84}$$

for all $1 \le i \le m$. So a_{ji} lands in the jth row and ith column in $[T]_\beta^\gamma$ since we are summing over j in (84).

Let $1 \le j \le n$. We compute

$$\begin{aligned} T^\star(\gamma_j^\star)(\beta_i) &= \gamma_j^\star(T(\beta_i)) \\ &= \gamma_k^\star\left(\sum_{k=1}^n a_{ki}\gamma_k\right) \\ &= \sum_{j=1}^n a_{ki}\gamma_j^\star(\gamma_k) \\ &= a_{ki} \end{aligned}$$

for all $1 \le i \le m$. In particular, this implies

$$T^\star(\gamma_j^\star) = \sum_{i=1}^m a_{ji}\beta_i^\star \tag{85}$$

since both sides of (85) agree on β. So a_{ji} lands in the ith row and jth column in $[T^\star]_{\gamma^\star}^{\beta^\star}$ since we are summing over i in (85). Therefore the transpose of $[T]_\beta^\gamma$ is $[T^\star]_{\gamma^\star}^{\beta^\star}$. □

34.5 Bilinear Forms

Definition 34.6. A **bilinear form** on V is a function $B : V \times V \to K$ which satisfies the following properties

1. It is linear in the first variable when the second variable is fixed: for fixed $w \in V$, we have $B(av + a'v', w) = aB(v, w) + a'B(v', w)$ for all $a, a' \in K$ and $v, v' \in V$.
2. It is linear in the second variable when the first variable is fixed: for fixed $v \in V$, we have $B(v, bw + b'w') = bB(v, w) + b'B(v, w')$ for all $b, b' \in K$ and $w, w' \in V$.

Moreover, we say

- B is **symmetric** if $B(v, w) = B(w, v)$ for all $v, w \in V$,
- B is **skew-symmetric** if $B(v, w) = -B(w, v)$ for all $v, w \in V$,
- B is **alternating** if $B(v, v) = 0$ for all $v \in V$.

Let B be a bilinear form on V. Pick v and w in V and express them in the basis β:

$$v = \sum_{i=1}^m a_i\beta_i \quad \text{and} \quad w = \sum_{j=1}^m b_j\beta_j.$$

Then bilinearity of B gives us

$$\begin{aligned} B(v, w) &= B\left(\sum_{i=1}^m a_i\beta_i, \sum_{j=1}^m b_j\beta_j\right) \\ &= \sum_{1 \le i,j \le m} a_i b_j B(\beta_i, \beta_j) \\ &= \begin{pmatrix} a_1 & \cdots & a_m \end{pmatrix} \begin{pmatrix} B(\beta_1, \beta_1) & \cdots & B(\beta_1, \beta_m) \\ \vdots & \ddots & \vdots \\ B(\beta_m, \beta_1) & \cdots & B(\beta_m, \beta_m) \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \\ &= [v]_\beta^\top [B]_\beta [w]_\beta. \end{aligned}$$

where $\cdot$ denoted the dot product and $[B]_\beta = (B(\beta_i, \beta_j))$. We call $[B]_\beta$ the **matrix representation of B with respect to the basis β.**

Bilinear forms are not linear maps, but each bilinear form B on V can be interpreted as a linear map $V \to V^*$ in two ways, as L_B and R_B, where $L_B(v) = B(v, \cdot)$ and $R_B(v) = B(\cdot, v)$ for all $v \in V$.

Theorem 34.3. *Let B be a bilinear form on V and let $[B]_\beta = (a_{ij})$ be the matrix representation of B with respect to the basis β. Then*

$$M = [R_B]_\beta^{\beta^*}.$$

Proof. For each $1 \le i, j \le m$, we have

$$B(\beta_j, \beta_i) = a_{ji}.$$

Therefore

$$R_B(\beta_i) = B(\cdot, \beta_i) = \sum_{j=1}^m a_{ji}\beta_j^*$$

for all $1 \le i \le m$. It follows that

$$[R_B]_\beta^{\beta^*} = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} = [B]_\beta.$$

□

Remark 49. That the matrix associated to B is the matrix of R_B rather than L_B is related to our *convention* that we view bilinear forms concretely using $[v]_\beta^\top M[w]_\beta$ instead of $(M[v]_\beta)^\top [w]_\beta$. If we adopted the latter convention, then the matrix associated to B would equal the matrix for L_B.

Proposition 34.7. *Let α be another basis of V, let C be a change of basis matrix from β to α, and let B be a bilinear form on V. Then*

$$[B]_\alpha = C^\top [B]_\beta C.$$

Proof. We have

$$\begin{aligned} [B]_\alpha &= [R_B]_\alpha^{\alpha^*} \\ &= [1_{V^*} \circ R_B \circ 1_V]_\alpha^{\alpha^*} \\ &= [1_{V^*}]_{\beta^*}^{\alpha^*} [R_B]_\beta^{\beta^*} [1_V]_\alpha^\beta \\ &= C^\top [B]_\beta C. \end{aligned}$$

□

Definition 34.7. Two bilinear forms B_1 and B_2 on the respective vector spaces V_1 and V_2 are called **equivalent** if there is a vector space isomorphism $A : V_1 \to V_2$ such that

$$B_2(Av, Aw) = B_1(v, w)$$

for all v and w in V_1.

Although all matrix representations of a linear transformation $T\colon V \to V$ have the same determinant, the matrix representations of a bilinear form B on V have the same determinant only up to a nonzero square factor since $\det(C^\top MC) = \det(C)^2\det(M)$. This provides a sufficient (although far from necessary) condition to show two bilinear forms are inequivalent.

Example 34.3. Let d be a squarefree positive integer. On $\mathbb{Q}^2$, the bilinear form $B_d(v, w) = v^\top \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) w$ has a matrix with determinant d, so different (squarefree) d's give inequivalent bilinear forms on $\mathbb{Q}^2$. As bilinear forms on $\mathbb{R}^2$, however, these B_d's are equivalent. Indeed, we have $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) = C^\top I_2 C$ for $C = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \sqrt{d} \end{smallmatrix}\right)$. Another way of framing that is that, relative to coordinates in the basis $\{(1, 0), (0, 1/\sqrt{d})\}$ of $\mathbb{R}^2$, B_d looks like the dot product B_1.

35 Characteristic Polynomial of a Linear Map

Throughout this section, let K be a field, let V be a K-vector space with ordered basis $\boldsymbol{\beta} = \{\beta_1, \ldots, \beta_m\}$, and let $T\colon V \to V$ be a linear map.

35.1 Definition of the Characteristic Polynomial of a Linear Map

Recall that the matrix representation of T with respect to the ordered basis $\boldsymbol{\beta}$ is given by

$$[T]_{\beta}^{\beta} = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix}$$

where the entries a_{ji} are uniquely determined by the equations

$$T(\beta_i) = \sum_{j=1}^{m} a_{ji}\beta_j \tag{86}$$

for all $1 \leq i \leq m$. Note that this matrix representation of T *depends on a choice of an ordered basis*. Anytime you have a construction which depends on a particular choice of something, you should observe how your construction changes by making a different choice. With this in mind, let $\boldsymbol{\beta}' = \{\beta_1', \ldots, \beta_m'\}$ be another choice of an ordered basis of V. The matrix representation of T with respect to the ordered basis $\boldsymbol{\beta}'$ is related to the matrix representation of T with respect to the ordered basis β by the equation

$$[T]_{\beta'}^{\beta'} = [1_V]_{\beta}^{\beta'}[T]_{\beta}^{\beta}[1_V]_{\beta'}^{\beta}. \tag{87}$$

In other words, setting $U = [1_V]_{\beta}^{\beta'}$[2] (so U is invertible and $U^{-1} = [1_V]_{\beta'}^{\beta}$), setting $M = [T]_{\beta}^{\beta}$, and setting $M' = [T]_{\beta'}^{\beta'}$, we arrive at the less clunky form of (87)

$$M' = UMU^{-1}. \tag{88}$$

In other words, M is conjugate to M' by a matrix $U \in \mathrm{GL}_m(K)$. Matrices which are conjugate to each other satisfy similar properties. For example, applying determinants to both sides of (88) gives us

$$\begin{aligned} \det(M') &= \det(UMU^{-1}) \\ &= \det(U)\det(M)\det(U^{-1}) \\ &= \det(U)\det(U^{-1})\det(M) \\ &= \det(U)\det(U)^{-1}\det(M) \\ &= \det(M). \end{aligned}$$

Thus the determinant is invariant with respect conjugacy classes of matrices. In particular, we are justified in defining the **determinant** of T to be

$$\det(T) := \det[T]_{\beta}^{\beta}.$$

Again the reason why this definition makes sense is because it does not depend on a choice of an ordered basis. The determinant of T is sometimes called an **invariant** of T, because again, it's construction does not depend on a choice of an ordered basis. It turns out that there is a more general invariant of T which includes the determinant of T; it is called the **characteristic polynomial** of T.

Definition 35.1. The **characteristic polynomial** of T is defined to be the polynomial

$$\chi_T(X) := \det(X\mathrm{I}_m - [T]_{\beta}^{\beta}).$$

The definition of characteristic polynomial of T involved a choice of an ordered basis, thus we had better check that this definition is independent of our choice of an ordered basis. Let $\boldsymbol{\beta}' = \{\beta_1', \ldots, \beta_m'\}$ be another choice of an ordered basis of V and let $U = [1_V]_{\beta}^{\beta'}$ be the change of basis matrix from β to β'. Setting $M = [T]_{\beta}^{\beta}$ and $M' = [T]_{\beta'}^{\beta'}$, we see that

$$\begin{aligned} \det(X\mathrm{I}_m - M') &= \det(U(X\mathrm{I}_m - M')U^{-1}) \\ &= \det(X\mathrm{I}_m - UM'U^{-1}) \\ &= \det(X\mathrm{I}_m - M). \end{aligned}$$

Thus the definition of $\chi_T(X)$ is independent of the choice of basis.

[2] We call U the **change of basis matrix from the ordered basis β to the ordered basis β'**.

35.1.1 Eigenvalues

Definition 35.2. Let $\lambda \in K$. We say λ is an **eigenvalue** of T if there exists a nonzero vector $v \in V$ such that $Tv = \lambda v$. In this case we call v an **eigenvector** of T corresponding to the **eigenvalue** λ. We denote by E_λ to be the set of all eigenvectors of T corresponding to λ. Observe that $E_\lambda = \ker(T - \lambda)$. In particular, E_λ is a subspace of V. We call this subspace the **eigenspace** of T corresponding to the **eigenvalue** λ.

Remark 50. When context is clear, we often refer to λ, v, and E_λ as "an eigenvalue", "an eigenvector", and "an eigenspace" respectively.

Proposition 35.1. *Let λ be an eigenvalue of T. Then λ is also an eigenvalue of $[T]^{\beta}_{\beta}$.*

Proof. Choose an eigenvector v corresponding to the eigenvalue λ. Then

$$\begin{aligned} [T]^{\beta}_{\beta}[v]_{\beta} &= [Tv]_{\beta} \\ &= [\lambda v]_{\beta} \\ &= \lambda [v]_{\beta}. \end{aligned}$$

□

Proposition 35.2. *Let $\lambda \in K$. Then λ is an eigenvalue of T if and only if it is a root of the characteristic polynomial of T, that is, if and only if $\chi_T(\lambda) = 0$.*

Proof. Setting $M = [T]^{\beta}_{\beta}$, we have

$$\begin{aligned} \chi_T(\lambda) = 0 &\iff \det(\lambda - M) = 0 \\ &\iff \ker(\lambda - M) \neq 0 \\ &\iff \lambda - M \text{ is not injective.} \\ &\iff \text{there exists } \mathbf{v} \in K^n \backslash \{0\} \text{ such that } (\lambda - M)\mathbf{v} = 0. \\ &\iff \text{there exists } \mathbf{v} \in K^n \backslash \{0\} \text{ such that } M\mathbf{v} = \lambda \mathbf{v}. \\ &\iff \lambda \text{ is an eigenvalue of } M. \\ &\iff \lambda \text{ is an eigenvalue of } T. \end{aligned}$$

□

Example 35.1. Consider the matrices $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. A quick calculation shows

$$\chi_A(X) = (X-1)^2 = \chi_B(X).$$

Thus the only root of $\chi_A(X) = \chi_B(X)$ is when $X = 1$. Proposition (35.2) implies 1 is an eigenvalue for both A and B (in fact it is the only one). On the other hand, note that $\ker(1 - A) = 2$ and $\ker(1 - B) = 1$.

35.1.2 Eigenspaces

Definition 35.3. Let $T\colon V \to V$ be a linear map and let $\lambda \in K$. The **eigenspace of** λ is defined to be

$$E_\lambda := \ker(\lambda - T).$$

the dimension of E_λ is called the **geometric multiplicity of** λ and is denoted $\gamma_T(\lambda)$.

Remark 51. We often write $\lambda - T$ instead of $\lambda 1_V - T$ and we often write $\gamma(\lambda)$ instead of $\gamma_T(\lambda)$.

Proposition 35.3. *Let $T\colon V \to V$ be a linear map and let Λ denote the set of eigenvalues of T. Then the characteristic polynomial of T factors as*

$$\chi_T(X) = \prod_{\lambda \in \Lambda} (X - \lambda)^{\mu_T(\lambda)},$$

in a splitting field of K, where $\mu_T(\lambda) \in \mathbb{N}$ satisfy

$$\sum_{\lambda \in \Lambda} \mu_T(\lambda) = n.$$

*We call $\mu_T(\lambda)$ the **algebraic multiplicity of** λ.*

Remark 52. We often write $\mu(\lambda)$ instead of $\mu_T(\lambda)$.

35.1.3 Properties of Characteristic Polynomials

Proposition 35.4. *Let $T\colon V \to V$ be a linear map.*

1. *Let $a \in K\backslash\{0\}$. Then we have*
$$\chi_{aT}(X) = a^n \chi_T(a^{-1}X)$$
.

2. *Let $U\colon V \to V$ be another linear map. Then we have*
$$\chi_{UT}(X) = \chi_{TU}(X).$$

Proof. 1. We have

$$\begin{aligned}\chi_{aT}(X) &= \det(X - aT) \\ &= \det(a(a^{-1}X - T)) \\ &= a^n \det(a^{-1}X - T) \\ &= a^n \chi_T(a^{-1}X).\end{aligned}$$

2. We first consider the case where U is invertible. In this case, we have

$$\begin{aligned}\chi_{UT}(X) &= \det(X - UT) \\ &= \det(U^{-1}) \det(X - UT) \det(U) \\ &= \det(U^{-1}(X - UT)U) \\ &= \det(X - TU) \\ &= \chi_{TU}(X).\end{aligned}$$

For the more general case where both U and T are singular, we remark that the desired identity is an equality between polynomials in X and the coefficients of the matrices. Thus, to prove this equality, it suffices to prove that it is verified on a nonempty open subset of the space of all the coefficients. As the nonsingular matrices form such an open subset of the space of all matrices, this proves the result.

□

35.2 Generalized Eigenvectors

We give V the structure of a $K[X]$-module by defining

$$p(X) \cdot v = p(T)(v) \tag{89}$$

for all $p(X) \in K[X]$ and for all $v \in V$. Let us check that the action (89) does indeed give V the structure of a $K[X]$-module. Obviously V is an abelian group since it is a K-vector space. Also we have $1 \cdot v = v$ for all $v \in V$. Let $p(X), q(X) \in K[X]$ and let $v, w \in V$. Write $p(X) = \sum_{i=0}^{l} c_i X^i$ and $q(X) = \sum_{j=0}^{m} d_j X^j$. Then

$$\begin{aligned}(p(X) + q(X)) \cdot v &= (p(T) + q(T))(v) \\ &= \left(\sum_{i=0}^{l} c_i T^i + \sum_{j=0}^{m} d_j T^j \right)(v) \\ &= \sum_{i=0}^{l} c_i T^i(v) + \sum_{j=0}^{m} d_j T^j(v) \\ &= p(T)(v) + q(T)(v) \\ &= p(X) \cdot v + q(X) \cdot v\end{aligned}$$

and

$$\begin{aligned} p(X)\cdot(v+w) &= p(T)(v+w) \\ &= \sum_{i=0}^{l} c_i T^i(v+w) \\ &= \sum_{i=0}^{l} c_i (T^i(v)+T^i(w)) \\ &= \sum_{i=0}^{l} c_i T^i(v) + \sum_{i=0}^{l} c_i T^i(w) \\ &= p(T)(v)+p(T)(w) \\ &= p(X)\cdot v + p(X)\cdot w \end{aligned}$$

and

$$\begin{aligned} p(X)\cdot(q(X)\cdot v) &= p(X)\cdot(q(T)(v)) \\ &= p(X)\cdot \sum_{j=0}^{m} d_j T^j(v) \\ &= \sum_{j=0}^{m} d_j (p(X)\cdot T^j(v)) \\ &= \sum_{j=0}^{m} d_j p(T)(T^j(v)) \\ &= \sum_{j=0}^{m} d_j \left(\sum_{i=0}^{l} c_i T^i(T^j(v)) \right) \\ &= \sum_{j=0}^{m} d_j \sum_{i=0}^{l} c_i T^{i+j}(v) \\ &= \sum_{k=0}^{l+m} \left(\sum_{i=0}^{k} c_i d_{k-i} \right) T^k(v) \\ &= (p(X)q(X))\cdot v. \end{aligned}$$

Thus all of the required properties for V to be a $K[X]$-module under the action (89) are satisfied.

Proposition 35.5. *Let $p(X) \in K[X]$. Define*

$$\ker p(X) := \{v \in V \mid p(X)\cdot v = 0\}.$$

Then $\ker p(X)$ is a linear subspace of V. In particular, if $p(X) = X-\lambda$ where λ is an eigenvalue of T, then

$$ker(p(X)) = E_\lambda$$

where E_λ is the eigenspace corresponding to λ.

Proof. First note that $\ker(p(X))$ is nonzero since $0 \in \ker(p(X))$. Let $v,w \in \ker(p(X))$ and let $a,b \in K$. Write $p(X) = \sum_{i=0}^{l} c_i X^i$. Then

$$\begin{aligned} p(X)\cdot(av+bw) &= p(T)(av+bw) \\ &= \sum_{i=0}^{l} c_i T^i(av+bw) \\ &= \sum_{i=0}^{l} c_i (aT^i(v)+bf^i(w)) \\ &= a\sum_{i=0}^{l} c_i T^i(v) + b\sum_{i=0}^{l} c_i T^i(w) \\ &= a(p(X)\cdot v)+b(p(X)\cdot w) \\ &= 0+0 \\ &= 0. \end{aligned}$$

Thus $av + bw \in \ker(p(X))$. Therefore $\ker(p(X))$ is a linear subspace of V. In the case where $p(X) = X - \lambda$ for some eigenvalue λ of T, then we have

$$\begin{aligned} v \in \ker(p(X)) &\iff v \in \ker(X - \lambda) \\ &\iff (X - \lambda) \cdot v = 0 \\ &\iff (T - \lambda)(v) = 0 \\ &\iff T(v) = \lambda v. \end{aligned}$$

Thus $v \in \ker(p(X))$ if and only if v is an eigenvector of T with eigenvalue λ. Therefore $\ker(p(X)) = E_\lambda$. □

Proposition 35.6. *Let $p(X)$ and $q(X)$ be polynomials in $K[X]$ so that $\gcd(p(X), q(X)) = 1$. Then we have*

$$ker(p(X)q(X)) = ker(p(X)) + ker(q(X)), \tag{90}$$

where the sum (90) is direct.

Proof. Write $p(X) = \sum_{i=0}^{l} c_i X^i$ and $q(X) = \sum_{j=0}^{m} d_j X^j$. We first show that $\ker(p(X)) + \ker(q(X)) \subseteq \ker(p(X)q(X))$. Let $v \in \ker(p(X)) + \ker(q(X))$. Write $v = v_1 + v_2$ where $v_1 \in \ker(p(X))$ and $v_2 \in \ker(q(X))$. Then

$$\begin{aligned} (p(X)q(X)) \cdot v &= p(X) \cdot (q(X) \cdot v) \\ &= p(X) \cdot (q(X) \cdot (v_1 + v_2)) \\ &= p(X) \cdot (q(X) \cdot v_1 + q(X) \cdot v_2) \\ &= p(X) \cdot (q(X) \cdot v_1) \\ &= (p(X)q(X)) \cdot v_1 \\ &= (q(X)p(X)) \cdot v_1 \\ &= q(X) \cdot (p(X) \cdot v_1) \\ &= q(X) \cdot 0 \\ &= 0. \end{aligned}$$

This implies $v \in \ker(p(X)q(X))$. Thus $\ker(p(X)) + \ker(q(X)) \subseteq \ker(p(X)q(X))$.

Now we show $\ker(p(X)q(X)) \subseteq \ker(p(X)) + \ker(q(X))$. Choose $a(X), b(X) \in K[X]$ so that

$$a(X)p(X) + b(X)q(X) = 1. \tag{91}$$

Such a choice is possible since $\gcd(p(X), q(X)) = 1$. Let $v \in \ker(p(X)q(X))$. Using (91), write $v = v_1 + v_2$ where

$$v_1 = (b(X)q(X)) \cdot v \quad \text{and} \quad v_2 = (a(X)p(X)) \cdot v.$$

Then $v_2 \in \ker(q(X))$ since

$$\begin{aligned} q(X) \cdot v_2 &= q(X) \cdot ((a(X)p(X)) \cdot v) \\ &= (q(X)a(X)p(X)) \cdot v \\ &= (a(X)p(X)q(X)) \cdot v \\ &= a(X) \cdot (p(X)q(X) \cdot v) \\ &= a(X) \cdot 0 \\ &= 0. \end{aligned}$$

Similarly, $v_1 \in \ker(p(X))$ since

$$\begin{aligned} p(X) \cdot v_1 &= p(X) \cdot ((b(X)q(X)) \cdot v) \\ &= (p(X)b(X)q(X)) \cdot v \\ &= (b(X)p(X)q(X)) \cdot v \\ &= b(X) \cdot (p(X)q(X) \cdot v) \\ &= b(X) \cdot 0 \\ &= 0. \end{aligned}$$

Therefore $v \in \ker(p(X)) + \ker(q(X))$, and this implies $\ker(p(X)q(X)) \subseteq \ker(p(X)) + \ker(q(X))$.

To see that (90) is a direct sum, let $v \in \ker(p(X)) \cap \ker(q(X))$. Then

$$\begin{aligned} v &= 1 \cdot v \\ &= (a(X)p(X) + b(X)q(X)) \cdot v \\ &= (a(X)p(X)) \cdot v + (b(X)q(X)) \cdot v \\ &= a(X) \cdot (p(X) \cdot v) + b(X) \cdot (q(X) \cdot v) \\ &= a(X) \cdot 0 + b(X) \cdot 0 \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Thus $\ker(p(X)) \cap \ker(q(X)) = 0$ and so the sum (90) is direct. □

Proposition 35.7. *Let $c(X) \in K[X]$ be any nonzero polynomial such that $c(T) = 0$. Suppose*

$$c(X) = p_1(X)p_2(X) \cdots p_m(X)$$

where each $p_i(X) \in K[X]$ and $\gcd(p_i(X), p_j(X)) = 1$ for all pairs $1 \leq i < j \leq m$. Then

$$V = \mathit{ker}(p_1(X)) + \mathit{ker}(p_2(X)) + \cdots + \mathit{ker}(p_m(X)), \tag{92}$$

where the sum (92) is direct.

Proof. We first prove by induction on $m \geq 2$ that for polynomials $p_i(X) \in K[X]$ such that $\gcd(p_i(X), p_j(X)) = 1$ for all $1 \leq i < j \leq m$, we have

$$\ker(p_1(X)p_2(X) \cdots p_m(X)) = \ker(p_1(X)) \oplus \ker(p_2(X)) \oplus \cdots \oplus \ker(p_m(X)), \tag{93}$$

where we use $\oplus$ to denote that the sum is direct. The base case $m = 2$ was established in Proposition (35.6). Now assume (93) is true for some $m \geq 2$. Let $p_i(X) \in K[X]$ such that $\gcd(p_i(X), p_j(X)) = 1$ for all $1 \leq i < j \leq m+1$. Since $\gcd(p_1(X), p_i(X)) = 1$ for all $2 \leq i \leq m+1$, we have $\gcd(p_1(X), p_2(X) \cdots p_{m+1}(X)) = 1$. Therefore

$$\begin{aligned} \ker(p_1(X)p_2(X) \cdots p_{m+1}(X)) &= \ker(p_1(X)) \oplus \ker(p_2(X) \cdots p_{m+1}(X)) \\ &= \ker(p_1(X)) \oplus \ker(p_2(X)) \oplus \cdots \oplus \ker(p_{m+1}(X)), \end{aligned}$$

where we used the base case on the first line and where we used the induction hypothesis to get from the first line to the second line.

To finish the problem, we just need to show that $V = \ker(c(X))$. Let $v \in V$. Then

$$\begin{aligned} c(X) \cdot v &= c(f)(v) \\ &= 0(v) \\ &= 0 \end{aligned}$$

implies $v \in \ker(c(X))$. Therefore $V \subseteq \ker(c(X))$, which implies $V = \ker(c(X))$. □

Lemma 35.1. *Let $W_1, \dots, W_t$ be subspaces of a vector space V. For each $1 \leq i \leq t$, let*

$$\mathcal{B}_i := \{u_{ij} \mid 1 \leq j \leq m_i\}$$

be a basis for W_i where $m_i := \dim W_i$. Assume that

$$W := W_1 + \cdots + W_t$$

is a direct sum. Then $\mathcal{B} := \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_t$ is a basis for W.

Proof. It suffices to show that $\mathcal{B}$ is a linearly independent set since $\operatorname{span}(\mathcal{B}) = W$ is clear. Suppose

$$\sum_{i=1}^{t} \sum_{j=1}^{m_i} a_{ij} u_{ij} = 0. \tag{94}$$

for some $a_{ij} \in K$ where $1 \leq i \leq t$ and $1 \leq j \leq m_i$. Then for each $1 \leq i \leq t$, we must have $\sum_{j=1}^{m_i} a_{ij} u_{ij} = 0$. Indeed, if $\sum_{j=1}^{m_k} a_{kj} u_{kj} \neq 0$ for some $1 \leq k \leq t$, then we can rearrange (94) to get

$$\sum_{j=1}^{m_k} a_{kj} u_{kj} = - \sum_{\substack{1 \leq i \leq t \\ i \neq k}} \sum_{j=1}^{m_i} a_{ij} u_{ij},$$

and so

$$\begin{aligned}0 &\neq \sum_{j=1}^{m_k} a_{kj}u_{kj}\\ &\in W_k \cap \sum_{\substack{1\le i\le t\\ i\neq k}} W_i\\ &= \{0\},\end{aligned}$$

gives us our desired contradiction. Thus, for each $1 \le i \le t$, we have

$$\sum_{j=1}^{m_i} a_{ij}u_{ij} = 0.$$

But this implies $a_{ij} = 0$ for all $1 \le j \le m_i$ since $\mathcal{B}_i$ is a basis for all $1 \le i \le t$. Thus $a_{ij} = 0$ for all $1 \le i \le t$ and $1 \le j \le m_i$, and hence $\mathcal{B}$ is linearly independent. □

35.3 Jordan Canonical Form

Theorem 35.2. *Assume K is algebraically closed. Let $T\colon V \to V$ be a linear map and let Λ denote the set of all eigenvalues of T. Then*

$$V = \bigoplus_{\substack{1\le j\le \mu(\lambda)\\ \lambda\in\Lambda}} E_{\lambda,j}^{r(j)}$$

35.3.1 Constructing a Basis for $\ker \varphi^m$

Construction: Assume K is algebraically closed. Let $T\colon V \to V$ be a linear map. Suppose the characteristic polynomial of T factors as

$$\chi_T(X) = (X-\lambda)^n.$$

Denote $\varphi := T - \lambda$. We want to construct a basis for $\ker\varphi^n = V$. Before doing so, we first make the following observation. For each $1 \le i \le n$, we have the short exact sequence

$$0 \to \ker \varphi^{i-1} \hookrightarrow \ker \varphi^i \to \ker \varphi^i/\ker \varphi^{i-1} \to 0. \tag{95}$$

It follows from (95) that

$$\begin{aligned}\sum_{i=1}^{n} \dim(\ker \varphi^i/\ker \varphi^{i-1}) &= \sum_{i=1}^{n} \dim(\ker \varphi^i) - \dim(\ker \varphi^{i-1})\\ &= \dim(\ker \varphi^n) - \dim(\ker \varphi^0)\\ &= n.\end{aligned} \tag{96}$$

Now we proceed to construct a basis for $\ker \varphi^n$ as follows: Let

$$m_1 := \max\{i \mid \dim(\ker\varphi^i/\ker\varphi^{i-1}) > 0\}.$$

Note that $1 \le m_1 \le n$. Indeed, we have $1 \le m_1$ since the dimension of the eigenspace E_λ is nonzero and we have $m_1 \le n$ since the characteristic polynomial kills V. If $m_1 = 1$, then

$$\begin{aligned}\dim E_\lambda &= \dim(\ker\varphi)\\ &= \sum_{i=1}^{n} \dim(\ker\varphi^i/\ker\varphi^{i-1})\\ &= n,\end{aligned}$$

by the dimension formula (96) above. In this case, T is diagonalizable, and we can find a basis of V consisting of eigenvectors. Thus assume $1 < m_1 \le n$. Let $\{\overline{v}_1^{m_1}, \dots, \overline{v}_{k_1}^{m_1}\}$[3] be a basis of $\ker \varphi^m/\ker \varphi^{m-1}$. It follows from linear independence of $\{\overline{v}_1^{m_1}, \dots, \overline{v}_{k_1}^{m_1}\}$ that if

$$a_1\overline{v}_1^{m_1} + \cdots + a_{k_1}\overline{v}_{k_1}^{m_1} = 0 \tag{97}$$

[3]When we write $\overline{v}_j^m$, it is understood that $v_j^m \in \ker \varphi^m$ is a representative of the coset $\overline{v}_j^m \in \ker \varphi^m/\ker \varphi^{m-1}$. Note that if $\{\overline{v}_1^m, \dots, \overline{v}_k^m\}$ is a linearly independent set $\ker \varphi^m/\ker \varphi^{m-1}$, then $\{v_1^m, \dots, v_k^m\}$ is a linearly independent set in $\ker \varphi^m$ since it is in the preimage of a linear map.

for some $a_1, \dots, a_{k_1} \in K$, then we must have $a_1 = \cdots = a_{k_1} = 0$. In other words, if

$$a_1 v_1^{m_1} + \cdots + a_{k_1} v_{k_1}^{m_1} \in \ker(\varphi^{m_1-1})$$

for some $a_1, \dots, a_{k_1} \in K$, then we must have $a_1 = \cdots = a_{k_1} = 0$. In other words, if

$$a_1 \varphi^{m_1-1}(v_1^{m_1}) + \cdots + a_{k_1} \varphi^{m_1-1}(v_{k_1}^{m_1}) = 0$$

for some $a_1, \dots, a_{k_1} \in K$, then we must have $a_1 = \cdots = a_{k_1} = 0$. Thus, $\{\varphi^{m_1-1}(v_1^{m_1}), \dots, \varphi^{m_1-1}(v_{k_1}^{m_1})\}$ is a linearly independent set in $\ker(\varphi)$. In fact, $\{\varphi^{m_1-i}(v_1^{m_1}), \dots, \varphi^{m_1-i}(v_{k_1}^{m_1})\}$ is a linearly independent set in $\ker(\varphi^i)$ for all $0 \le i < m_1$ since $\{\varphi^{m_1-i}(v_1^{m_1}), \dots, \varphi^{m_1-i}(v_{k_1}^{m_1})\}$ is in the preimage of $\{\varphi^{m_1-1}(v_1^{m_1}), \dots, \varphi^{m_1-1}(v_{k_1}^{m_1})\}$ under the map $\varphi^{i-1} \colon \ker(\varphi^i) \to \ker(\varphi)$. Moreover, $\{\varphi^{m_1-i}(\overline{v}_1^{m_1}), \dots, \varphi^{m_1-i}(\overline{v}_{k_1}^{m_1})\}$ is a linearly independent set in $\ker(\varphi^i)/\ker(\varphi^{i-1})$ all $1 \le i < m_1$. Indeed, if

$$a_1 \varphi^{m_1-i}(v_1^{m_1}) + \cdots + a_{k_1} \varphi^{m_1-i}(v_{k_1}^{m_1}) \in \ker(\varphi^{i-1})$$

for some $a_1, \dots, a_{k_1}$, then

$$\begin{aligned} a_1 \varphi^{m_1-1}(v_1^{m_1}) + \cdots + a_{k_1} \varphi^{m_1-1}(v_{k_1}^{m_1}) &= a_1 \varphi^{i-1}(\varphi^{m_1-i}(v_1^{m_1})) + \cdots + a_{k_1} \varphi^{i-1}(\varphi^{m_1-i}(v_{k_1}^{m_1})) \\ &= \varphi^{i-1}(a_1 \varphi^{m_1-i}(v_1^{m_1}) + \cdots + a_{k_1} \varphi^{m_1-i}(v_{k_1}^{m_1})) \\ &= 0 \end{aligned}$$

which implies $a_1 = \cdots = a_{k_1} = 0$. Since $\{\varphi^{m_1-i}(\overline{v}_1^{m_1}), \dots, \varphi^{m_1-i}(\overline{v}_{k_1}^{m_1})\}$ is a linearly independent set in $\ker(\varphi^i)/\ker(\varphi^{i-1})$ we have the following inequality

$$\dim(\ker(\varphi^i)/\ker(\varphi^{i-1})) \ge \dim(\ker(\varphi^{m_1})/\ker(\varphi^{m_1-1})). \tag{98}$$

for all $1 \le i \le m_1$.

If the inequality (98) is an equality for all $1 \le i < m_1$, then we must have $m_1 = n$ and

$$\dim(\ker(\varphi^i)/\ker(\varphi^{i-1})) = 1$$

by dimension formula (96) and the inequality (98). In this case, $\{v_1^n, \varphi(v_1^n), \dots, \varphi^n(v_1^n)\}$ gives us a basis for V and we are done. Otherwise, let

$$m_2 := \max\{i \mid \dim(\ker(\varphi^i)/\ker(\varphi^{i-1})) > \dim(\ker(\varphi^{m_1})/\ker(\varphi^{m_1-1}))\}.$$

Note that $1 \le m_2 < m_1$. Extend $\{\varphi^{m_1-m_2}(\overline{v}_1^{m_1}), \dots, \varphi^{m_1-m_2}(\overline{v}_{k_1}^{m_1})\}$ to a basis of $\ker(\varphi^{m_2})/\ker(\varphi^{m_2-1})$, say

$$\{\varphi^{m_1-m_2}(\overline{v}_1^{m_1}), \dots, \varphi^{m_1-m_2}(\overline{v}_{k_1}^{m_1}), \overline{v}_1^{m_2}, \dots, \overline{v}_{k_2}^{m_2}\}. \tag{99}$$

If $m_2 = 1$, then (99) gives us our desired basis. Otherwise, by the same arguments as above, the set

$$\{\varphi^{m_1-m_2-i}(\overline{v}_1^{m_1}), \dots, \varphi^{m_1-m_2-i}(\overline{v}_{k_1}^{m_1}), \varphi^{m_2-i}(\overline{v}_1^{m_2}), \dots, \varphi^{m_2-i}(\overline{v}_{k_2}^{m_2})\}$$

is a linearly independent set in $\ker(\varphi^i)/\ker(\varphi^{i-1})$ for all $1 \le i < m_2$. Hence we have the following inequality

$$\dim(\ker(\varphi^i)/\ker(\varphi^{i-1})) \ge \dim(\ker(\varphi^{m_2})/\ker(\varphi^{m_2-1}))$$

for all $1 \le i \le m_2$.

At some point this process must terminate, say at m_t for some $t > 1$. Thus we obtain a decreasing sequence

$$n > m_1 > m_2 > \cdots > m_t \ge 1,$$

$$m_2 := \max\{i \mid \dim(\ker(\varphi^i)/\ker(\varphi^{i-1})) > \dim(\ker(\varphi^{m_1})/\ker(\varphi^{m_1-1}))\}.$$

Note that $1 \le m_2 < m_1$.
First note that for each $1 \le i \le n$, we have the short exact sequence

$$0 \to \ker(\varphi^{i-1}) \hookrightarrow \ker(\varphi^i) \to \ker(\varphi^i)/\ker(\varphi^{i-1}) \to 0 \tag{100}$$

It follows from (100) that

$$\begin{aligned}\sum_{i=1}^{n} \dim(\ker(\varphi^i)/\ker(\varphi^{i-1})) &= \sum_{i=1}^{n} \dim(\ker(\varphi^i)) - \dim(\ker(\varphi^{i-1})) \\ &= \dim(\ker(\varphi^n)) - \dim(\ker(\varphi^0)) \\ &= n.\end{aligned}$$

For each $0 \leq i < m$, we will lift a basis of $\ker(\varphi^{i+1})/\ker(\varphi^i)$ to a linearly independent set in $\ker(\varphi^{i+1})$. Then we will show that the union of all of these linearly independent subsets forms a basis of $\ker(\varphi^m)$.
The final basis will be

$$\bigcup_{s=1}^{t} \{\varphi^{m_s - i}(v_j^{m_s}) \mid 1 \leq i \leq k_s \text{ and } 1 \leq j \leq m_s\}$$

Example 35.2. Let $A\colon K^{10} \to K^{10}$ be given by the matrix

$$A := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

In this case, we have $m_1 = 4$, $m_2 = 2$, $m_3 = 1$, and $k_1 = 1$, $k_2 = 2$, $k_3 = 2$. Note that

$$m_1 k_1 + m_2 k_2 + m_3 k_3 = \mu(1),$$

where $\mu(1) = 10$ is the algebraic multiplicity of the eigenvalue 1. We also note that

$$k_1 + k_2 + k_3 = \gamma(1),$$

where $\gamma(1) = 5$ is the geometric multiplicity of the eigenvalue 1, i.e. the dimension of the eigenspace E_1. The generalized eigenvectors are given by

$$\begin{aligned} v_1^4 &= e_4 \\ \varphi(v_1^4) &= e_3 \\ \varphi^2(v_1^4) &= e_2 \\ \varphi^3(v_1^4) &= e_1 \\ v_1^2 &= e_6 \\ \varphi(v_1^2) &= e_5 \\ v_2^2 &= e_8 \\ \varphi(v_2^2) &= e_7 \\ v_1^1 &= e_9 \\ v_2^1 &= e_{10} \end{aligned}$$

Using our notation as above, we can line up the generalized eigenvectors like so:

$$\begin{array}{ccccccc} \ker(\varphi^4)/\ker(\varphi^3): & v_1^4 & & & & \\ & | & & & & \\ \ker(\varphi^3)/\ker(\varphi^2): & \varphi(v_1^4) & & & & \\ & | & & & & \\ \ker(\varphi^2)/\ker(\varphi): & \varphi^2(v_1^4) & v_1^2 & v_2^2 & & \\ & | & | & | & & \\ \ker(\varphi): & \varphi^3(v_1^4) & \varphi(v_1^2) & \varphi(v_2^2) & v_1^1 & v_2^1 \end{array}$$

Now assume that $m_1 = n$. Then it follows from the dimension formula (96) and the inequality (98) that

$$\dim(\ker(\varphi^i)/\ker(\varphi^{i-1})) = 1$$

for all $1 \leq i \leq n$. In this case, $\{v_1^n, \varphi(v_1^n), \ldots, \varphi^n(v_1^n)\}$ gives us a basis for V and we are done. So assume $1 < m_1 < n$. Let

$$m_2 := \max\{i \mid \dim(\ker(\varphi^i)/\ker(\varphi^{i-1})) > \dim(\ker(\varphi^{m_1})/\ker(\varphi^{m_1 - 1}))\}.$$

Note that $1 \leq m_2 < m_1$.

35.4 Invariant Subspaces

Proposition 35.8. *Let $\Psi\colon V_1 \to V_2$ be an isomorphism from the vector space V_1 to the vector space V_2 and let $T\colon V_1 \to V_1$ be a linear map. Then the T-invariant subspaces of V_1 are in one-to-one correspondence with the $(\Psi \circ T \circ \Psi^{-1})$-invariant subspaces of V_2.*

Proof. Let $\mathrm{Inv}_T(V_1)$ denote the set of T-invariant subspaces of V_1 and let $\mathrm{Inv}_{\Psi\circ T\circ\Psi^{-1}}(V_2)$ denote the set of $(\Psi \circ T \circ \Psi^{-1})$-invariant subspaces of V_2. The isomorphism $\Psi\colon V_1 \to V_2$ induces a bijection $\Psi\colon \mathrm{Inv}_T(V_1) \to \mathrm{Inv}_{\Psi\circ T\circ\Psi^{-1}}(V_2)$ given by $W_1 \mapsto \Psi(W_1)$. Observe that this map lands in the target space. Indeed, if $W_1 \in \mathrm{Inv}_T(V_1)$, then

$$\begin{aligned}(\Psi \circ T \circ \Psi^{-1})(\Psi(W_1)) &= (\Psi \circ T)(\Psi \circ \Psi^{-1})(W_1)\\ &= (\Psi \circ T)(W_1)\\ &= \Psi(T(W_1))\\ &\subset \Psi(W_1).\end{aligned}$$

The inverse map is given by $\Psi^{-1}\colon \mathrm{Inv}_{\Psi\circ T\circ\Psi^{-1}}(V_2) \to \mathrm{Inv}_T(V_1)$. □

Proposition 35.9. *Let $V = V_1 \oplus \cdots \oplus V_n$ be a direct sum of vectors spaces $V_1, \dots, V_n$. Let $T\colon V \to V$ be given by $T = \oplus_i T_i$ where $T_i\colon V_i \to V_i$ are linear maps for each $1 \le i \le n$. Then the T-invariant subspaces of V consist of subspaces of the form*

$$W = W_1 \oplus \cdots \oplus W_n \tag{101}$$

where W_i is a T_i-invariant subspace for each $1 \le i \le n$.

Proof. Let $W = W_1 \oplus \cdots \oplus W_n$ be a subspace of V such that W_i is T_i-invariant for all $1 \le i \le n$. Let $w \in W$ and write $w = w_1 + \cdots + w_n$ where $w_i \in W_i$ for all $1 \le i \le n$. Then

$$\begin{aligned}T(w) &= T(w_1 + \cdots + w_n)\\ &= T(w_1) + \cdots + T(w_n)\\ &= T_1(w_1) + \cdots + T_n(w_n)\\ &\in W_1 \oplus \cdots \oplus W_n\\ &= W.\end{aligned}$$

Thus W is T-invariant. Conversely, let $W = W_1 \oplus \cdots \oplus W_n$ be any T-invariant subspace of V. Then for any $1 \le i \le n$ and for any $w \in W_i$, we have

$$\begin{aligned}T_i(w) &= T(w)\\ &\subseteq W.\end{aligned}$$

Since $\mathrm{im}(T_i) \subseteq V_i$, this implies $T_i(w) \in W \cap V_i = W_i$. Thus W_i is T_i-invariant for all $1 \le i \le n$. □

36 Minimal Polynomial of a Linear Map

The easiest matrices to compute with are the diagonal ones. The sum and product of diagonal matrices can be computed componentwise along the main diagonal, and taking powers of a diagonal matrix is simple too. All the complications of matrix operations are gone when working only with diagonal matrices. If a matrix A is not diagonal but can be conjugated to a diagonal matrix, say $D := PAP^{-1}$ is diagonal, then $A = P^{-1}DP$ so $A^k = P^{-1}D^kP$ for all integers k, which reduces us to computations with a diagonal matrix. In many applications of linear algebra (e.g., dynamical systems, differential equations, Markov chains, recursive sequences) powers of a matrix are crucial to understanding the situation, so the relevance of knowing when we can conjugate a nondiagonal matrix into a diagonal matrix is clear.

We want look at the coordinate-free formulation of the idea of a diagonal matrix, which will be called a diagonalizable operator. There is a special polynomial, the minimal polynomial (generally not equal to the characteristic polynomial), which will tell us exactly when a linear operator is diagonalizable. The minimal polynomial will also gives us information about nilpotent operators.

All linear operators under discussion are understood to be acting on nonzero finite-dimensional vector spaces over a given field F.

36.1 Diagonalizable Operators

Definition 36.1. We say the linear operator $A\colon V \to V$ is **diagonalizable** when it admits a diagonal matrix representation with respect to some basis of V: there is a basis $\mathcal{B}$ of V such that the matrix $[A]_{\mathcal{B}}$ is diagonal.

Let's translate diagonalizability into the language of eigenvectors rather than matrices.

Theorem 36.1. *The linear operator $A\colon V \to V$ is diagonalizable if and only if there is a basis of eigenvectors for A in V.*

Proof. Suppose there is a basis $\mathcal{B} = \{e_1, \dots, e_n\}$ of V in which $[A]_\beta$ is diagonal:

$$[A]_\beta = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & a_n \end{pmatrix}.$$

Then $Ae_i = a_i e_i$ for all i, so each e_i is an eigenvector for A. Conversely, if V has a basis $\{v_1, \dots, v_n\}$ of eigenvectors of A, with $Av_i = \lambda_i v_i$ for $\lambda_i \in F$, then in this basis the matrix representation of A is $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$. $\square$

36.2 The Minimal Polynomial

By the Cayley-Hamilton Theorem, there is a nonzero monic polynomial that kills a linear operator A: its characteristic polynomial.

Definition 36.2. The nonzero monic polynomial in $F[T]$ that kills A and has least degree is called the **minimal** polynomial of A in $F[T]$.

What this means for a matrix $A \in \mathrm{M}_n(F)$, viewed as an operator on F^n, is that its minimal polynomial is the polynomial $f(T)$ of least degree such that $f(A)$ is the zero matrix.

Example 36.1. Both $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ have the same characteristic polynomial $(T-1)^2$, but $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has minimal polynomial $T-1$ while $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has minimal polynomial $(T-1)^2$. No linear polynomial can kill $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ since that would imply $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is a scalar diagonal matrix.

Theorem 36.2. *The minimal polynomial of a linear operator $A : V \to V$ is equal to that of any matrix representation for it.*

Proof. Picking a basis of V lets us identify $\mathrm{Hom}_F(V, V)$ and $M_n(F)$ as F-algebras. If M is the matrix in $M_n(F)$ corresponding to A under this isomorphism, then for any $f(T) \in F[T]$, the matrix representaiton of $f(A)$ is $f(M)$. Therefore $f(A) = O$ if and only if $f(M) = O$. Using f of least degree in either equation shows A and M have the same minimal polynomial in $F[T]$. $\square$

We will usually denote the minimal polynomial of A as $m_A(T)$.

Theorem 36.3. *Let $A : V \to V$ be linear. A polynomial $f(T) \in F[T]$ satisfies $f(A) = O$ if and only if $m_A(T) \mid f(T)$.*

Proof. Suppose $m_A(T) \mid f(T)$, so $f(T) = m_A(T)g(T)$. Since substitution of A for T gives a homomorphism $F[T] \to \mathrm{Hom}_F(V, V)$, we have $f(A) = m_A(A)g(A) = O \cdot g(A) = O$.

Conversely, suppose $f(A) = O$. Using polynomial division in $F[T]$, write $f(T) = m_A(T)q(T) + r(T)$ where $q(T), r(T) \in F[T]$ and $r(T) = 0$ or $\deg r < \deg m_A$. Substituting A for T in the polynomials, we have

$$O = m_A(A)q(A) + r(A) = r(A).$$

Since $r(T)$ vanishes at A and either $r(T) = 0$ or $r(T)$ has degree less than the degree of the minimal polynomial of A, it must be the case that $r(T) = 0$. Therefore $f(T) = m_A(T)q(T)$, so $m_A(T) \mid f(T)$. $\square$

Theorem (36.3) justifies speaking of *the* minimal polynomial. If two monic polynomials are both of least degree killing A, then Theorem (36.3) shows that they divide each other, and therefore they are equal (since they are both monic). Minimal polynomials of linear operators need not be irreducible (e.g., $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has minimal polynomial $(T-1)^2$).

Example 36.2. Write V as a direct sum of subspaces, say $V = U \oplus W$. Let $P : V \to V$ be the projection onto the subspace U from this particular decomposition: $P(u + w) = u$. Since $P(u) = u$, we have $P^2(u + w) = P(u + w)$, so $P^2 = P$. Thus P is killed by the polynomials $T^2 - T = T(T - 1)$. If $T^2 - T$ is not the minimal polynomial, then by Theorem (36.3), either T or $T - 1$ kills P; the first case means $P = O$ (so $U = \{0\}$) and the second case means $P = \mathrm{id}_V$ (so $U = V$). As long as U and W are both nonzero, P is neither O nor id_V and $T^2 - T$ is the minimal polynomial of the projection P.

Theorem 36.4. *Any eigenvalue of a linear operator is a root of its minimal polynomial in $F[T]$, so the minimal polynomial and characteristic polynomial have the same roots.*

Proof. The minimal polynomial of a linear operator and any of its matrix representations are the same, so we pick a basis to work with a matrix A acting on F^n. Say λ is an eigenvalue of A, in some extension field E. We want to show $m_A(\lambda) = 0$. There is an eigenvector in E^n for this eigenvalue: $Av = \lambda v$ and $v \neq 0$. Then $A^k v = \lambda^k v$ for all $k \geq 1$, so $f(A)v = f(\lambda)v$ for all $f \in E[T]$. In particular, taking $f(T) = m_A(T)$, $m_A(A) = O$ so $0 = m_A(\lambda)v$. Thus $m_A(\lambda) = 0$. □

We say a polynomial in $F[T]$ **splits** if it is a product of linear factors in $F[T]$. For instance, $T^2 - 5$ splits in $\mathbb{R}[T]$, but not in $\mathbb{Q}[T]$. Using the minimal polynomial in place of the characteristic polynomial provides a good criterion for diagonalizability over any field, which is our main result:

Theorem 36.5. *Let $A : V \to V$ be a linear operator. Then A is diagonalizable if and only if its minimal polynomial in $F[T]$ splits in $F[T]$ and has distinct roots.*

Proof. Suppose $m_A(T)$ splits in $F[T]$ with distinct roots. We will show V has a basis of eigenvectors for A, so A is diagonalizable. Let

$$m_A(T) = (T - \lambda_1) \cdots (T - \lambda_r),$$

so the $\lambda_i's$ are the eigenvalues of A and by hypothesis they are distinct.

For any eigenvalue λ_i, let

$$E_{\lambda_i} = \{v \in V \mid Av = \lambda_i v\}$$

be the corresponding eigenspace. We will show

$$V = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_r},$$

so using bases from E_{λ_i} provides an eigenbasis for A. Since eigenvectors with different eigenvalues are linearly independent, it suffices to show

$$V = E_{\lambda_1} + \cdots + E_{\lambda_r},$$

as the sum will then automatically be direct by linear independence.

The way to get the eigenspace components of a vector is to show that it is possible to "project" from V to each eigenspace E_{λ_i} using *polynomials* in the operator A. Specifically, we want to find polynomials $h_1(T), \ldots, h_r(T)$ in $F[T]$ such that

$$1 = h_1(T) + \cdots + h_r(T), \qquad h_i(T) \equiv 0 \bmod m_A(T)/(T - \lambda_i).$$

The congruence condition implies the polynomial $(T - \lambda_i)h_i(T)$ is divisible by $m_A(T)$, so $(A - \lambda_i)h_i(A)$ acts on V as O. □

37 Bilinear Spaces

Definition 37.1. Let V be a vector space over a field K. A **bilinear form** on V is a function $B \colon V \times V \to K$ which satisfies the following properties

1. It is linear in the first variable when the second variable is fixed: for fixed $w \in V$, we have $B(av + a'v', w) = aB(v, w) + a'B(v', w)$ for all $a, a' \in K$ and $v, v' \in V$.

2. It is linear in the second variable when the first variable is fixed: for fixed $v \in V$, we have $B(v, bw + b'w') = bB(v, w) + b'B(v, w')$ for all $b, b' \in K$ and $w, w' \in V$.

Moreover, we say

- B is **symmetric** if $B(v, w) = B(w, v)$ for all $v, w \in V$,
- B is **skew-symmetric** if $B(v, w) = -B(w, v)$ for all $v, w \in V$,
- B is **alternating** if $B(v, v) = 0$ for all $v \in V$.

We call the pair (V, B) a **bilinear space**.

Theorem 37.1. *In all characteristics, an alternating bilinear form is skew-symmetric. In characteristic not* 2*, a bilinear form is skew-symmetric if and only if it is alternating. In characteristic* 2*, a bilinear form is skew-symmetric if and only if it is symmetric.*

Proof. Let B be a bilinear form on V. Assume that B is alternating. Then

$$\begin{aligned}0 &= B(v+w, v+w) \\ &= B(v,v) + B(v,w) + B(w,v) + B(w,w) \\ &= B(v,w) + B(w,v)\end{aligned}$$

implies $B(v,w) = -B(w,v)$ for all $v, w \in V$. Thus B is skew-symmetric.

Now assume that the characteristic of K is $\neq 2$ and that B is skew-symmetric. Then

$$\begin{aligned}B(v,v) &= -B(v,v) \\ &\implies 2B(v,v) = 0 \\ &\implies B(v,v) = 0\end{aligned}$$

for all $v \in V$. Thus B is alternating.

That skew-symmetric and symmetric bilinear forms coincide in characteristic 2 is immediate since $1 = -1$ in characteristic 2. $\square$

Let B be a bilinear form on V. Pick v and w in V and express them in the basis β:

$$v = \sum_{i=1}^{m} a_i \beta_i \quad \text{and} \quad w = \sum_{j=1}^{m} b_j \beta_j.$$

Then bilinearity of B gives us

$$\begin{aligned}B(v,w) &= B\left(\sum_{i=1}^{m} a_i\beta_i, \sum_{j=1}^{m} b_j\beta_j\right) \\ &= \sum_{1 \le i,j \le m} a_i b_j B(\beta_i, \beta_j) \\ &= \begin{pmatrix} a_1 & \cdots & a_m \end{pmatrix} \begin{pmatrix} B(\beta_1,\beta_1) & \cdots & B(\beta_1,\beta_m) \\ \vdots & \ddots & \vdots \\ B(\beta_m,\beta_1) & \cdots & B(\beta_m,\beta_m) \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \\ &= [v]_\beta^\top [B]_\beta [w]_\beta.\end{aligned}$$

where $\cdot$ denoted the dot product and $[B]_\beta = (B(\beta_i, \beta_j))$. We call $[B]_\beta$ the **matrix representation of** B **with respect to the basis** β.

Bilinear forms are not linear maps, but each bilinear form B on V can be interpreted as a linear map $V \to V^*$ in two ways, as L_B and R_B, where $L_B(v) = B(v, \cdot)$ and $R_B(v) = B(\cdot, v)$ for all $v \in V$.

Theorem 37.2. *Let B be a bilinear form on V and let $[B]_\beta = (a_{ij})$ be the matrix representation of B with respect to the basis β. Then*

$$M = [R_B]_\beta^{\beta^*}.$$

Proof. For each $1 \le i, j \le m$, we have

$$B(\beta_j, \beta_i) = a_{ji}.$$

Therefore

$$R_B(\beta_i) = B(\cdot, \beta_i) = \sum_{j=1}^{m} a_{ji}\beta_j^*$$

for all $1 \le i \le m$. It follows that

$$[R_B]_\beta^{\beta^*} = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} = [B]_\beta.$$

$\square$

Remark 53. That the matrix associated to B is the matrix of R_B rather than L_B is related to our *convention* that we view bilinear forms concretely using $[v]_\beta^\top M[w]_\beta$ instead of $(M[v]_\beta)^\top[w]_\beta$. If we adopted the latter convention, then the matrix associated to B would equal the matrix for L_B.

Proposition 37.1. *Let α be another basis of V, let C be a change of basis matrix from β to α, and let B be a bilinear form on V. Then*

$$[B]_\alpha = C^\top[B]_\beta C.$$

Proof. We have

$$\begin{aligned}
[B]_\alpha &= [R_B]_\alpha^{\alpha^*} \\
&= [1_{V^*} \circ R_B \circ 1_V]_\alpha^{\alpha^*} \\
&= [1_{V^*}]_{\beta^*}^{\alpha^*}[R_B]_\beta^{\beta^*}[1_V]_\alpha^\beta \\
&= C^\top[B]_\beta C.
\end{aligned}$$

□

Definition 37.2. Two bilinear forms B_1 and B_2 on the respective vector spaces V_1 and V_2 are called **equivalent** if there is a vector space isomorphism $A : V_1 \to V_2$ such that

$$B_2(Av, Aw) = B_1(v, w)$$

for all v and w in V_1.

Although all matrix representations of a linear transformation $T\colon V \to V$ have the same determinant, the matrix representations of a bilinear form B on V have the same determinant only up to a nonzero square factor since $\det(C^\top MC) = \det(C)^2\det(M)$. This provides a sufficient (although far from necessary) condition to show two bilinear forms are inequivalent.

Example 37.1. Let d be a squarefree positive integer. On $\mathbb{Q}^2$, the bilinear form $B_d(v,w) = v^\top \left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right) w$ has a matrix with determinant d, so different (squarefree) d's give inequivalent bilinear forms on $\mathbb{Q}^2$. As bilinear forms on $\mathbb{R}^2$, however, these B_d's are equivalent. Indeed, we have $\left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right) = C^\top I_2 C$ for $C = \left(\begin{smallmatrix}1&0\\0&\sqrt{d}\end{smallmatrix}\right)$. Another way of framing that is that, relative to coordinates in the basis $\{(1,0),(0,1/\sqrt{d})\}$ of $\mathbb{R}^2$, B_d looks like the dot product B_1.

37.1 Bilinear Forms and Matrices

A linear transformation $L : V \to W$ between two finite-dimensional vector spaces over F can be written as a matrix once we pick (ordered) bases for V and W. When $V = W$ and we use the same basis for the inputs and outputs of L then changing the basis leads to a new matrix representation that is conjugate to the old matrix. In particular, the trace, determinant, and (more generally) characteristic polynomial of a linear operator $L : V \to V$ are well-defined, independent of the choice of basis. In this section we will see how bilinear forms can be described using matrices.

Let V have finite dimension with basis $\{e_1, \ldots, e_n\}$. Pick v and w in V and express them in this basis: $v = \sum_{i=1}^n x_i e_i$ and $w = \sum_{j=1}^n y_j e_j$. For any bilinear form B on V, its bilinearity gives

$$\begin{aligned}
B(v,w) &= B\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_i\right) \\
&= \sum_{i=1}^n x_i B\left(e_i, \sum_{j=1}^n y_j e_j\right) \\
&= \sum_{i=1}^n \sum_{j=1}^n x_i y_j B(e_i, e_j).
\end{aligned}$$

Set $M = (B(e_i, e_j))$, which is an $n \times n$ matrix. By a direct calculation, we have

$$B(v,w) = [v] \cdot M[w] \tag{102}$$

for all v and w in V, where $\cdot$ on the right is the usual dot product on F^n and

$$[v] = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad [w] = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

are the coordinate vectors of v and w for our choice of basis $\{e_1, \ldots, e_n\}$. The "coordinate" isomorphism $[\cdot] : V \to F^n$ will be understood to refer to a fixed choice of basis throughout a given discussion. We call the matrix $M = (B(e_i, e_j))$ the **matrix associated to** B in the basis $\{e_1, \ldots, e_n\}$. " isomorphism with respect to this basis. These two coordinate systems are related by a change of basis matrix $U \in \mathrm{GL}_n(F)$: $U[v] = [v]'$ for all $v \in V$.

Theorem 37.3. *Let V be a vector space of F of finite dimension $n \geq 1$. For a fixed choice of basis $\{e_1, \ldots, e_n\}$ of V, which gives an isomorphism $v \mapsto [v]$ from V to F^n by coordinatization, each bilinear form on V has the expression (102) for a unique $n \times n$ matrix M over F and each $n \times n$ matrix M over F defines a bilinear form on V by (102).*

Proof. We already showed each bilinear form looks like (102) once we choose a basis. It's easy to see for each M that (102) is a bilinear form on V. It remains to verify uniqueness. If $B(v, w) = [v] \cdot N[w]$ for a matrix N, then $B(e_i, e_j) = [e_i] \cdot N[e_j]$, which is tthe (i, j) entry of N, so $N = (B(e_i, e_j))$. □

Example 37.2. Let $V = \mathbb{R}^n$. Pick nonnegative integers p and q such that $p + q = n$. For $v = (x_1, \ldots, x_n)$ and $v' = (x'_1, \ldots, x'_n)$ in $\mathbb{R}^n$, set

$$\begin{aligned}\langle v, v' \rangle_{p,q} &:= x_1 x'_1 + \cdots + x_p x'_p - x_{p+1} x'_{p+1} - \cdots - x_n x'_n \\ &= v \cdot \begin{pmatrix} I_p & 0 \\ 0 & -I_1 \end{pmatrix} v'.\end{aligned}$$

This symmetric bilinear form is like the dot product, except the coefficients involve p plus signs and $n - p = q$ minus signs. The dot product on $\mathbb{R}^n$ is the special case $(p, q) = (n, 0)$.

The space $\mathbb{R}^n$ with bilinear form $\langle \cdot, \cdot \rangle_{p,q}$ is denoted $\mathbb{R}^{p,q}$. We call $\mathbb{R}^{p,q}$ a **pseudo-Euclidean space** when p and q are both positive. The example $\mathbb{R}^{1,3}$ or $\mathbb{R}^{3,1}$ is called **Minkowski space** and arises in relativity theory. A pseudo-Euclidean space is the same vector space as $\mathbb{R}^n$, but its geometric structure (e.g., the notion of perpendicularity) is different. The label **Euclidean space** is actually not just another name for $\mathbb{R}^n$ as a vector space, but it is the name for $\mathbb{R}^n$ equipped with a specific bilinear form: the dot product.

Bilinear forms are not linear maps, but each bilinear form B on V can be interpreted as a linear map $V \to V^\vee$ in two ways, as L_B and R_B, where $L_B(v) = B(v, \cdot)$ and $R_B(v) = B(\cdot, v)$ for all $v \in V$.

Theorem 37.4. *If B is a bilinear form on V, then the matrix for B in the basis $\{e_1, \ldots, e_n\}$ of V equals the matrix of the linear map $R_B : V \to V^\vee$ with respect to the given basis of V and its dual basis in $V^\vee$.*

Proof. Let $[\cdot] : V \to F^n$ be the coordinate isomorphism coming from the basis in the theorem and let $[\cdot]' : V^\vee \to F^n$ be the coorinate isomorphism using the dual basis. The matrix for R_B has columns $[R_B(e_1)]', \ldots, [R_B(e_n)]'$. To compute the entries of the jth column, we simply have to figure out how to write $R_B(e_j)$ as a linear combination of the dual basis $\{e_1^\vee, \ldots, e_n^\vee\}$ of $V^\vee$ and use the coefficients that occur.

There is one expression for $R_B(e_j)$ in the dual basis:

$$R_B(e_j) = c_1 e_1^\vee + \cdots + c_n e_n^\vee$$

in $V^\vee$, with unknown c_i's. To find c_i we just evaluate both sides at e_i: the left side is $(R_B(e_j))(e_i) = (B(\cdot, e_j))(e_i) = B(e_i, e_j)$ and the right side is $c_i \cdot 1 = c_i$. Therefore the ith entry of the column vector $[R_B(e_j)]'$ is $B(e_i, e_j)$, which means the matrix for R_B is the matrix $(B(e_i, e_j))$; they agree column-by-column. □

Remark 54. That the matrix associated to B is the matrix of R_B rather than L_B is related to our *convention* that we view bilinear forms concretely using $[v] \cdot A[w]$ instead of $A[v] \cdot [w]$. If we adopted the latter convention, then the matrix associated to B would equal the matrix for L_B.

37.1.1 Change of Basis Matrix

When a linear transformation $L : V \to V$ has matrix M in some basis, and C is the change-of-basis matrix expressing a new basis in terms of the old basis, then the matrix for L in the new basis is $C^{-1}MC$. Let us recall how this works.

The change-of-basis matrix C, whose columns express the coordinates of the second basis in terms of the first basis, satisfies

$$[v]_1 = C[v]_2$$

for all $v \in V$, where $[\cdot]_i$ is the coordinate isomorphism of V with F^n using the ith basis. Indeed, both sides are linear in v, so it suffices to check this identity when v runs through the second basis, which recovers the definition of C by its columns. Since $[Lv]_1 = M[v]_1$ for all $v \in V$,

$$\begin{aligned}[Lv]_2 &= C^{-1}[Lv]_1 \\ &= C^{-1}M[v]_1 \\ &= C^{-1}MC[v]_2,\end{aligned}$$

so we've proved the matrix for L in the second basis is $C^{-1}MC$.

Theorem 37.5. *Let C be a change-of-basis matrix on V. A bilinear form on V with matrix M in the first basis has matrix $C^\top MC$ in the second basis.*

Proof. Let B be the bilinear form in the theorem. Then

$$\begin{aligned} B(v,w) &= [v]_1 \cdot M[w]_1 \\ &= C[v]_2 \cdot MC[w]_2 \\ &= [v]_2 \cdot C^\top MC[w]_2, \end{aligned}$$

so the matrix for B in the second basis is $C^\top MC$. □

Definition 37.3. Two bilinear forms B_1 and B_2 on the respective vector spaces V_1 and V_2 are called **equivalent** if there is a vector space isomorphism $A : V_1 \to V_2$ such that

$$B_2(Av, Aw) = B_1(v,w)$$

for all v and w in V_1.

Theorem 37.6. *Let bilinear forms B_1 and B_2 on V_1 and V_2 have respective matrix representations M_1 and M_2 in two bases. Then B_1 is equivalent to B_2 if and only if $M_1 = C^\top M_2 C$ for some invertible matrix C.*

Proof. The equivalence of B_1 and B_2 means there is an isomorphism $A : V_1 \to V_2$ such that $A^\vee R_{B_2} A = R_{B_1}$. Using the bases on V_i ($i = 1,2$) in which B_i is represented by M_i and the dual bases on $V_i^\vee$, this equation is equivalent to $C^\top M_2 C = M_1$, where C represents A. (Invertibility of C is equivalent to A being an isomorphism.) □

Although all matrix representations of a linear transformation $V \to V$ have the same determinant, the matrix representations of a bilinear form on V have the same determinant only up to a nonzero square factor: $\det(C^\top MC) = \det(C)^2 \det(M)$. Since equivalent bilinear forms can be represented by the same matrix using a suitable bases, the determinants of any matrix representation for two equivalent bilinear forms must differ by a nonzero square factor. This provides a sufficient (although far from necessary) condition to show two bilinear forms are inequivalent.

Example 37.3. Let d be a squarefree positive integer. On $\mathbb{Q}^2$, the bilinear form $B_d(v,w) = v \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) w$ has a matrix with determinant d, so different (squarefree) d's give inequivalent bilinear forms on $\mathbb{Q}^2$. As bilinear forms on $\mathbb{R}^2$, however, these B_d's are equivalent: $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) = C^\top I_2 C$ for $C = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{d} \end{pmatrix}$. Another way of putting that is that, relative to coordinates in the basis $\{(1,0), (0, 1/\sqrt{d})\}$ of $\mathbb{R}^2$, B_d looks like the dot product B_1.

37.2 Nondegenerate Bilinear Forms

Theorem 37.7. *Let (V,B) be a bilinear space. The following conditions are equivalent:*

1. *for some basis $\{e_1, \ldots, e_n\}$ of V, the matrix $(B(e_i, e_j))$ is invertible,*
2. *if $B(v,v') = 0$ for all $v' \in V$ then $v = 0$, or equivalently ifv $\neq 0$ then $B(v,v') \neq 0$ for some $v' \in V$,*
3. *every element of $V^\vee$ has the form $B(v,\cdot)$ for some $v \in V$,*
4. *every element of $V^\vee$ has the form $B(v,\cdot)$ for a unique $v \in V$.*

When this occurs, every matrix representation for B is invertible.

Proof. The matrix $(B(e_i,e_j))$ is a matrix representation of the linear map $R_B : V \to V^\vee$. So the first condition says R_B is an isomorphism. The functions $B(v,\cdot)$ in $V^\vee$ are the values of $L_B : V \to V^\vee$, so the second condition says $L_B : V \to V^\vee$ is injective. The third condition says L_B is surjective and the fourth condition says L_B is an isomorphism. Since L_B is a linear map between vector spaces of the same dimension, injectivity, surjectivity, and isomorphy are equivalent properties. So the second, third, and fourth conditions are equivalent. Since L_B and R_B are dual to each other, the first and fourth condition are equivalent.

Different matrix representations M and M' of a bilinear form are related by $M' = C^\top MC$ for some invertible matrix C, so if one matrix representation is invertible then so are the others. □

38 Quadratic Forms

Let V be a vector space over a field F. A **quadratic form** on V is a map $Q : V \to F$ which satisfies the following two properties:

1. $Q(cv) = c^2 Q(v)$ for all $v \in V$ and $c \in F$,

2. The symmetric pairing $\beta_Q : V \times V \to F$ defined by

$$\beta_Q(v, w) := Q(v + w) - Q(v) - Q(w)$$

   for all $v, w \in V$ is bilinear.

A **quadratic space** over F is a pair (V, Q) consisting of a vector space V over F and a quadratic form Q on V. One way to think of β_Q is that it measures the failure of Q to being additive. In particular, we have

$$Q(v + w) = Q(v) + Q(v) + \beta_Q(v, w)$$

for all $v, w \in V$.

Note that $\beta_Q(v, v) = Q(2v) - 2Q(v) = 2Q(v)$, so as long as $2 \neq 0$ in F we can run the procedure in reverse: for any symmetric bilinear mapping $B : V \times V \to F$, the map $Q_B : V \to F$, defined by

$$Q_B(v) := B(v, v)$$

for all $v \in V$ is a quadratic form on V and the two operations $Q \mapsto B_Q = \beta_Q/2$ and $B \mapsto Q_B$ are inverse bijections between quadratic forms on V and symmetric bilinear forms on V. Over general fields, one cannot recover Q from β_Q (for example $q(x) = x^2$ and $Q(x) = 0$ on $V = F$ have $\beta_q = 0 = \beta_Q$ when $2 = 0$ in F, yet $q \neq 0$). When $2 \neq 0$ in F, we say that Q is **non-degenerate** exactly when the associated symmetric bilinear pairing $B_Q = \beta_Q/2 : V \times V \to F$ is perfect (that is, the associated self-dual linear map $V \to V^\vee$ defined by $v \mapsto B_Q(v, \cdot) = B_Q(\cdot, v)$ is an isomorphism, or more concretely the "matrix" of B_Q with respect to a basis of V is invertible). In other cases (with $2 \neq 0$ in F) we say Q is **degenerate**.

38.1 Expressing quadratic forms with respect to a basis

If $\dim V = n$ is finite and positive, and we choose a basis $\{e_1, \ldots, e_n\}$ of V, then for $v = \sum x_i e_i$ we have

$$\begin{aligned}
Q(v) &= Q\left(\sum_{i<n} x_i e_i + x_n e_n\right) \\
&= Q\left(\sum_{i<n} x_i e_i\right) + Q(x_n e_n) + \beta_Q\left(\sum_{i<n} x_i e_i, x_n e_n\right) \\
&= Q\left(\sum_{i<n} x_i e_i\right) + x_n^2 Q(e_n) + \sum_{i<n} x_i x_n \beta_Q(e_i, e_n) \\
&= Q\left(\sum_{i<n} x_i e_i\right) + c_{nn} x_n^2 + \sum_{i<n} c_{in} x_i x_n
\end{aligned}$$

with $c_{in} = \beta_Q(e_i, e_n) \in F$ and $c_{nn} = Q(e_n) \in F$. Hence, inducting on the number of terms in the sum readily gives

$$Q\left(\sum_i x_i e_i\right) = \sum_{i \leq j} c_{ij} x_i x_j = \sum_{i<j} \beta_Q(e_i, e_j) x_i x_j + \sum_i Q(e_i) x_i^2.$$

with $c_{ij} \in F$, and conversely any such formula is readily checked to define a quadratic form. Note also that the c_{ij}'s are uniquely determined by Q (and the choice of basis).

Example 38.1. Suppose $2 \neq 0$ in F anddim $V = 2$. After choosing a basis of V, say $\{e_1, e_2\}$ with dual basis $\{x_1, x_2\}$, we can write

$$\begin{aligned}
Q(v) &= Q(e_1) x_1(v)^2 + (Q(e_1 + e_2) - Q(e_1) - Q(e_2)) x_1(v) x_2(v) + Q(e_2) x_2(v)^2 \\
&= \frac{1}{2} \beta_Q(e_1, e_1) x_1(v)^2 + \beta_Q(e_1, e_2) x_1(v) x_2(v) + \frac{1}{2} \beta_Q(e_2, e_2) x_2(v)^2.
\end{aligned}$$

Example 38.2. Suppose $\dim V = 2$ and $F = \mathbb{R}$. Let $\mathbf{e} = \{e_1, e_2\}$ be an ordered basis of V. Then for $v = x_1e_1 + x_2e_2$, we have

$$Q(v) = Q(e_1){x_1}^2 + (Q(e_1+e_2) - Q(e_1) - Q(e_2))x_1x_2 + Q(e_2){x_2}^2. \tag{103}$$

Suppose that $Q(e_1) = 1$, $Q(e_2) = -1$, and $Q(e_1 + e_2) = Q(e_1) + Q(e_2)$. Then we can simplify (103) to

$$Q(v) = Q(x_1e_1 + x_2e_2) = x_1^2 - x_2^2.$$

Now consider the ordered basis $\mathbf{e}' = \{e_1', e_2'\}$ of V where $e_1' = 2e_1 + e_2$ and $e_2' = e_1 + 2e_2$. Then the change-of-basis matrix from $\mathbf{e}$ to $\mathbf{e}'$ is $C := \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. Let us express v in terms of this new basis:

$$\begin{aligned}
v &= x_1e_1 + x_2e_2 \\
&= \begin{pmatrix} e_1 & e_2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\
&= \begin{pmatrix} e_1 & e_2 \end{pmatrix} CC^{-1} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\
&= \begin{pmatrix} e_1' & e_2' \end{pmatrix} \begin{pmatrix} \frac{2}{3}x_1 - \frac{1}{3}x_2 \\ \frac{-1}{3}x_1 + \frac{2}{3}x_2 \end{pmatrix} \\
&= \left(\frac{2}{3}x_1 - \frac{1}{3}x_2\right) e_1' + \left(\frac{-1}{3}x_1 + \frac{2}{3}x_2\right) e_2' \\
&= x_1'e_1' + x_2'e_2',
\end{aligned}$$

where $x_1' = \frac{2}{3}x_1 - \frac{1}{3}x_2$ and $x_2' = \frac{-1}{3}x_1 + \frac{2}{3}x_2$. Therefore,

$$Q(v) = Q(e_1')x_1'^2 + (Q(e_1' + e_2') - Q(e_1') - Q(e_2'))x_1'x_2' + Q(e_2')x_2'^2. \tag{104}$$

By a direct calculation, we have $Q(e_1') = 3$, $Q(e_2') = -3$, and $Q(e_1' + e_2') - Q(e_1') - Q(e_2') = 0$. Thus, (103) simplifies to

$$Q(v) = Q(x_1'e_1' + x_2'e_2') = 3x_1'^2 - 3x_2'^2.$$

So we get a different polynomial representation for Q, depending on our choice of basis.

Example 38.3. Suppose $2 \neq 0$ in F, so we have seen that there is a bijective correspondence between symmetric bilinear forms on V and quadratic forms on V; this bijective is even linear with respect to the evident linear structures on the sets of symmetric bilinear forms on V and quadratic forms on V (using pointwise operations; $(a_1B_1 + a_2B_2)(v, v') = a_1B_1(v, v') + a_2B_2(v, v')$, which one checks is symmetric bilinear, and $(a_1Q_1 + a_2Q_2)(v) = a_1Q_1(v) + a_2Q_2(v)$ which is checked to be a quadratic form). Let us make this bijection concrete, as follows. Fix an ordered basis $\mathbf{e} = \{e_1, \ldots, e_n\}$ of V. Then we can describe a symmetric bilinear $B : V \times V \to F$ in terms of the matrix $[B] =_{\mathbf{e}^\vee} [\varphi_\ell]_{\mathbf{e}} = (b_{ij})$ for the "left/right-pairing" map $\varphi_\ell = \varphi_r$ from V to $V^\vee$ defined by $v \mapsto B(v, \cdot) = B(\cdot, v)$, namely $b_{ij} = B(e_j, e_i) = B(e_i, e_j)$. However, in terms of the dual linear coordinates $\{x_i = e_i^*\}$ we have just seen that we can uniquely write $Q_B : V \to F$ as $Q_B(v) = \sum_{i \leq j} c_{ij}x_i(v)x_j(v)$. What is the relationship between the c_{ij}'s and the b_{ij}'s? We simply compute: for $v = \sum x_ie_i$, bilinearity of B implies $Q_B(v) = B(v, v)$ is given by

$$\sum x_ix_jB(e_i, e_j) = \sum_i B(e_i, e_i)x_i^2 + \sum_{i<j} \left(B(e_i, e_j) + B(e_j, e_i)\right) x_ix_j = \sum_i b_{ii}x_i^2 + \sum_{i<j} 2b_{ij}x_ix_j,$$

where $b_{ij} = B(e_j, e_i) = B(e_i, e_j) = b_{ji}$. Hence $c_{ii} = b_{ii}$, but for $i < j$ we have $c_{ij} = 2b_{ij} = b_{ij} + b_{ji}$.

Thus, for B and Q that correspond to each other, given the polynomial $[Q]$ for Q with respect to a choice of basis of V, we "read off" the symmetrix matrix $[B]$ describing B (in the same linear coordinate system) as follows: the ii-diagonal entry of $[B]$ is the coefficient of the square term x_i^2 in Q, and the "off-diagonal" matrix entry b_{ij} for $i \neq j$ is given by *half* the coefficient for $x_ix_j = x_jx_i$ appearing in $[Q]$. For example, if $Q(x, y, z) = x^2 + 7y^2 - 3z^2 + 4xy + 3xz - 5yz$, then the corresponding symmetric bilinear form B is computed via the symmetric matrix

$$[B] = \begin{pmatrix} 1 & 2 & 3/2 \\ 2 & 7 & -5/2 \\ 3/2 & -5/2 & -3 \end{pmatrix}.$$

Going in the other direction, if someone hands us a *symmetric matrix* $[B] = (b_{ij})$, then we "add across the main diagonal" to compute that the corresponding homogeneous quadratic polynomial $[Q]$ is $\sum_i b_{ii}x_i^2 + \sum_{i<j}(b_{ij} + b_{ji})x_ix_j = \sum_i b_{ii}x_i^2 + \sum_{i<j} 2b_{ij}x_ix_j$.

38.2 Diagonalizing Quadratic Forms

It is an elementary algebraic fact (to be proved in a moment) for any field F in which $2 \neq 0$ that, relative to some basis $\mathbf{e} = \{e_1, \ldots, e_n\}$ of V, we can express Q in the form $Q = \sum \lambda_i x_i^2$ for some scalars $\lambda_1, \ldots, \lambda_n$ (some of which may vanish). In other words, we can "diagonalize" Q, or rather the "matrix" of B_Q (and so the property that some λ_i vanishes is equivalent to the intrinsic property that Q is degenerate). To see why this is, we note that Q is uniquely determined by B_Q (as $1+1 \neq 0$ in F) and in terms of B_Q this says that the basis consists of vectors $\{e_1, \ldots, e_n\}$ that are mutually perpendicular with respect to B_Q (i.e. $B_Q(e_i, e_j) = 0$ for all $i \neq j$). Thus, we can restate the assertion as the general claim that if $B : V \times V \to F$ is a symmetric bilinear pairing, then there exists a basis $\{e_i\}$ of V such that $B(e_i, e_j) = 0$ for all $i \neq j$. To prove this we may induct on $\dim V$, the case $\dim V = 1$ being clear. In general, suppose $n = \dim V > 1$. Choose a nonzero $e_n \in V$ and let

$$W := \operatorname{Ker}\left(R_B(e_n)\right) = \left\{v \in V \mid B_Q(v, e_n) = 0\right\}.$$

Since the target space for $R_B(e_n)$ is $\mathbb{R}$, we see that either $\dim W = n$ or $\dim W = n-1$. In either case, we can choose a subspace W' of W such that $\dim W' = n-1$. Now use induction for B restricted to $W' \times W'$ to find a suitable $e_1, \ldots, e_{n-1}$ that, together with e_n, solve the problem.

Example 38.4. Let $f \colon \mathbb{R}^2 \to \mathbb{R}$ be defined by

$$f(\boldsymbol{x}) = 3x_1^2 + 3x_2^2 - 2x_1x_2 + 2x_1 - 6x_2.$$

The Hessian of f at a point $\boldsymbol{a} \in \mathbb{R}^2$ is a symmetric bilinear form whose matrix representation is given by

$$\mathrm{H}_f(\boldsymbol{a}) = \begin{pmatrix} 6 & -2 \\ -2 & 6 \end{pmatrix}.$$

Let Q be the associated quadratic form. Then

$$Q = 6x_1^2 - 4x_1x_2 + 6x_2^2.$$

If we set $x_1 = x_1'$ and $x_2 = x_2'/3 + x_2'$, then in the new coordinates, we have

$$Q = \frac{16}{3}x_1'^2 + \frac{18}{3}x_2'^2$$

38.3 Some Generalities Over $\mathbb{R}$

Now assume that $F = \mathbb{R}$. Since all positive elements of $\mathbb{R}$ are squares, after passing to a basis of V that "diagonalizes" Q (which, as we have seen, is a purely algebraic fact), we can rescale the basis vectors using $e_i' = e_i/\sqrt{|\lambda_i|}$ when $\lambda_i \neq 0$ to get (upon reordering the basis)

$$Q = x_1'^2 + \cdots + x_r'^2 - x_{r+1}'^2 - \cdots - x_{r+s}'^2$$

for some $r, s \geq 0$ with $r + s \leq \dim V$. Let $t = \dim V - r - s \geq 0$ denote the number of "missing variables" in such a diagonalization (so $t = 0$ if and only if Q is non-degenerate). The value of r here is just the number of λ_i's which were positive, s is the number λ_i's which were negative, and t is the number of λ_i's which vanish.

To shed some light on the situation, we introduce some terminology that is specific to the case of the field $\mathbb{R}$. The quadratic form Q is **positive-definite** if $Q(v) > 0$ for all $v \in V \backslash \{0\}$, and Q is **negative-definite** if $Q(v) < 0$ for all $v \in V \backslash \{0\}$. Since $Q(v) = B_Q(v, v)$ for all $v \in V$, clearly if Q is either positive-definite or negative-definite then Q is non-degenerate. In terms of the diagonalization with all coefficients equal to ± 1 or 0, positive-definiteness is equivalent to the condition $r = n$ (and so this possibility is coordinate-independent), and likewise negative-definiteness is equivalent to the condition $s = n$. In general we define the **null cone** to be

$$C = \{v \in V \mid Q(v) = 0\},$$

so for example if $V = \mathbb{R}^3$ and $Q(x, y, z) = x^2 + y^2 - z^2$, then the null cone consists of vectors $(x, y, \pm\sqrt{x^2 + y^2})$ and this is physically a cone (or really two cones with a common vertex at the origin and common central axis). In general C is stable under scaling and so if it is not the origin then it is a (generally infinite) union of lines through the origin; for $\mathbb{R}^2$ and $Q(x, y) = x^2 - y^2$ it is a union of two lines.

Any vector v not in the null cone satisfies exactly one of the two possibilities $Q(v) > 0$ or $Q(v) < 0$, and we correspondingly say (following Einstein) that v is **space-like** or **time-like** (with respect to Q). The set V^+ of space-like vectors is an open subset of V, as is the set V^- of time-like vectors. These open subsets are disjoint and cover the complement of the null cone.

Lemma 38.1. *The open set V^+ in V is non-empty and path-connected if $r > 1$, with r as above in terms of a diagonalizing basis for Q, and similarly for V^- if $s > 1$.*

Proof. By replacing Q with $-Q$ if necessary, we may focus on V^+. Obviously V^+ is non-empty if and only if $r > 0$, so we may now assume $r \geq 1$. We have

$$Q(x_1, \ldots, x_n) = x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2$$

with $r \geq 1$ and $0 \leq s \leq n-r$. Choose $v, v' \in V^+$, so $x_j(v) \neq 0$ for some $1 \leq j \leq r$. We may move along a line segment contained in V^+ to decrease all $x_j(v)$ to 0 for $j > r$, and similarly for v', so for the purposes of connectivity we can assume $x_j(v) = x_j(v') = 0$ for all $j > r$ (for instance write $v = v_1 + v_2$ where $v_1 = x_1(v)e_1 + \cdots + x_r(v)e_r$ and $v_2 = x_{r+1}(v)e_{r+1} + \cdots + x_{r+s}(v)e_{r+s}$. Then $\{v_1 + \varepsilon v_2 \mid 0 < \varepsilon < 1\}$ is a line segment in V^+ which connects v_1 to v, and v_1 has the desired property). If $r > 1$, then v and v' lie in the subspace $W = \text{span}(e_1, \ldots, e_r)$ of dimension $r > 1$ on which Q has positive-definite restriction. Hence, $W \backslash \{0\} \subseteq V^+$, and $W \backslash \{0\}$ is path-connected since $\dim W > 1$. $\square$

The basis giving such a diagonal form is simply a basis consisting of r space-like vectors, s time-like vectors, and $n - (r+s)$ vectors on the null cone such that all n vectors are B_Q-perpendicular to each other. In general such a basis is rather non-unique, and even the subspaces

$$V_{+,\mathbf{e}} = \text{span}(e_i \mid \lambda_i > 0), \quad V_{-,\mathbf{e}} = \text{span}(e_i \mid \lambda_i < 0)$$

are *not* intrinsic. For example, if $V = \mathbb{R}^2$ and $Q(x,y) = x^2 - y^2$ then we can take $\{e_1, e_2\}$ to be either $\{(1,0),(0,1)\}$ or $\{(2,1),(1,2)\}$, and thereby get different spanning lines. Remarkably, it turns out that the values

$$r_{\mathbf{e}} = |\{i \mid \lambda_i > 0\}| = \dim V_{+,\mathbf{e}} \quad s_{\mathbf{e}} = \{|i \mid \lambda_i < 0\}| = \dim V_{-,\mathbf{e}}, \quad t_{\mathbf{e}} = |\{i \mid \lambda_i = 0\}| = \dim V - r_{\mathbf{e}} - s_{\mathbf{e}}$$

are independent of the choice of "diagonalizing basis" $\mathbf{e}$ for Q. One thing that is clear right away is that the subspace

$$V_{0,\mathbf{e}} = \text{span}(e_i \mid \lambda_i = 0)$$

is actually intrinsic to V and Q: it is the set of $v \in V$ that are B_Q-perpendicular to the entirety of V: $B_Q(v, \cdot) = 0$ in $V^\vee$. (Beware that this is not the set of $v \in V$ such that $Q(v) = 0$).

Theorem 38.2. *Let V be a finite-dimensional $\mathbb{R}$-vector space, and Q a quadratic form on V. Let $\mathbf{e}$ be a diagonalizing basis for Q on V. The quantities $\dim V_{+,\mathbf{e}}$ and $\dim V_{-,\mathbf{e}}$ are independent of $\mathbf{e}$.*

Definition 38.1. Let Q be a quadratic form on a finite-dimensional $\mathbb{R}$-vector space V. We define the **signature** of (V, Q) (or of Q) to be the ordered pair of non-negative integers (r, s) where $r = \dim V_{+,\mathbf{e}}$ and $s = \dim V_{-,\mathbf{e}}$ respectively denote the number of positive and negative coefficients for a diagonal form of Q. In particular, $r + s \leq \dim V$ with equality if and only if Q is non-degenerate.

The signature is an invariant that is intrinsically attached to the finite-dimensional quadratic space (V, Q) over $\mathbb{R}$. In the study of quadratic spaces over $\mathbb{R}$ with the fixed dimension, it is really the "only" invariant. Indeed, we have:

Corollary 31. *Let (V, Q) and (V', Q') be finite-dimensional quadratic spaces over $\mathbb{R}$ with the same finite positive dimension. The signatures coincide if and only if the quadratic spaces are isomorphic; i.e. if and only if there exists a linear isomorphism $T : V \to V$ with $Q'(T(v)) = Q(v)$ for all $v \in V$.*

Proof. Assume such a T exists. If $\mathbf{e}$ is a diagonalizing basis for Q, clearly $\{T(e_i)\}$ is a diagonalizing basis for Q' with the same diagonal coefficients, whence Q' has the same signature as Q. Conversely, if Q and Q' have the same signatures (r, s), there exist ordered bases $\mathbf{e}$ and $\mathbf{e}'$ of V and V' such that in terms of the corresponding linear coordinate systems $x_1, \ldots, x_n$ and $x'_1, \ldots, x'_n$, we have

$$Q = x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2, \quad Q' = x_1'^2 + \cdots + x_r'^2 - x_{r+1}'^2 - \cdots - x_{r+s}'^2.$$

Note in particular that

$$Q\left(\sum a_i e_i\right) = \sum_{i=1}^{r} a_i^2 - \sum_{i=r+1}^{s} a_i^2 = Q'\left(\sum a_i e'_i\right)$$

for all i. Thus, if $T : V \to V'$ is the linear map determined by $T(e_i) = e'_i$, then T sends a basis to a basis. Thus, T is a linear isomorphism, and also

$$Q'(T\left(\sum a_i e_i\right)) = Q'\left(\sum a_i e'_i\right) = Q\left(\sum a_i e_i\right)$$

$\square$

38.4 Quaternion Algebras

In this subsection, we assume $2 \neq 0$ in F. An interesting source of quadratic forms comes from quaternion algebras. These are defined as follows: for any two elements $a, b \in F^\times$ the **quaternion algebra** $(a,b)_F$ over F as the 4-dimensional F-algebra with a basis $\{1, \alpha, \beta, \alpha\beta\}$, multipication being

$$\alpha^2 = a \quad \beta^2 = b \quad \alpha\beta = -\beta\alpha$$

One calls the set $\{1, \alpha, \beta, \alpha\beta\}$ a **quaternion basis** of $(a,b)_F$.

The isomorphism class of the quaternion algebra $(a,b)_F$ depends only on the classes of a and b in $F^\times/F^{\times 2}$ because the substitution $\alpha \mapsto u\alpha$, $\beta \mapsto v\beta$ induces an isomorphism

$$(a,b)_F \cong (u^2 a, v^2 b)_F$$

for all $u, v \in F^\times$. This implies in particular that the algebra $(a,b)_F$ is isomorphic to $(b,a)_F$; indeed, mapping $\alpha \mapsto ab\beta$, $\beta \mapsto ab\alpha$ we get

$$(a,b)_F \cong (a^2b^3, a^3b^2)_F \cong (b,a)_F$$

Given an element $q = x + y\alpha + z\beta + w\alpha\beta$ in $(a,b)_F$, we define its **conjugate** by

$$\overline{q} = x - y\alpha - z\beta - w\alpha\beta$$

The map from $(a,b)_F$ to $(a,b)_F$ given by $q \mapsto \overline{q}$ is an **anti-automorphism** of the F-algebra $(a,b)_F$, i.e. it is an F-vector space automorphism of $(a,b)_F$ satisfying $\overline{q_1q_2} = \overline{q}_2\overline{q}_1$. Moreover, we have $\overline{\overline{q}} = q$; an anti-automorphism with this property is called an **involution** in ring theory. We define the **norm** of q by $\mathrm{N}(q) = q\overline{q}$. A calculation yields

$$\mathrm{N}(q) = x^2 - ay^2 - bz^2 + abw \in F.$$

Taking norms of elements can be viewed as a map $N : (a,b)_F \to F$. This map is multiplicative: for all $q_1, q_2 \in (a,b)_F$, we have

$$\begin{aligned} \mathrm{N}(q_1q_2) &= q_1q_2\overline{q_1q_2} \\ &= q_1q_2\overline{q}_2\overline{q}_1 \\ &= q_1\mathrm{N}(q_2)\overline{q}_1 \\ &= \mathrm{N}(q_1)\mathrm{N}(q_2), \end{aligned}$$

This map is also an example of a nondegenerate quadratic form: for all $c \in F$ and $q \in (a,b)_F$, we have

$$\mathrm{N}(cq) = cq\overline{cq} = c^2\mathrm{N}(q),$$

since c is fixed by conjugation and since c belongs to the center of $(a,b)_F$. Also for all $q_1, q_2 \in (a,b)_F$, the map

$$\begin{aligned} \beta_Q(q_1,q_2) &= \mathrm{N}(q_1+q_2) - \mathrm{N}(q_1) - \mathrm{N}(q_2) \\ &= (q_1+q_2)\overline{(q_1+q_2)} - q_1\overline{q}_1 - q_2\overline{q}_2 \\ &= (q_1+q_2)(\overline{q}_1+\overline{q}_2) - q_1\overline{q}_1 - q_2\overline{q}_2 \\ &= q_1\overline{q}_1 + q_1\overline{q}_2 + q_2\overline{q}_1 + q_2\overline{q}_2 - q_1\overline{q}_1 - q_2\overline{q}_2 \\ &= q_1\overline{q}_2 + q_2\overline{q}_1 \end{aligned}$$

is symmetric bilinear and nondegenerate. The only nontrivial part here is nondegeneracy. To see why it is nondegenerate, first note that nondegeneracy of β_Q means if $\beta_Q(q_1,q_2) = 0$ for all $q_2 \in (a,b)_F$, then $q_1 = 0$. So suppose $q_1\overline{q}_2 + q_2\overline{q}_1 = 0$ for all $q_2 \in (a,b)_F$. In particular, this implies $\mathrm{N}(q_1) = 0$ (set $q_2 = q_1$ and note that $2 \neq 0$ in F) and $\mathrm{Tr}(q_1) := q_1 + \overline{q}_1 = 0$ (set $q_2 = 1$). These two conditions taken together implies $q_1^2 = 0$. However, this only implies that q_1 is nilpotent (and not that $q_1 = 0$).

The associated bilinear form β_N for the quadratic form $\mathrm{N} : (a,b)_F \mapsto F$ can be written down in matrix format as follows:

$$B_N(q,q') = \begin{pmatrix} x' & y' & z' & w' \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -a & 0 & 0 \\ 0 & 0 & -b & 0 \\ 0 & 0 & 0 & ab \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = xx' - ayy' - bzz' + abww'$$

Where $q = x + y\alpha + z\beta + w\alpha\beta$ and $q' = x' + y'\alpha + z'\beta + w'\alpha\beta$. The nondeneracy of the bilinear form can be seen in the matrix representation. If the matrix is invertible, then the bilinear form is nondegenerate.

Lemma 38.3. *An element q of the quaternion algebra $(a,b)_F$ is invertible if and only if it has a nonzero norm. In particular, $(a,b)_F$ is a division algebra if and only if the norm $N : (a,b)_F \mapsto F$ does not vanish outside* 0.

Proof. Suppose q has a nonzero norm. Then the inverse of q is given by $\overline{q}/N(q)$. Conversely, suppose q is invertible. To obtain a contradiction, assume $N(q) = 0$. Then $q\overline{q} = N(q) = 0$ implies $\overline{q} = 0$ (apply q^{-1} to both sides), but this implies $q = 0$, which is a contradiction since q is invertible. □

39 Differential Equations and Linear Algebra

Consider the following homogeneous linear differential equation with constant (real) coefficients:

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0 \tag{105}$$

The "homogeneous" label means if y fits (105), then so does cy for any constant $c \in \mathbb{R}$ (if the right side were a nonzero function then cy would no longer be a solution and (105) is then called "inhomogeneous." The "linear" part refers to the linear operator

$$D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0 I,$$

where $D = \mathrm{d}/\mathrm{d}t$ is the basic differentiation operator on functions.

Let $C^\infty(\mathbb{R})$ be the space of all functions $\mathbb{R} \to \mathbb{R}$ that are infinitely differentiable. This is an infinite-dimensional vector space, and it is this space in which we search for solutions to (105) because any solution to (105) must be in here.

Let

$$p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

be the polynomial having the coefficients from (105). When the polynomial $p(t)$ factors, the operator $p(D)$ factors in a similar way: if

$$p(t) = (t - c_1)\cdots(t - c_n)$$

then

$$p(D) = (D - c_1 I)\cdots(D - c_n I). \tag{106}$$

Real polynomials do not always factor into linear factors with real coefficients, but the fundamental theorem of algebra tells us that complex polynomials always factor into linear factors with complex coefficients. Therefore, we generalize our point of view and consider equations like (105) with *complex* coefficients in order to have the factorization (106) available. For example, if $y'' + y = 0$ then $(D^2 + I)(y) = 0$ and the corresponding polynomial is $t^2 + 1$, which factors as $(t + i)(t - i)$. We want to regard $y'' + y$ as $(D + iI)(D - iI)(y)$, and a meaning has to be given to $D + iI$ and $D - iI$. So let $C^\infty(\mathbb{R}, \mathbb{C})$ be the set of infinitely-differentiable functions $f\colon \mathbb{R} \to \mathbb{C}$. The domain is still $\mathbb{R}$; only the range has been enlarged.

Theorem 39.1. *For $c \in \mathbb{C}$, the solutions to $y' = cy$ are the functions $y(t) = re^{ct}$ for $r \in \mathbb{C}$.*

Proof. Since $(e^{ct})' = ce^{ct}$, and re^{ct} satisfies $y' = cy$. Conversely, suppose $y' = cy$. Then the ratio y/e^{ct} has derivative $(e^{ct}y' - y(e^{ct})')/(e^{ct})^2 = (e^{ct}cy - yce^{ct})/(e^{ct})^2 = 0$, so y/e^{ct} is a constant. Call the constant r, so $y = re^{ct}$. □

The equation $y' = cy$ is the same as $y' - cy = 0$, so $D - cI$ on $C^\infty(\mathbb{R}, \mathbb{C})$ has a one-dimensional kernel with e^{ct} as a basis:

$$\operatorname{Ker}(D - cI) = \mathbb{C}e^{ct}.$$

For example, the solution space of $y' = y$ is $\mathbb{C}e^t$ and not just $\mathbb{R}e^t$. For other differential equations like $y' = iy$, with honest complex coefficients, there may be no real-valued solutions besides the zero function while there are nonzero complex solutions.

Lemma 39.2. *For each $c \in \mathbb{C}$, $D - cI$ is onto. That is, for every $f \in C^\infty(\mathbb{R}, \mathbb{C})$, there is a $u \in C^\infty(\mathbb{R}, \mathbb{C})$ such that $u' - cu = f$.*

Proof. First, we check the special case $c = 0$, which says for every f there is a u such that $u' = f$. This is just a matter of antidifferentiating real and imaginary parts. Indeed, write $f(t) = a(t) + ib(t)$ and choose antiderivatives for $a(t)$ and $b(t)$, say $A(t) = \int_0^t a(x)dx$ and $B(t) = \int_0^t b(x)dx$. Then $u(t) = A(t) + iB(t)$ has derivative $a(t) + ib(t) = f(t)$, since $f(t)$ is infinitely differentiable and $u' = f$, so is u. We're done with the case $c = 0$.

Now we show any $D - cI$ is onto, i.e. the differentiable equation $u' - cu = f$, where f is given, has a solution u in $C^\infty(\mathbb{R}, \mathbb{C})$. The strategy is to reduce to the previously treated case $c = 0$ by a "change of coordinates." Multiply through the equation by e^{-ct} (which is an invertible procedure, since e^{ct} is a nonvanishing function):

$$e^{-ct}u' - ce^{-ct}u = e^{-ct}f.$$

By the product rule, this equation is the same as

$$(e^{-ct}u)' = e^{-ct}f.$$

This equation has the form $v' = g$, where $g = e^{-ct}f$ is given and v is sought. That is the case treated in the previous paragraph: pick antiderivatives for the real and imaginary parts of $g(t)$ to get an antiderivative $v(t)$ for $g(t)$, and then multiply $v(t)$ by e^{ct} to find a solution u. So if $f(t) = a(t) + ib(t)$, then $u(t)$ is

$$u(t) = e^{ct}\left(\int_0^t a(x)e^{-cx}dx + i\int_0^t b(x)e^{-cx}dx\right).$$

□

Remark 55. We can actually replace c with a $\mathbb{C}$-valued function f, i.e. $D - fI$ is onto.

Lemma 39.3. *Let V be an F-vector space and let $T, U \in Hom_F(V, V)$ such that $Ker(T)$ and $Ker(U)$ are finite-dimensional and U is onto. Then $Ker(TU)$ is finite-dimensional and*

$$dim(Ker(TU)) = dim(Ker(T)) + dim(Ker(U)).$$

Proof. Write $m = \dim(\mathrm{Ker}(T))$ and $n = \dim(\mathrm{Ker}(U))$. We want to prove $\dim(\mathrm{Ker}(TU)) = m + n$. First we will prove $\mathrm{Ker}(TU)$ is finite-dimensional, with a spanning set of $m + n$ vectors, so $\dim(\mathrm{Ker}(TU)) \leq m + n$. Then we will prove the spanning set we find for $\mathrm{Ker}(TU)$ is linearly independent, so $\dim(\mathrm{Ker}(TU)) = m + n$.

Let $v_1, \ldots, v_m$ be a basis of $\mathrm{Ker}(T)$ and $w_1, \ldots, w_n$ be a basis of $\mathrm{Ker}(U)$. For any $v \in \mathrm{Ker}(TU)$, the equation $(TU)(v) = 0$ says $T(Uv) = 0$, so Uv is in the kernel of T :

$$Uv = c_1v_1 + \cdots + c_mv_m$$

for some $c_1, \ldots, c_m \in F$.

To get anywhere with this equation, we use the hypothesis that U is onto to write the v_i's in another way. Since U is onto, we can write $v_i = U(\tilde{v}_i)$ for some $\tilde{v}_i$ in V. Then the above equation becomes

$$\begin{aligned} Uv &= c_1U(\tilde{v}_1) + \cdots + c_mU(\tilde{v}_m) \\ &= U(c_1\tilde{v}_1 + \cdots + c_m\tilde{v}_m). \end{aligned}$$

When U takes the same value at two vectors, the difference of those vectors is in the kernel of U. Therefore

$$v = c_1\tilde{v} + \cdots + c_m\tilde{v}_m + v', \tag{107}$$

where $v' \in \mathrm{Ker}(U)$. Writing v' in terms of the basis $w_1, \ldots, w_n$ of $\mathrm{Ker}(U)$ and feeding this into (107), we have

$$v = c_1\tilde{v}_1 + \cdots + c_m\tilde{v}_m + d_1w_1 + \cdots + d_nw_n$$

for some $d_1, \ldots, d_n \in F$.

We have written a general element v of $\mathrm{Ker}(TU)$ as a linear combination of $m + n$ vectors: the $\tilde{v}_i$'s and the w_j's. Moreover, the $\tilde{v}_i$'s and w_j's are in $\mathrm{Ker}(TU)$:

$$(TU)(\tilde{v}_i) = T(U\tilde{v}_i) = T(v_i) = 0, \qquad (TU)(w_j) = T(Uw_j) = T(0) = 0.$$

Since we have shown the $\tilde{v}_i$'s and w_j's are a spanning set for $\mathrm{Ker}(TU)$, this kernel has dimension at most $m + n$.

To prove $\tilde{v}_1, \cdots, \tilde{v}_m, w_1, \ldots, w_n$ is a linearly independent set, suppose some F-linear combination is 0:

$$c_1\tilde{v}_1 + \cdots + c_m\tilde{v}_m + d_1w_1 + \cdots + d_nw_n = 0. \tag{108}$$

Applying U to this equation turns each $\tilde{v}_i$ into v_i and turns each w_j into 0, so we find

$$c_1v_1 + \cdots + c_mv_m = 0.$$

The v_i's are linearly independent, so each c_i is 0. This turns (108) into

$$d_1w_1 + \cdots + d_nw_n = 0.$$

Now, since the w_j's are linearly independent, each d_j is 0. And we are done. □

Example 39.1. We want to construct the kernel of $(D - \alpha_2)(D - \alpha_1)$ where $\alpha_1 \neq \alpha_2$. By Theorem (39.1), $e^{\alpha_1 t}$ spans $\mathrm{Ker}(D - \alpha_1)$ and $e^{\alpha_2 t}$ spans $\mathrm{Ker}(D - \alpha_2)$. A basis for $\mathrm{Ker}((D - \alpha_2)(D - \alpha_1))$ is given by $\{e^{\alpha_1 t}, \widetilde{e^{\alpha_2 t}}\}$, where $\widetilde{e^{\alpha_2 t}}$ is a lift of $e^{\alpha_2 t}$ via $D - \alpha_1$. We can compute this explicitely using Lemma (39.2). We get:

$$\begin{aligned} \widetilde{e^{\alpha_2 t}} &= e^{\alpha_1 t}\int_0^t e^{\alpha_2 x}e^{-\alpha_1 x}dx \\ &= e^{\alpha_1 t}\int_0^t e^{(\alpha_2 - \alpha_1)x}dx \\ &= e^{\alpha_1 t}\left(\frac{e^{(\alpha_2-\alpha_1)t} - 1}{\alpha_2 - \alpha_1}\right) \\ &= \frac{e^{\alpha_2 t} - e^{\alpha_1 t}}{\alpha_2 - \alpha_1}. \end{aligned}$$

Example 39.2. We want to construct the kernel of $(D-\alpha_3)(D-\alpha_2)(D-\alpha_1)$ where α_1, α_2 and α_3 are distinct complex numbers. By Theorem (39.1), $e^{\alpha_1 t}$ spans $\operatorname{Ker}(D-\alpha_1)$, $e^{\alpha_2 t}$ spans $\operatorname{Ker}(D-\alpha_2)$, and $e^{\alpha_3 t}$ spans $\operatorname{Ker}(D-\alpha_3)$. A basis for $\operatorname{Ker}((D-\alpha_3)(D-\alpha_2))$ is given by $\left\{e^{\alpha_2 t}, \frac{e^{\alpha_3 t}-e^{\alpha_2 t}}{\alpha_3-\alpha_2}\right\}$ by the previous example. We need to lift these solutions via $D-\alpha_1$ to get a basis for $\operatorname{Ker}((D-\alpha_3)(D-\alpha_2)(D-\alpha_1))$. We've already lifted $e^{\alpha_2 t}$ in the previous example, so let's focus on lifting $\frac{e^{\alpha_3 t}-e^{\alpha_2 t}}{\alpha_3-\alpha_2}$. We get:

$$\begin{aligned}
\widetilde{\frac{e^{\alpha_3 t}-e^{\alpha_2 t}}{\alpha_3-\alpha_2}} &= e^{\alpha_1 t}\int_0^t \left(\frac{e^{\alpha_3 x}-e^{\alpha_2 x}}{\alpha_3-\alpha_2}\right)e^{-\alpha_1 x}dx \\
&= \frac{e^{\alpha_1 t}}{\alpha_3-\alpha_2}\int_0^t (e^{\alpha_3 x}-e^{\alpha_2 x})e^{-\alpha_1 x}dx \\
&= \frac{e^{\alpha_1 t}}{\alpha_3-\alpha_2}\left(\int_0^t e^{(\alpha_3-\alpha_1)x}dx - \int_0^t e^{(\alpha_2-\alpha_1)x}dx\right) \\
&= \frac{e^{\alpha_1 t}}{\alpha_3-\alpha_2}\left(\frac{e^{(\alpha_3-\alpha_1)t}-1}{\alpha_3-\alpha_1} - \frac{e^{(\alpha_2-\alpha_1)t}-1}{\alpha_2-\alpha_1}\right). \\
&= \frac{1}{\alpha_3-\alpha_2}\left(\frac{e^{\alpha_3 t}-e^{\alpha_1 t}}{\alpha_3-\alpha_1} - \frac{e^{\alpha_2 t}-e^{\alpha_1 t}}{\alpha_2-\alpha_1}\right) \\
&= \frac{(e^{\alpha_3 t}-e^{\alpha_1 t})(\alpha_2-\alpha_1)-(e^{\alpha_2 t}-e^{\alpha_1 t})(\alpha_3-\alpha_1)}{(\alpha_3-\alpha_2)(\alpha_3-\alpha_1)(\alpha_2-\alpha_1)} \\
&= \frac{\alpha_2 e^{\alpha_3 t}-\alpha_2 e^{\alpha_1 t}-\alpha_1 e^{\alpha_3 t}+\alpha_1 e^{\alpha_1 t}-\alpha_3 e^{\alpha_2 t}+\alpha_3 e^{\alpha_1 t}+\alpha_1 e^{\alpha_2 t}-\alpha_1 e^{\alpha_1 t}}{(\alpha_3-\alpha_2)(\alpha_3-\alpha_1)(\alpha_2-\alpha_1)} \\
&= \frac{(\alpha_3-\alpha_2)e^{\alpha_1 t}+(\alpha_1-\alpha_3)e^{\alpha_2 t}+(\alpha_2-\alpha_1)e^{\alpha_3 t}}{(\alpha_3-\alpha_2)(\alpha_3-\alpha_1)(\alpha_2-\alpha_1)}.
\end{aligned}$$

Thus a basis for $\operatorname{Ker}((D-\alpha_3)(D-\alpha_2)(D-\alpha_1))$ is given by

$$\left\{e^{\alpha_1 t}, \frac{e^{\alpha_2 t}-e^{\alpha_1 t}}{\alpha_2-\alpha_1}, \frac{(\alpha_3-\alpha_2)e^{\alpha_1 t}+(\alpha_1-\alpha_3)e^{\alpha_2 t}+(\alpha_2-\alpha_1)e^{\alpha_3 t}}{(\alpha_3-\alpha_2)(\alpha_3-\alpha_1)(\alpha_2-\alpha_1)}\right\},$$

or

$$\left\{e^{\alpha_1 t}, \frac{e^{\alpha_2 t}}{\alpha_2-\alpha_1}+\frac{e^{\alpha_1 t}}{\alpha_1-\alpha_2}, \frac{e^{\alpha_1 t}}{(\alpha_3-\alpha_1)(\alpha_2-\alpha_1)}+\frac{e^{\alpha_2 t}}{(\alpha_3-\alpha_2)(\alpha_1-\alpha_2)}+\frac{e^{\alpha_3 t}}{(\alpha_3-\alpha_2)(\alpha_3-\alpha_1)}\right\}$$

If we let $p(T)=(T-\alpha_3)(T-\alpha_2)(T-\alpha_1)$ and $q(T)=(T-\alpha_2)(T-\alpha_1)$, then we can write this as

$$\left\{e^{\alpha_1 t}, \sum_{i=1}^{2}\frac{e^{\alpha_i t}}{q'(\alpha_i)}, \sum_{i=1}^{3}\frac{e^{\alpha_i t}}{p'(\alpha_i)}\right\}$$

Part V
Module Theory

In this part, we will study the theory of modules over a commutative ring[4].

40 Basic Definitions

40.1 Definition of an R-Module

Definition 40.1. Let R be a commutative ring. An R-**module** M consists of an abelian group on which R acts by additive maps: there is a scalar multiplication function $R \times M \to M$ denoted by $(a, m) \mapsto am$ such that for all $u, v \in M$, $a, b \in R$ we have

1. $1u = u$ and $a(bu) = (ab)u$.
2. $a(u+v) = au + av$ and $(a+b)u = au + bu$.

Throughout these notes, we often write "let M be an R-module" or "let I be an ideal in R" without specifying what R is. In either case, it is understood that R is a commutative ring. We will also say "let M be a module over

[4]There is a theory of modules over a non-commutative ring, but we leave that topic to another document.

R" instead of "let M be an R-module". Sometimes the base ring R isn't important to know and we will refer to M simply as a module rather than an R-module.

40.1.1 Consistency in Notation

When learning Mathematics, it's a good practice to write things down in an organized way. Doing so will help organize ideas and concepts in your mind, making it easier to work with them. For instance, we will typically use the capital letters R, S or A, B to denote rings. Similarly, we will typically use the capital letters M, N to denote modules. If M is an R-module, then we will typically use lower case letters a, b, c to denote elements of R and use lower case letters u, v, w to denote elements of M. Many authors use the lower case letters r, s to denote elements of R and use the lower case letter m, n to denote elements of M. This is completely fine! Sometimes we will even use the lower case letters r, s to denote elements of R. In fact, if we are dealing with a ring R together with a ring A, then we will try to use the lower case letters r, s to denote elements of R and the lower case letters a, b to denote elements of A. However we will try to avoid using the lower case letters m, n to denote elements of M. This is because we try to use lower case letters like i, j, k, l, m, n as indices. For instance, we may write an element in M as

$$\sum_{i=1}^{m} a_i u_i = a_1 u_1 + \cdots + a_m u_m. \tag{109}$$

where the a_i are elements of R and the u_i are elements of M. The lower case m here is simply the number of terms in (109).

Throughout this document, the reader will find many more examples of consistency in notation as in the case described above. Keep in mind however that this rule is not set in stone; we may violate it. The point however is that if you try to be as consistent as possible with your notation, it will make learning Mathematics much easier (and more fun!).

40.1.2 Examples of R-Modules

Let R be a ring and let X be a nonempty set. At the moment, the ring R and the set X have nothing to do with each other, however we'd like to turn X into an R-module somehow. How can we do this? Well, the first step would be to give X the **structure of an abelian group**! In particular, we need define an addition map $+\colon X \times X \to X$ such that the pair $(X, +)$ forms an abelian group. In this case, we say addition $+$ **gives** X **the structure of an abelian group**. Once X is given the structure of an abelian group, the next thing we'd need to do is to define a scalar multiplication map $\cdot\colon R \times X \to X$ such that the triple $(X, +, \cdot)$ forms an R-module. In this case, we say addition $+$ and multiplication $\cdot$ **gives** X **the structure of an** R**-module**. We often use this language when describing modules.

Example 40.1. Let R be a ring and let $n \geq 1$. Then the set $R^n = \{(a_1, \ldots, a_n) \mid a_i \in R\}$ can be given the structure of an R-module as follows: addition and scalar multiplication are defined by

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n) \quad \text{and} \quad a(a_1, \ldots, a_n) := (aa_1, \ldots, aa_n)$$

$a \in R$ and $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in R^n$. Check that addition and scalar multiplication defined in this way really does give R^n an R-module structure.

Example 40.2. One of the reasons why we study R-modules is because they help us obtain information about the ring R itself. For instance, if R is a principal ideal domain, then it turns out that every finitely generated R-module is isomorphic to a direct sum of a free module plus a torsion module. The proof of this fact uses the in an essential way the fact that R is a principal ideal domain.

40.2 Definition of an R-Linear Map

Definition 40.2. Let M and N be R-modules. A map $\varphi\colon M \to N$ is called an R**-linear map** if for all a, b in R and u, v in M, we have

$$\varphi(au + bv) = a\varphi(u) + b\varphi(v).$$

An R-linear map $\varphi\colon M \to N$ is also called an R**-module homomorphism**. A bijective R-module homomorphism is called an R**-module isomorphism**. If $\varphi\colon M \to N$ is an R-module isomorphism, then we say M is **isomorphic to** N, and we denote this by $M \cong N$. The collection of all R-modules and R-linear maps forms a category which we will denote by $\mathbf{Mod}_R$.

Remark 56. Note that $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$ implies $\varphi(0) = 0$.

When the base ring R is understood from context, we will sometimes drop "R" in "R-linear map" and simply write "linear map". We also write "let $\varphi\colon M \to N$ be an R-linear map" without specifying what R, M, and N is. In thise case, it is understood that R is a commutative ring and that M and N are R-modules.

40.3 Submodules, Kernels, and Quotient Modules

Definition 40.3. Let $\varphi\colon M \to N$ be an R-linear map.

1. The **kernel** of φ, denoted $\ker\varphi$, is defined to be the set

$$\ker\varphi := \{u \in M \mid \varphi(u) = 0\}.$$

   In a moment, we will show that $\ker\varphi$ can be given the structure of an R-module.

2. The **image** of φ, denoted $\operatorname{im}\varphi$, is defined to be the set

$$\operatorname{im}\varphi := \{\varphi(u) \in N \mid u \in M\}.$$

   In a moment, we will show that $\operatorname{im}\varphi$ can be given the structure of an an R-module.

3. If M is a subset of N and φ is the inclusion map, then we say M is an R**-submodule** of N. In this case, we also define the **quotient** of N with respect to M, denoted N/M, to be the set

$$N/M = \{v + M \mid v \in N\}.$$

   That is, N/M is the set of equivalence classes of elements of N, where $v_1, v_2 \in N$ are equivalent if $v_1 - v_2 \in M$. An equivalent class in N/M is denoted by $v + M$ or more simply by $\overline{v}$. In this case, we call v a **representative** of the equivalence class $\overline{v}$. From basic group theory, we know that N/M has the structure of an abelian group, where addition is defined by $\overline{v_1} + \overline{v_2} = \overline{v_1 + v_2}$ for all $\overline{v_1}, \overline{v_2} \in N/M$. In fact, N/M has the structure of an R-module, where scalar multiplication is defined by $a\overline{v} = \overline{av}$ for all $a \in R$ and $\overline{v} \in N/M$. One checks that this is well-defined and together with addition defined above does indeed give N/M the structure of an R-module.

4. The **cokernel** of φ, denote $\operatorname{coker}\varphi$, is defined to be the R-module

$$\operatorname{coker}\varphi = N/\operatorname{im}\varphi. \tag{110}$$

   In a moment, we will show that $\operatorname{im}\varphi$ can be given the structure of an an R-submodule of N, so that definition (110) makes sense.

Remark 57. Let N be an R-module and let M be a subset of N. Then M is an R-submodule of N if and only if M is nonempty and $au + bv \in M$ for all $a, b \in R$ and $u, v \in M$. Equivalently, M is an R-submodule of N if and only if M is nonempty $au + v \in M$ for all $a \in R$ and $u, v \in M$. This is sometimes called the **submodule criterion test**. If M satisfies the submodule criterion test, then it is easy to check that we can give it the structure of an R-module by using the R-module operations from N.

Proposition 40.1. *Let $\varphi\colon M \to N$ be an R-linear map. Then* $\ker\varphi$ *is a submodule of M and* $\operatorname{im}\varphi$ *is a submodule of N.*

Proof. Let us first show that $\ker\varphi$ is a submodule of M. Observe that $\ker\varphi$ is nonempty since $0 \in \ker\varphi$. Let $a \in R$ and let $u, v \in \ker\varphi$. Then we have

$$\begin{aligned}\varphi(au + v) &= a\varphi(u) + \varphi(v)\\ &= a \cdot 0 + 0\\ &= 0 + 0\\ &= 0.\end{aligned}$$

It follows that $au + v \in \ker\varphi$. Thus $\ker\varphi$ is a submodule of M.

Now we will show that $\operatorname{im}\varphi$ is a submodule of N. Observe that $\operatorname{im}\varphi$ is nonempty since $\varphi(0) \in \operatorname{im}\varphi$. Let $a \in R$ and let $\varphi(u), \varphi(v) \in \operatorname{im}\varphi$. Then we have

$$\begin{aligned}a\varphi(u) + \varphi(v) &= \varphi(au) + \varphi(v)\\ &= \varphi(au + v).\end{aligned}$$

It follows that $a\varphi(u) + \varphi(v) \in \operatorname{im}\varphi$. Thus $\operatorname{im}\varphi$ is a submodule of N. □

40.4 Base Change

Throughout this subsection, let $f\colon R \to S$ be a ring homomorphism.

40.4.1 Restriction of scalars functor

If N is an S-module, then we can restrict it to an R-module N_R where N_R has the same underlying abelian group structure as N but with scalar multiplication given by

$$a \cdot v = f(a)v$$

for all $a \in R$ and $v \in N$. This is called **restriction of scalars** since in the case where $R \subseteq S$ we are just restricting the S-action to an R-action. If $\psi \colon N \to N'$ is an S-module linear map, then we define an R-module linear map $\psi_R \colon N_R \to N'_R$ by

$$\psi_R(v) = \psi(v)$$

for all $v \in N_R$. Let us check that ψ_R is indeed an R-linear map. We just need to check that ψ_R respects scalar multiplication since additivity is clear. Let $a \in R$ and let $v \in N_R$. Then

$$\begin{aligned} \psi_R(a \cdot v) &= \psi_R(f(a)v) \\ &= \psi(f(a)v) \\ &= f(a)\psi(v) \\ &= a \cdot \psi(v) \\ &= a \cdot \psi_R(v). \end{aligned}$$

It follows that ψ_R is an R-module linear map. It is easy to check that we obtain a functor

$$-_R \colon \mathbf{Mod}_S \to \mathbf{Mod}_R.$$

40.4.2 Extension of scalars functor

If M is an R-module, then we can extend it to an S-module $S \otimes_R M$ where scalar multiplication is defined by

$$a \cdot (b \otimes u) = ab \otimes u$$

for all $a, b \in S$ and $u \in M$. This is called **extension of scalars** since in the case where $R \subseteq S$ we are just extending the R-action to an S-action. If $\varphi \colon M \to M'$ is an R-module linear map, then we define an S-module linear map $1 \otimes \varphi \colon S \otimes_R M \to S \otimes_R M$ on elementary tensors $a \otimes u \in S \otimes_R M$ by

$$(1 \otimes \varphi)(a \otimes u) = a \otimes \varphi(u),$$

and then extend this linearly everywhere else. We just need to check that $1 \otimes \varphi$ respects scalar multiplication since additivity is clear. Let $a \in S$ and let $b \otimes u$ be an elementary tensor in $S \otimes_R M$. Then

$$\begin{aligned} (1 \otimes \varphi)(a \cdot (b \otimes u)) &= (1 \otimes \varphi)(ab \otimes u) \\ &= ab \otimes \varphi(u) \\ &= a \cdot (b \otimes \varphi(u)) \\ &= a \cdot ((1 \otimes \varphi)(b \otimes u)). \end{aligned}$$

It follows that $1 \otimes \varphi$ is an R-module linear map. It is easy to check that we obtain a functor

$$S \otimes_R - \colon \mathbf{Mod}_R \to \mathbf{Mod}_S.$$

40.4.3 Restricting scalars and extending scalars form an adjoint pair

Proposition 40.2. *The functors $-_R \colon \mathbf{Mod}_S \to \mathbf{Mod}_R$ and $- \otimes_R S \colon \mathbf{Mod}_R \mapsto \mathbf{Mod}_S$ are adjoint functors. In a formula*

$$\mathrm{Hom}_R(M, N_R) \cong \mathrm{Hom}_S(M \otimes_R S, N)$$

for all R-modules M and for all S-modules N.

Example 40.3. Let I be an ideal in R. Let us calculate $\mathrm{Hom}_R(R/I, R/I)$. We have

$$\begin{aligned} \mathrm{Hom}_R(R/I, R/I) &\cong \mathrm{Hom}_{R/I}((R/I) \otimes_R (R/I), R/I) \\ &\cong \mathrm{Hom}_{R/I}(R/I, R/I) \\ &\cong R/I. \end{aligned}$$

40.4.4 Base Change

There is another type of R-module that can be viewed as an S-module. For simplicity, assume that $R \subset S$ is an extension of rings. Suppose M is an R-module and N is an S-module. Through restriction of scalars, we can view N as an R-module. Thus we can consider $\mathrm{Hom}_R(N, M)$. In fact, $\mathrm{Hom}_R(N, M)$ can be viewed as an S-module via the action

$$b \cdot \varphi(v) = \varphi(bv)$$

for all $b \in S$, $\varphi \in \mathrm{Hom}_R(N, M)$, and $v \in N$.

Theorem 40.1. *Let $R \subset S$ be a ring extension and let $\varphi \in \mathrm{Hom}_S(N, N')$ and let $\psi \in \mathrm{Hom}_R(M, M')$ where M, M' are R-modules and N, N' are S-modules. Then $\varphi^*\colon \mathrm{Hom}_R(N', M) \to \mathrm{Hom}_R(N, M)$ and $\psi_*\colon \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, M')$ are S-module homomorphisms.*

40.4.5 Translated Modules

In this section, we want to discuss how to translate an A-module M by an element $x \in M$. Let $M^x := \{y + x \mid y \in M\}$. We define addition and scaling operations as follows. Suppose a is an element in A and, $y + x$ and $y' + x$ are two elements in M^x. Then

$$\begin{aligned}(y + x)\dot{+}(y' + x) &= y + y' + x\\ a \cdot (y + x) &= a \cdot y + x.\end{aligned}$$

Addition $\dot{+}$ makes M^x into an abelian group with identity being x, and one can check that all of the conditions for M^x to be an A-module are satisfied.

We can generalize the above constrution as follows: Let $\varphi : M \to M^\varphi$ be an isomorphism from M to some set M^φ. We define addition and scaling operations as follows: Suppose $a \in A$ and $x, y \in M^\varphi$. Then we define

$$\begin{aligned}x\dot{+}y &= \varphi\left(\varphi^{-1}(x) + \varphi^{-1}(y)\right)\\ a \cdot x &= \varphi\left(a\varphi^{-1}(x)\right)\end{aligned}$$

Addition $\dot{+}$ makes M^φ into an abelian group with identity being $\varphi(0)$. For instance, we have associativity:

$$\begin{aligned}(x\dot{+}y)\dot{+}z &= \varphi\left(\varphi^{-1}(x) + \varphi^{-1}(y)\right)\dot{+}z\\ &= \varphi\left(\varphi^{-1}\left(\varphi\left(\varphi^{-1}(x) + \varphi^{-1}(y)\right)\right)\dot{+}\varphi^{-1}(z)\right)\\ &= \varphi\left(\left(\varphi^{-1}(x) + \varphi^{-1}(y)\right)\dot{+}\varphi^{-1}(z)\right)\\ &= \varphi\left(\varphi^{-1}(x) + \left(\varphi^{-1}(y)\dot{+}\varphi^{-1}(z)\right)\right)\\ &= \varphi\left(\varphi^{-1}(x) + \varphi\left(\varphi^{-1}\left(\varphi^{-1}(y)\dot{+}\varphi^{-1}(z)\right)\right)\right)\\ &= x\dot{+}\varphi\left(\varphi^{-1}(y) + \varphi^{-1}(z)\right)\\ &= x\dot{+}(y\dot{+}z).\end{aligned}$$

and we have commutativity:

$$\begin{aligned}x\dot{+}y &= \varphi\left(\varphi^{-1}(x) + \varphi^{-1}(y)\right)\\ &= \varphi\left(\varphi^{-1}(y) + \varphi^{-1}(x)\right)\\ &= y\dot{+}x.\end{aligned}$$

One can check that all of the conditions for M^φ to be an A-module are satisfied. For instance, suppose $a, b \in A$, and $x, y \in M^\varphi$, we have

$$\begin{aligned}a \cdot (x\dot{+}y) &= a \cdot \left(\varphi\left(\varphi^{-1}(x) + \varphi^{-1}(y)\right)\right)\\ &= \varphi\left(a\left(\varphi^{-1}\left(\varphi\left(\varphi^{-1}(x) + \varphi^{-1}(y)\right)\right)\right)\right)\\ &= \varphi\left(a\left(\varphi^{-1}(x) + \varphi^{-1}(y)\right)\right)\\ &= \varphi\left(a\varphi^{-1}(x) + a\varphi^{-1}(y)\right)\\ &= \varphi\left(\varphi^{-1}(a \cdot x) + \varphi^{-1}(a \cdot y)\right)\\ &= a \cdot x\dot{+}a \cdot y.\end{aligned}$$

and

$$\begin{aligned}(a+b)\cdot x &= \varphi\left((a+b)\varphi^{-1}(x)\right)\\ &= \varphi\left(a\varphi^{-1}(x)+b\varphi^{-1}(x)\right)\\ &= \varphi\left(\varphi^{-1}(a\cdot x)+\varphi^{-1}(b\cdot x)\right)\\ &= a\cdot x\dot{+}b\cdot x\end{aligned}$$

and

$$\begin{aligned}(ab)\cdot x &= \varphi\left(ab\varphi^{-1}(x)\right)\\ &= \varphi\left(a\varphi^{-1}\left(\varphi(b\varphi^{-1}(x))\right)\right)\\ &= a\cdot(\varphi(b\varphi^{-1}(x)))\\ &= a\cdot(b\cdot x)\end{aligned}$$

The way we defined addition and A-scaling on M^{φ} makes φ an A-linear map. Indeed, we have

$$\begin{aligned}\varphi(ax+by) &= \varphi(\varphi^{-1}(\varphi(ax))+\varphi^{-1}(\varphi(by)))\\ &= \varphi(ax)\dot{+}\varphi(by)\\ &= \varphi(a\varphi^{-1}(\varphi(x)))\dot{+}\varphi(b\varphi^{-1}(\varphi(y)))\\ &= a\cdot\varphi(x)\dot{+}b\cdot\varphi(y)\end{aligned}$$

for all $a,b\in A$ and $x,y\in M$.

Now suppose $M^{\varphi}=M$ and let φ be additive, that is, $\varphi(x+y)=\varphi(x)+\varphi(y)$ for all $x,y\in M$. Then $\dot{+}$ is the same $+$ since φ^{-1} is additive and

$$\begin{aligned}x\dot{+}y &= \varphi(\varphi^{-1}(x)+\varphi^{-1}(y))\\ &= \varphi(\varphi^{-1}(x+y))\\ &= x+y\end{aligned}$$

for all $x,y\in M$. On the other hand, we can still have a different scaling map, as long as φ is not A-linear.

41 Free Modules

41.0.1 Generating Sets

Definition 41.1. Let M be an R-module and let $\{u_\lambda\}_{\lambda\in\Lambda}$ be a collection of elements in M. We say $\{u_\lambda\}$ **generates** M if for all $u\in M$ there exists $u_{\lambda_1},\dots u_{\lambda_n}\in\{u_\lambda\}$ and $a_{\lambda_1},\dots,a_{\lambda_n}\in R$ such that

$$u=a_{\lambda_1}u_{\lambda_1}+a_{\lambda_2}u_{\lambda_2}+\cdots+a_{\lambda_n}u_{\lambda_n}.$$

If $\{u_\lambda\}$ generates M, then we say $\{u_\lambda\}$ is a **generating set** for M. We say M is **finitely-generated** if there exists a finite generating set for M.

41.0.2 Free Modules

Definition 41.2. Let M be an R-module and let $u_1, \dots, u_n \in M$. We say the set $\{u_1, \dots, u_n\}$ is a **basis for** M if the following conditions hold:

1. it generates M as an R-module: for each $u \in M$ there exists $a_1, \dots, a_n \in R$ such that
$$u = a_1 u_1 + \cdots + a_n u_n,$$
2. it is linearly independent: if $a_1, \dots, a_n \in R$ such that
$$a_1 u_1 + \cdots + a_n u_n = 0,$$
then $a_i = 0$ for all $1 \leq i \leq n$.

More generally, let $\{u_\lambda\}$ be a collection of elements in M indexed over some (possibly infinite) set Λ. We say the set $\{u_\lambda\}$ is a **basis for** M if

1. it generates M as an R-module: for each $u \in M$ there exists $u_{\lambda_1}, \dots, u_{\lambda_n} \in \{u_\lambda\}$ and $a_{\lambda_1}, \dots, a_{\lambda_n} \in R$ such that
$$u = a_{\lambda_1} u_{\lambda_1} + \cdots + a_{\lambda_n} u_{\lambda_n}.$$
2. every finite subset of $\{u_\lambda\}$ is linearly independent: if $a_{\lambda_1}, \dots, a_{\lambda_n} \in R$ such that
$$a_{\lambda_1} u_{\lambda_1} + \cdots + a_{\lambda_n} u_{\lambda_n} = 0,$$
then $a_{\lambda_i} = 0$ for all $1 \leq i \leq n$.

We say M is a **free** R**-module** if it has a basis.

Example 41.1. R^n is the **standard free** R**-module of rank** n. It has as basis the **standard basis elements** e_i where e_i is the vector with 1 in the ith entry and 0 everywhere else.

Example 41.2. If I is a nonzero ideal in R, then R/I is not a free R-module. Indeed, if r is a nonzero element in I, then for all $s \in R$, we have $r\overline{s} = \overline{rs} = 0$ in R/I. In other words, "**torsion**" makes linear independence fail for elements of R/I when taking coefficients from R.

41.0.3 Universal Mapping Property of Free R-Modules

Free modules are characterized by the following universal mapping property: Let F be a free R-module with basis $\{e_\lambda\}$ indexed over a set Λ. Then for all R-modules M and for all $\{u_\lambda\} \subseteq M$ there exists a unique R-module homomorphism $\varphi \colon F \to M$ such that $\varphi(e_\lambda) = u_\lambda$ for all $\lambda \in \Lambda$. In terms of diagrams, this is pictured as follows:

$$\begin{tikzcd}
\{e_\lambda\} \arrow[r, hook] \arrow[dr, "e_\lambda \mapsto u_\lambda"'] & F \arrow[d, dashed, "\exists! \varphi"] \\
& M
\end{tikzcd}$$

Using the universal mapping property of free R-modules, let us prove the following theorem:

Theorem 41.1. *If F and G are finite rank free R-modules with basis $e_1, \dots, e_n$ and $f_1, \dots, f_n$ respectively, then $F \cong G$.*

Proof. By the universal mapping property of free R-modules there exists a unique R-module homomorphism $\varphi \colon F \to G$ such that $\varphi(e_i) = f_i$ for all $i = 1, \dots, n$. Similarly, there exists a unique R-module homomorphism $\psi \colon G \to F$ such that $\psi(f_i) = e_i$ for all $i = 1, \dots, n$. In particular, we see that $\psi \circ \varphi \colon F \to F$ satisfies $(\psi \circ \varphi)(e_i) = e_i$. But we also have $1(e_i) = e_i$ for all $i = 1, \dots, n$, where $1 \colon F \to F$ is the identity map. Therefore by uniqueness of the map in the universal mapping property of free R-modules, we must have $\psi \circ \varphi = 1$. A similar argument shows that $\varphi \circ \psi = 1$. $\square$

Corollary 32. *Let F be a free R-module with basis $e_1, \dots, e_n \in F$. Then $F \cong R^n$.*

Remark 58. Note that you can prove Theorem (41.1) without the universal mapping property of free R-modules, but the point is that you'd have to show well-definedness, linearity, etc... of the maps constructed. The point is that all of this is built into the universal mapping property of free R-modules.

41.0.4 Representing R-module Homomorphisms By Matrices

Let F be a R-module with basis $\beta = \{\beta_1, \dots, \beta_m\}$ and let G be a free R-module with basis $\gamma = \{\gamma_1, \dots, \gamma_n\}$. If $v \in F$, then for each $1 \leq i \leq m$, there exists unique $a_i \in R$ such that

$$v = \sum_{i=1}^{m} a_i \beta_i.$$

Since the a_i are uniquely determined, we are justified in making the following definition:

Definition 41.3. The **column representation of** v **with respect to the basis** β, denoted $[v]_\beta$, is defined by

$$[v]_\beta := \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}.$$

Proposition 41.1. *Let* $[\cdot]_\beta \colon V \to R^m$ *be given by*

$$[\cdot]_\beta(v) = [v]_\beta$$

for all $v \in V$. *Then* $[\cdot]_\beta$ *is an isomorphism.*

Proof. We first show that $[\cdot]_\beta$ is R-linear. Let $v_1, v_2 \in V$ and $c_1, c_2 \in R$. Then for each $1 \leq i \leq m$, there exists unique $a_{i1}, a_{i2} \in R$ such that

$$v_1 = \sum_{i=1}^{m} a_{i1}\beta_i \quad \text{and} \quad v_2 = \sum_{i=1}^{m} a_{i2}\beta_i.$$

Therefore we have

$$\begin{aligned} a_1 v_1 + a_2 v_2 &= a_1 \sum_{i=1}^{m} a_{i1}\beta_i + a_2 \sum_{i=1}^{m} a_{i2}\beta_i \\ &= \sum_{i=1}^{m} (a_1 a_{i1} + a_2 a_{i2})\beta_i. \end{aligned}$$

This implies

$$\begin{aligned} [a_1 v_1 + a_2 v_2]_\beta &= \begin{pmatrix} a_1 a_{11} + a_2 a_{12} \\ \vdots \\ a_1 a_{m1} + a_2 a_{m2} \end{pmatrix} \\ &= a_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + a_2 \begin{pmatrix} a_{12} \\ \vdots \\ a_{m2} \end{pmatrix} \\ &= a_1 [v_1]_\beta + a_2 [v_2]_\beta. \end{aligned}$$

Therefore $[\cdot]_\beta$ is linear. To see that $[\cdot]_\beta$ is an isomorphism, note that $[\beta_i] = e_i$, where e_i is the column vector in K^n whose i-th entry is 1 and whose entry everywhere else is 0. Thus, $[\cdot]_\beta$ restricts to a bijection on basis sets

$$[\cdot]_\beta \colon \{\beta_1, \dots, \beta_m\} \to \{e_1, \dots, e_n\},$$

and so it must be an isomorphism. $\square$

41.0.5 Matrix Representation of a Linear Map

Let φ be an R-linear map from F to G. Then for each $1 \leq i \leq m$ and $1 \leq j \leq n$, there exists unique elements $a_{ji} \in R$ such that

$$\varphi(\beta_i) = \sum_{j=1}^{n} a_{ji}\gamma_j \tag{111}$$

for all $1 \leq i \leq m$. Since the a_{ji} are uniquely determined, we are justified in making the following definition:

Definition 41.4. The **matrix representation of** φ **with respect to the bases** β **and** γ, denoted $[\varphi]_\beta^\gamma$, is defined to be the $n \times m$ matrix

$$[\varphi]_\beta^\gamma := \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}.$$

Proposition 41.2. *Let φ be a linear map from F to G. Then*

$$[\varphi]^{\gamma}_{\beta}[v]_{\beta} = [\varphi(v)]_{\gamma}$$

for all $v \in F$.

Remark 59. In terms of diagrams, this proposition says that the following diagram is commutative

$$\begin{array}{ccc} R^m & \xrightarrow{[\varphi]^{\gamma}_{\beta}} & R^n \\ {\scriptstyle [\cdot]_\beta}\uparrow & & \uparrow{\scriptstyle [\cdot]_\gamma} \\ F & \xrightarrow[\varphi]{} & G \end{array}$$

Definition 41.5. Let M be an A-module. M is called of **finite presentation** or **finitely presented** if there exists an $n \times m$-matrix φ such that M is isomorphic to the cokernel of the map $\varphi : A^m \to A^n$. We call φ a **presentation matrix** of M. We write

$$A^m \xrightarrow{\varphi} A^n \longrightarrow M \longrightarrow 0$$

to denote a presentation of M.

Constructive module theory is concerned with modules of finite presentation, that is, with modules which can be given as the cokernel of some matrix. All operations with modules are then represented by operations with the corresponding presentation matrices. We shall see later on that every finitely generated module over a Noetherian ring is finitely presented. As polynomial rings and localizations thereof are Noetherian every finitely generated module over these rings is of finite presentation.

Example 41.3. Let $A = \mathbb{Q}[x, y, z]$ and let M be the submodule of A^2 generated by the column vectors $(xy, yz)^t$ and $(xz, z^2)^t$. This means we have a map

$$\begin{array}{ccc} A^2 & \xrightarrow{\begin{pmatrix} xy & xz \\ yz & z^2 \end{pmatrix}} & M \\ e_1 & \longmapsto & xye_1 + yze_2 \\ e_2 & \longmapsto & xze_1 + z^2e_2 \end{array}$$

To obtain a presentation of N, we need to compute the kernel of this map. The kernel is generated by the column vector $(-z, y)^t$. So $(-z, y)^t$ is the presentation matrix of M.

$$\begin{array}{ccccc} A & \xrightarrow{\begin{pmatrix} -z \\ y \end{pmatrix}} & A^2 & \xrightarrow{\begin{pmatrix} xy & xz \\ yz & z^2 \end{pmatrix}} & M \\ e_1 & \longmapsto & -ze_1 + ye_2 & & \\ & & e_1 & \longmapsto & xye_1 + yze_2 \\ & & e_2 & \longmapsto & xze_1 + z^2e_2 \end{array}$$

Lemma 41.2. *Let M and N be two A-modules with presentations*

$$A^m \xrightarrow{\varphi} A^n \xrightarrow{\pi} M \longrightarrow 0 \quad \text{and} \quad A^r \xrightarrow{\psi} A^s \xrightarrow{\kappa} N \longrightarrow 0.$$

1. *Let $\lambda : M \to N$ be an A-module homomorphism, then there exist A-module homomorphisms $\alpha : A^m \to A^r$ and $\beta : A^n \to A^s$ such that the following diagram commutes:*

$$\begin{array}{ccccccc} A^m & \xrightarrow{\varphi} & A^n & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\lambda} & & \\ A^r & \xrightarrow{\psi} & A^s & \xrightarrow{\kappa} & N & \longrightarrow & 0. \end{array}$$

   that is, $\beta \circ \varphi = \psi \circ \alpha$ and $\lambda \circ \pi = \kappa \circ \beta$.

2. *Let $\beta : A^n \to A^s$ be an A-module homomorphism such that $\beta(Im(\varphi)) \subset Im(\psi)$. Then there exist A-module homomorphisms $\alpha : A^m \to A^r$ and $\lambda : M \to N$ such that the corresponding diagram commutes.*

Proof. (1) : Let $\{e_1, \ldots, e_n\}$ be an A-basis for A^n and choose $x_i \in A^s$ such that $\kappa(x_i) = (\lambda \circ \pi)(e_i)$. We define $\beta(\sum_{i=1}^n a_i e_i) = \sum_{i=1}^n a_i x_i$. Obviously β is an A-module homomorphism and $\lambda \circ \pi = \kappa \circ \beta$. Let $\{f_1, \ldots, f_m\}$ be a basis of A^m. Then $(\kappa \circ \beta \circ \varphi)(f_i) = (\lambda \circ \pi \circ \varphi)(f_i) = 0$, so $\beta(\varphi(f_i)) \in \mathrm{Ker}(\kappa)$. Therefore, there exists $y_i \in A^r$ such that $\psi(y_i) = (\beta \circ \varphi)(f_i)$. We define $\alpha(\sum_{i=1}^n b_n f_i) = \sum_{i=1}^n b_i y_i$. Again α is an A-module homomorphism and $\psi \circ \alpha = \beta \circ \varphi$.

(2) : Define $\lambda(m) = (\kappa \circ \beta)(\tilde{m})$, for some $\tilde{m} \in A^n$ with $\pi(\tilde{m}) = m$. To see that this definition does not depend on the choice of $\tilde{m}$, let $\tilde{m} + \varphi(x)$ be another lift where $x \in A^m$. Then $(\kappa \circ \beta)(\tilde{m} + \varphi(x)) = (\kappa \circ \beta)(\tilde{m}) + (\kappa \circ \beta \circ \varphi)(x) = (\kappa \circ \beta)(\tilde{m})$. Obviously, λ is an A-module homomorphism satisfying $\lambda \circ \pi = \kappa \circ \beta$. We can define α as in (1). □

42 Short Exact Sequences and Splitting Modules

Definition 42.1. A sequence of R-modules and R-linear maps

$$L \xrightarrow{\varphi} M \xrightarrow{\psi} N$$

is called **exact at** M if $\operatorname{im} \varphi = \ker \psi$. A **short exact sequence** is a sequence of R-modules and R-linear maps

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

which is exact at L, M, and N.

42.0.1 Five Lemma

Proposition 42.1. *Suppose the following diagram of R-modules and R-linear maps is commutative with exact rows*

$$\begin{tikzcd}
M_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "\psi_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "\psi_3"] & M_4 \arrow[r, "\varphi_4"] \arrow[d, "\psi_4"] & M_5 \arrow[d, "\psi_5"] \\
M_1' \arrow[r, "\varphi_1'"] & M_2' \arrow[r, "\varphi_2'"] & M_3' \arrow[r, "\varphi_3'"] & M_4' \arrow[r, "\varphi_4'"] & M_5'
\end{tikzcd}$$

1. *If ψ_2, ψ_4 are surjective and ψ_5 is injective, then ψ_3 is surjective.*
2. *If ψ_2, ψ_4 are injective and ψ_1 is surjective, then ψ_3 is injective.*

Proof.

1. Suppose ψ_2, ψ_4 are surjective and ψ_5 is injective and let $u_3' \in M_3'$. Since ψ_4 is surjective, we may choose a $u_4 \in M_4$ such that $\psi_4(u_4) = \varphi_3'(u_3')$. Observe that

$$\begin{aligned}
\psi_5 \varphi_4(u_4) &= \varphi_4' \psi_4(u_4) \\
&= \varphi_4' \varphi_3'(u_3') \\
&= 0.
\end{aligned}$$

It follows that $\varphi_4(u_4) = 0$ since ψ_5 is injective. Therefore we may choose a $u_3 \in M_3$ such that $\varphi_3(u_3) = u_4$ (by exactness of the top row). Now observe that

$$\begin{aligned}
\varphi_3'(u_3' - \psi_3(u_3)) &= \varphi_3'(u_3') - \varphi_3' \psi_3(u_3) \\
&= \psi_4(u_4) - \psi_4 \varphi_3(u_3) \\
&= \psi_4(u_4) - \psi_4(u_4) \\
&= 0.
\end{aligned}$$

Therefore we may choose a $u_2' \in M_2'$ such that $\varphi_2'(u_2') = u_3' - \psi_3(u_3)$ (by exactness of the bottom row). Since ψ_2 is surjective, we may choose a $u_2 \in M_2$ such that $\psi_2(u_2) = u_2'$. Finally we see that

$$\begin{aligned}
\psi_3(\varphi_2(u_2) + u_3) &= \psi_3 \varphi_2(u_2) + \psi_3(u_3) \\
&= \varphi_2' \psi_2(u_2) + \psi_3(u_3) \\
&= \varphi_2'(u_2') + \psi_3(u_3) \\
&= u_3' - \psi_3(u_3) + \psi_3(u_3) \\
&= u_3'.
\end{aligned}$$

It follows that ψ_3 is surjective.

2. Suppose ψ_2, ψ_4 are injective and ψ_1 is surjective and let $u_3 \in \ker \psi_3$. Observe that

$$\begin{aligned} \psi_4\varphi_3(u_3) &= \varphi_3'\psi_3(u_3) \\ &= \varphi_3'(0) \\ &= 0. \end{aligned}$$

It follows that $\varphi_3(u_3) = 0$ since ψ_4 is injective. Therefore we may choose a $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ (by exactness of the top row). Now observe that

$$\begin{aligned} \varphi_2'\psi_2(u_2) &= \psi_3\varphi_2(u_2) \\ &= \psi_3(u_3) \\ &= 0. \end{aligned}$$

Therefore we may choose a $u_1' \in M_1'$ such that $\varphi_1'(u_1') = \psi_2(u_2)$ (by exactness of the bottom row). Since ψ_1 is surjective, we may choose a $u_1 \in M_1$ such that $\psi_1(u_1) = u_1'$. Now observe that

$$\begin{aligned} \psi_2\varphi_1(u_1) &= \varphi_1'\psi_1(u_1) \\ &= \varphi_1'(u_1') \\ &= \psi_2(u_2). \end{aligned}$$

It follows that $\varphi_1(u_1) = u_2$ since ψ_2 is injective. Therefore

$$\begin{aligned} u_3 &= \varphi_2(u_2) \\ &= \varphi_2\varphi_1(u_1) \\ &= 0, \end{aligned}$$

which implies $\ker \psi_3 = 0$. Thus ψ_3 is injective. □

42.0.2 The 3×3 Lemma

Proposition 42.2. *Consider the following diagram*

$$\begin{tikzcd} & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\ 0 \arrow[r] & M_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "\psi_2"] & M_3 \arrow[r] \arrow[d, "\psi_3"] & 0 \\ 0 \arrow[r] & M_1' \arrow[r, "\varphi_1'"] \arrow[d, "\psi_1'"] & M_2' \arrow[r, "\varphi_2'"] \arrow[d, "\psi_2'"] & M_3' \arrow[r] \arrow[d, "\psi_3'"] & 0 \\ 0 \arrow[r] & M_1'' \arrow[r, "\varphi_1''"] \arrow[d] & M_2'' \arrow[r, "\varphi_2''"] \arrow[d] & M_3'' \arrow[r] \arrow[d] & 0 \\ & 0 & 0 & 0 & \end{tikzcd}$$

If the columns and top two rows are exact, then the bottom row is exact.

Proof. We first show φ_1'' is injective. Let $u_1'' \in \ker \varphi_1''$. Since ψ_1' is surjective (by exactness of first column) we may choose a $u_1' \in M_1'$ such that $\psi_1'(u_1') = u_1''$. Then

$$\begin{aligned} \psi_2'\varphi_1'(u_1') &= \varphi_1''\psi_1'(u_1') \\ &= \varphi_1''(u_1'') \\ &= 0 \end{aligned}$$

implies $\varphi_1'(u_1') \in \ker \psi_2'$. Therefore there exists a unique $u_2 \in M_2$ such that $\psi_2(u_2) = \varphi_1'(u_1')$ (by exac Then

$$\begin{aligned} \psi_3\varphi_2(u_2) &= \varphi_2'\psi_2(u_2) \\ &= \varphi_2'\varphi_1'(u_1') \\ &= 0 \end{aligned}$$

implies $\varphi_2(u_2) = 0$ since ψ_3 is injective (by exactness of third column). Thus $u_2 \in \ker \varphi_2$ and so there exists a unique $u_1 \in M_1$ such that $\varphi_1(u_1) = u_2$ (by exactness of first row). Therefore

$$\begin{aligned} \varphi_1'\psi_1(u_1) &= \psi_2\varphi_1(u_1) \\ &= \psi_2(u_2) \\ &= \varphi_1'(u_1') \end{aligned}$$

implies $\psi_1(u_1) = u_1'$ since φ_1' is injective (by exactness of second row). Thus

$$\begin{aligned} u_1'' &= \psi_1'(u_1') \\ &= \psi_1'\psi_1(u_1) \\ &= 0. \end{aligned}$$

Now we show $\ker \varphi_2'' = \operatorname{im} \varphi_1''$. Let $u_2'' \in \ker \varphi_2''$. Since ψ_2' is surjective (by exactness of second colunn), we may choose a $u_2' \in M_2'$ such that $\psi_2'(u_2') = u_2''$. Then

$$\begin{aligned} \psi_3'\varphi_2'(u_2') &= \varphi_2''\psi_2'(u_2') \\ &= \varphi_2''(u_2'') \\ &= 0 \end{aligned}$$

implies $\varphi_2'(u_2') \in \ker \psi_3'$. Therefore there exists a unique $u_3 \in M_3$ such that $\psi_3(u_3) = \varphi_2'(u_2')$ (by exactness of third column). Since φ_2 is surjective, we may choose a $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$. Then

$$\begin{aligned} \varphi_2'(\psi_2(u_2) - u_2') &= \varphi_2'\psi_2(u_2) - \varphi_2'(u_2') \\ &= \psi_3\varphi_2(u_2) - \varphi_2'(u_2') \\ &= \psi_3(u_3) - \varphi_2'(u_2') \\ &= \varphi_2'(u_2') - \varphi_2'(u_2') \\ &= 0 \end{aligned}$$

implies $\psi_2(u_2) - u_2' \in \ker \varphi_2'$. Therefore there exists a uniuqe $u_1' \in M_1'$ such that $\varphi_1'(u_1') = \psi_2(u_2) - u_2'$ (by exactness of second row). Therefore

$$\begin{aligned} \varphi_1''\psi_1'(u_1') &= \psi_2'\varphi_1'(u_1') \\ &= \psi_2'(\psi_2(u_2) - u_2') \\ &= \psi_2'\psi_2(u_2) - \psi_2'(u_2') \\ &= \psi_2'(u_2') \\ &= u_2''. \end{aligned}$$

It follows that $u_2'' \in \operatorname{im} \varphi_1''$. Thus $\ker \varphi_2'' \subseteq \operatorname{im} \varphi_1''$. For the reverse inclusion, let $u_2'' \in M_2''$. Choose $u_1'' \in M_1''$ such that $\varphi_1''(u_1'') = u_2''$. Since ψ_1' is surjective (by exactness of first column), we may choose a $u_1' \in M_1'$ such that $\psi_1'(u_1') = u_1''$. Then

$$\begin{aligned} 0 &= \psi_3'\varphi_2'\varphi_1'(u_1') \\ &= \varphi_2''\psi_2'\varphi_1'(u_1') \\ &= \varphi_2''\varphi_1''\psi_1'(u_1') \\ &= \varphi_2''\varphi_1''(u_1'') \\ &= \varphi_2''(u_2'') \end{aligned}$$

implies $u_2'' \in \ker \varphi_2''$. Thus $\ker \varphi_2'' \supseteq \operatorname{im} \varphi_1''$.

The last step is to show φ_2'' is surjective. Let $u_3'' \in M_3''$. Since ψ_3' is surjective (by exactness of third column), we may choose a $u_3' \in M_3'$ such that $\psi_3'(u_3') = u_3''$. Since φ_2' is surjective (by exactness of second row), we may choose a $u_2' \in M_2'$ such that $\varphi_2'(u_2') = u_3'$. Then

$$\begin{aligned} \varphi_2''\psi_2'(u_2') &= \psi_3'\varphi_2'(u_2') \\ &= \psi_3'(u_3') \\ &= u_3'' \end{aligned}$$

implies φ_2'' is surjective. $\square$

42.0.3 The Snake Lemma

Proposition 42.3. *Consider the following commutative diagram with exact rows*

$$\begin{tikzcd} & M_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "\psi_2"] & M_3 \arrow[r] \arrow[d, "\psi_3"] & 0 \\ 0 \arrow[r] & M_1' \arrow[r, "\varphi_1'"] & M_2' \arrow[r, "\varphi_2'"] & M_3' & \end{tikzcd} \tag{112}$$

Then there exists an exact sequence

$$\ker\psi_1 \xrightarrow{\widetilde{\varphi_1}} \ker\psi_2 \xrightarrow{\widetilde{\varphi_2}} \ker\psi_3 \xrightarrow{\partial} \operatorname{coker}\psi_1 \xrightarrow{\overline{\varphi_1'}} \operatorname{coker}\psi_2 \xrightarrow{\overline{\varphi_2'}} \operatorname{coker}\psi_3. \tag{113}$$

Moreover, if φ_1 is injective, then $\widetilde{\varphi_1}$ is injective; and if φ_2' is surjective, then $\overline{\varphi_2'}$ is surjective.

Proof.

Step 1: We first define the maps in question. Define $\widetilde{\varphi_1}\colon \ker\psi_1 \to \ker\psi_2$ by

$$\widetilde{\varphi_1}(u_1) = \varphi_1(u_1)$$

for all $u_1 \in \ker\psi_1$. Note that $\widetilde{\varphi_1}$ lands in $\ker\psi_2$ by the commutativity of the diagram. Indeed,

$$\begin{aligned} \psi_2\widetilde{\varphi_1}(u_1) &= \psi_2\varphi_1(u_1) \\ &= \varphi_1'\psi_1(u_1) \\ &= \varphi_1'(0) \\ &= 0 \end{aligned}$$

implies $\widetilde{\varphi_1}(u_1) \in \ker\psi_2$ for all $u_1 \in \ker\psi_1$. Also note that $\widetilde{\varphi_1}$ is an R-module homomorphism since φ_1 is an R-module homomorphism. Similarly, we define $\widetilde{\varphi_2}\colon \ker\psi_2 \to \ker\psi_3$ by

$$\widetilde{\varphi_2}(u_2) = \varphi_2(u_2)$$

for all $u_2 \in \ker\psi_2$.

Next we define $\partial\colon \ker\psi_3 \to \operatorname{coker}\psi_1$ as follows: let $u_3 \in \ker\psi_3$. Choose $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ (such an element exists because φ_2 is surjective by exactness of the first row). By the commutativity of the diagram, we have

$$\begin{aligned} \varphi_2'\psi_2(u_2) &= \psi_3\varphi_2(u_2) \\ &= \psi_3(u_3) \\ &= 0. \end{aligned}$$

It follows that $\psi_2(u_2) \in \ker\varphi_2'$. Therefore there exists a unique $u_1' \in M_1'$ such that $\varphi_1'(u_1') = \psi_2(u_2)$ (by exactness of the second row). We set

$$\partial(u_3) = \overline{u_1'}$$

where $\overline{u_1'}$ is the coset in $\operatorname{coker}\psi_1$ with u_1' as a representative. We must check that ∂ defined in this is in fact a well-defined map. There was one choice that we made in our construction, namely the lift of u_3 under φ_2 to u_2. So let v_2 be another element in M_2 such that $\varphi_2(v_2) = u_3$. Denote by v_1' to be the unique element in M_1' such that $\varphi_1'(v_1') = \psi_2(v_2)$. We must show that $\overline{u_1'} = \overline{v_1'}$ in $\operatorname{coker}\psi_1$. In other words, we must show that $v_1' - u_1' \in \operatorname{im}\psi_1$. Observe that

$$\begin{aligned} \varphi_2(v_2 - u_2) &= \varphi_2(v_2) - \varphi_2(u_2) \\ &= u_3 - u_3 \\ &= 0 \end{aligned}$$

implies $v_2 - u_2 \in \ker\varphi_2$. It follows that there exists a unique element $u_1 \in M_1$ such that $\varphi_1(u_1) = v_2 - u_2$ (by exactness of the first row). Then

$$\begin{aligned} \varphi_1'\psi_1(u_1) &= \psi_2\varphi_1(u_1) \\ &= \psi_2(v_2 - u_2) \\ &= \psi_2(v_2) - \psi_2(u_2) \\ &= \varphi_1'(v_1') - \varphi_1'(u_1') \\ &= \varphi_1'(v_1' - u_1') \end{aligned}$$

implies $\psi_1(u_1) = v_1' - u_1'$ since φ_1' is injective (by exactness of the second row). It follows that $v_1' - u_1' \in \operatorname{im}\psi_1$, and hence ∂ is well-defined.

Finally, we define $\overline{\varphi_1'}\colon \operatorname{coker}\psi_1 \to \operatorname{coker}\psi_2$ by

$$\overline{\varphi_1'}(\overline{u_1'}) = \overline{\varphi_1'(u_1')}$$

for all $\overline{u_1'} \in \operatorname{coker}\psi_1$. The map $\overline{\varphi_1'}$ is well-defined by the commutativity of the diagram. Indeed, let v_1' be another representative of the coset $\overline{u_1'}$ in $\operatorname{coker}\psi_1$. Choose $u_1 \in M_1$ such that $v_1' - u_1' = \psi_1(u_1)$. Then

$$\begin{aligned}\psi_2\varphi_1(u_1) &= \varphi_1'\psi_1(u_1)\\ &= \varphi_1'(v_1' - u_1')\\ &= \varphi_1'(v_1') - \varphi_1'(u_1').\end{aligned}$$

It follows that $\varphi_1'(v_1') - \varphi_1'(u_1') \in \operatorname{im}\psi_2$, and hence $\varphi_1'(v_1')$ and $\varphi_1'(u_1')$ represent the same coset in $\operatorname{coker}\psi_2$. Similarly, we define $\overline{\varphi_2'}\colon \operatorname{coker}\psi_2 \to \operatorname{coker}\psi_3$ by

$$\overline{\varphi_2'}(\overline{u_2'}) = \overline{\varphi_2'(u_2')}$$

for all $\overline{u_2'} \in \operatorname{coker}\psi_2$.

Step 2: Now that we've defined the maps in question, we will now show that the sequence (310) is exact as well as prove the "moreover" part of the proposition. First we show exactness at $\ker\psi_2$. Observe that

$$\begin{aligned}\widetilde{\varphi_2}\widetilde{\varphi_1}(u_1) &= \varphi_2\varphi_1(u_1)\\ &= 0\end{aligned}$$

for all $u_1 \in \ker\psi_1$. It follows that $\ker\widetilde{\varphi_2} \supseteq \operatorname{im}\widetilde{\varphi_1}$. Conversely, let $u_2 \in \ker\widetilde{\varphi_2}$. Thus $u_2 \in \ker\varphi_2 \cap \ker\psi_2$. By exactness of the top row in (309), we may choose a $u_1 \in M_1$ such that $\varphi_1(u_1) = u_2$. Moreover,

$$\begin{aligned}\varphi_1'\psi_1(u_1) &= \psi_2\varphi_1(u_1)\\ &= \psi_2(u_2)\\ &= 0\end{aligned}$$

implies $\psi_1(u_1) = 0$ since φ_1' is injective (by exactness of the bottom row in (309)). Therefore $u_1 \in \ker\psi_1$, and so $u_2 \in \operatorname{im}\widetilde{\varphi_1}$. Thus $\ker\widetilde{\varphi_2} \subseteq \operatorname{im}\widetilde{\varphi_1}$.

Next we show exactness at $\ker\psi_3$: let $u_3 \in \ker\partial$. Choose $u_2 \in M_2$ and $u_1' \in M_1'$ such that $\varphi_2(u_2) = u_3$ and $\varphi_1'(u_1') = \psi_2(u_2)$. Then

$$\begin{aligned}0 &= \partial(u_3)\\ &= \overline{u_1'}\end{aligned}$$

implies $u_1' \in \operatorname{im}\psi_1$. Choose $u_1 \in M_1$ such that $\psi_1(u_1) = u_1'$. Then

$$\begin{aligned}\psi_2(u_2 - \varphi_1(u_1)) &= \psi_2(u_2) - \psi_2\varphi_1(u_1)\\ &= \psi_2(u_2) - \varphi_1'\psi_1(u_1)\\ &= \psi_2(u_2) - \varphi_1'(u_1')\\ &= \psi_2(u_2) - \psi_2(u_2)\\ &= 0\end{aligned}$$

implies $u_2 - \varphi_1(u_1) \in \ker\psi_2$. Furthermore, we have

$$\begin{aligned}\varphi_2(u_2 - \varphi_1(u_1)) &= \varphi_2(u_2) - \varphi_2\varphi_1(u_1)\\ &= \varphi_2(u_2)\\ &= u_3.\end{aligned}$$

It follows that $u_3 \in \operatorname{im}\widetilde{\varphi_2}$. Thus $\ker\partial \subseteq \operatorname{im}\widetilde{\varphi_2}$. Convsersely, let $u_3 \in \operatorname{im}\widetilde{\varphi_2}$. Choose $u_2 \in \ker\psi_2$ such that $\varphi_2(u_2) = u_3$. Then $0 \in M_1'$ is the unique element in M_1' which maps to $\psi_2(u_2) = 0$. Thus $\partial(u_3) = \overline{0}$ which implies $\ker\partial \supseteq \operatorname{im}\widetilde{\varphi_2}$.

Next we show exactness at $\operatorname{coker}\psi_1$: let $\overline{u_1'} \in \ker\overline{\varphi_1'}$. Then $\varphi_1'(u_1') = \psi_2(u_2)$ for some $u_2 \in M_2$. Moreover,

$$\begin{aligned}\psi_3\varphi_2(u_2) &= \varphi_2'\psi_2(u_2)\\ &= \varphi_2'\varphi_1'(u_1')\\ &= 0\end{aligned}$$

implies $\varphi_2(u_2) \in \ker \psi_3$. Also we have $\partial(\varphi_2(u_2)) = \overline{u_1'}$, and so $\overline{u_1'} \in \operatorname{im}\partial$. Thus $\ker \overline{\varphi}_1' \subseteq \operatorname{im}\partial$. Conversely, let $\overline{u_1'} \in \operatorname{im}\partial$. Choose $u_3 \in M_3$ and $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ and $\psi_2(u_2) = \varphi_1'(u_1')$. It follows that

$$\begin{aligned}
\overline{\varphi_1'}(\overline{u_1'}) &= \overline{\varphi_1'(u_1')} \\
&= \overline{\psi_2(u_2)} \\
&= \overline{0}
\end{aligned}$$

in $\operatorname{coker}\psi_2$. Thus $\ker \overline{\varphi_1'} \supseteq \operatorname{im}\partial$.

Next we check exactness at $\operatorname{coker}\psi_2$: let $\overline{u_2'} \in \ker \overline{\varphi_2'}$. Choose $u_3 \in M_3$ such that $\psi_3(u_3) = \varphi_2'(u_2')$ and choose $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$. Since

$$\begin{aligned}
\varphi_2'(u_2' - \psi_2(u_2)) &= \varphi_2'(u_2') - \varphi_2'\psi_2(u_2) \\
&= \varphi_2'(u_2') - \psi_3\varphi_2(u_2) \\
&= \varphi_2'(u_2') - \psi_3(u_3) \\
&= \varphi_2'(u_2') - \varphi_2'(u_2') \\
&= 0,
\end{aligned}$$

it follows that $u_2' - \psi_2(u_2) \in \ker \varphi_2'$. Therefore there exists a unique $u_1' \in M_1'$ such that $\varphi_1'(u_1') = u_2' - \psi_2(u_2)$ (by exactness of the bottom row in (309)). Then

$$\begin{aligned}
\overline{\varphi_1'}(\overline{u_1'}) &= \overline{\varphi_1'(u_1')} \\
&= \overline{u_2' - \psi_2(u_2)} \\
&= \overline{u_2'}
\end{aligned}$$

in $\operatorname{coker}\psi_2$. It follows that $\overline{u_2'} \in \operatorname{im}\overline{\varphi_2'}$ and hence $\ker \overline{\varphi_2'} \subseteq \operatorname{im}\overline{\varphi_1'}$. Conversely, let $\overline{u_2'} \in \operatorname{im}\overline{\varphi_2'}$. Choose $u_1' \in M_1'$ such that $\varphi_1'(u_1') = u_2'$. Then

$$\begin{aligned}
0 &= \varphi_2'\varphi_1'(u_1') \\
&= \varphi_2'(u_2')
\end{aligned}$$

implies $u_2' \in \ker \varphi_2$. Therefore $\overline{\varphi_2'}(\overline{u_2'}) = \overline{0}$ in $\operatorname{coker}\psi_3$, and it follows that $\ker \overline{\varphi_2'} \supseteq \operatorname{im}\overline{\varphi_1'}$.

Finally, we prove the moreover part of this proposition. Suppose that φ_1 is injective. We want to show that $\widetilde{\varphi_1}$ is injective. Let $u_1 \in \ker \widetilde{\varphi_1}$. Then

$$\begin{aligned}
0 &= \widetilde{\varphi_1}(u_1) \\
&= \varphi_1(u_1)
\end{aligned}$$

implies $u_1 = 0$ since φ_1 is injective. It follows that $\widetilde{\varphi_1}$ is injective. Now suppose that φ_2' is surjective. We want to show that $\overline{\varphi_2'}$ is surjective. Let $\overline{u_3'} \in \operatorname{coker}\psi_3$. Since φ_2' is surjective, we may choose a $u_2' \in M_2'$ such that $\varphi_2'(u_2') = u_3'$. Then

$$\begin{aligned}
\overline{\varphi_2'}(\overline{u_2'}) &= \overline{\varphi_2'(u_2')} \\
&= \overline{u_3'}.
\end{aligned}$$

It follows that $\overline{\varphi_2'}$ is surjective. □

42.0.4 Split Short Exact Sequences

Let M be an R-module and let N be an R-submodule of M. Then

$$0 \longrightarrow N \hookrightarrow M \longrightarrow M/N \longrightarrow 0 \tag{114}$$

is a short exact sequence. It turns out that a short exact sequence like (**??**) is isomorphic to a short exact sequence like (114) in the following way:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "f"] \arrow[d] & M \arrow[r, "g"] \arrow[d, "id"] & P \arrow[r] \arrow[d, "\varphi"] & 0 \\
0 \arrow[r] & f(N) \arrow[r, hook] & M \arrow[r] & M/f(N) \arrow[r] & 0
\end{tikzcd}$$

where the unlabled arrows are the obvious ones and φ is defined as follows: Given $p \in P$, choose $\widetilde{p} \in M$ such that $g(\widetilde{p}) = p$. Then set $\varphi(p) = \overline{\widetilde{p}}$. This is well-defined since if $\widetilde{p}' \in M$ was another lift of p, then $g(\widetilde{p} - \widetilde{p}') = 0$ implies $\widetilde{p} - \widetilde{p}' \in \operatorname{Ker}(g) = \operatorname{Im}(f)$. So $\widetilde{p}' = f(k) + \widetilde{p}$ for some $k \in K$, and hence $\overline{\widetilde{p}'} = \overline{f(k) + \widetilde{p}} = \overline{\widetilde{p}}$. It is also easy to verify that all vertical arrows are in fact A-module isomorphisms.

Example 42.1. Let I and J be ideals in R such that $I + J = R$. Then there is a short exact sequence of R-modules given by

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I \cap J & \xrightarrow{\varphi} & I \oplus J & \xrightarrow{\psi} & R & \longrightarrow & 0 \\ & & x & \longmapsto & (x, -x) & & & & \\ & & & & (i, j) & \longmapsto & i + j & & \end{array}$$

Definition 42.2. A short exact sequence

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

is called **split** when there is an R-module isomorphism $\theta \colon M \to L \oplus N$ such that the diagram

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}"] & M \arrow[r, "\psi"] \arrow[d, "\theta"] & N \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ 0 \arrow[r] & L \arrow[r, "\iota_1"] & L \oplus N \arrow[r, "\pi_2"] & N \arrow[r] & 0 \end{tikzcd}$$

commutes, where the bottom maps to and from the direct sum are the standard embedding and projection; that is

$$\iota_1(u) = (u, 0) \quad \text{and} \quad \pi_2(u, v) = v$$

for all $u \in L$ and $(u, v) \in N$.

Theorem 42.1. *Let*

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

be a short exact sequence of R-modules. The following are equivalent:

1. *There is an R-linear map $\widetilde{\varphi} \colon M \to L$ such that $\widetilde{\varphi}\varphi(u) = u$ for all $u \in L$.*
2. *There is an R-linear map $\widetilde{\psi} \colon N \to M$ such that $\psi\widetilde{\psi}(w) = w$ for all $w \in N$.*
3. *The short exact sequence splits.*

Proof. We first show that (2) and (3) are equivalent. One direction is easy, so let us prove the other one. Suppose $\widetilde{\psi} \colon N \to M$ is an R-linear map such that $\psi\widetilde{\psi}(w) = w$ for all $w \in N$. Define $\vartheta \colon L \oplus N \to M$ by

$$\vartheta(u, w) = \varphi(u) + \widetilde{\psi}(w)$$

for all $(u, w) \in L \oplus N$. The map ϑ is easily checked to be R-linear. We claim it is an isomorphism. Indeed, we first show that it is injective. Suppose $(u, w) \in \ker\vartheta$. Then $-\widetilde{\psi}(w) = \varphi(u)$. Therefore

$$\begin{aligned} 0 &= -\psi\varphi(u) \\ &= \psi\widetilde{\psi}(u)) \\ &= u, \end{aligned}$$

which also implies

$$\begin{aligned} 0 &= -\psi\varphi(0) \\ &= -\psi\varphi(u) \\ &= \psi\widetilde{\psi}(w) \\ &= w, \end{aligned}$$

and so $(u, w) = (0, 0)$. It follows that ϑ is injective.

Now we will show ϑ is surjective. Let $v \in M$. Observe that

$$\begin{aligned}\psi(v - \widetilde{\psi}\psi(v)) &= \psi(v) - \psi\widetilde{\psi}\psi(v)) \\ &= \psi(v) - \psi(v) \\ &= 0.\end{aligned}$$

It follows that $v - \widetilde{\psi}\psi(v) \in \ker \psi$. So we may choose a $u \in L$ such that $\varphi(u) = v - \widetilde{\psi}\psi(v)$ by exactness of the short exact sequence. Then $(u, \psi(v)) \in L \oplus N$, and moreover we have

$$\begin{aligned}\vartheta(u, \psi(v)) &= \varphi(u) + \widetilde{\psi}\psi(v) \\ &= v - \widetilde{\psi}\psi(v) + \widetilde{\psi}\psi(v) \\ &= v.\end{aligned}$$

It follows that ϑ is surjective. Thus $\vartheta^{-1} \colon L \oplus N \to M$ is an isomorphism. It remains to check that ϑ^{-1} splits the short exact sequence. Let $u \in L$. Then u is the unique element in L which maps to $\varphi(u)$ under φ, and so

$$\begin{aligned}\vartheta^{-1}\varphi(u) &= (u, \psi\varphi(u)) \\ &= (u, 0) \\ &= \iota_1(u).\end{aligned}$$

Thus the left square commutes. Similarly, let $v \in M$ and let u be the unique element in L such that $\varphi(u) = v - \widetilde{\psi}\psi(v)$. Then

$$\begin{aligned}\pi_2\vartheta^{-1}(v) &= \pi_2(u, \psi(v)) \\ &= \psi(v).\end{aligned}$$

Thus the right square commutes too. This concludes the proof that (2) and (3) are equivalent.

Now we will show that (1) and (3) are equivalent. One direction is easy, so let us prove the other one. Suppose $\widetilde{\varphi} \colon M \to L$ is an R-linear map such that $\widetilde{\varphi}\varphi(u) = u$ for all $u \in L$. Define a map $\theta \colon M \to L \oplus N$ by

$$\theta(v) = (\widetilde{\varphi}(v), \psi(v))$$

for all $v \in M$. The map θ is easily checked to be R-linear. We claim it is an isomorphism. Indeed, we first show that it is injective. Suppose $v \in \ker\theta$. Then $\widetilde{\varphi}(v) = 0$ and $\psi(v) = 0$. So we may choose a $u \in L$ such that $\varphi(u) = v$ by exactness of the short exact sequence. Then

$$\begin{aligned}0 &= \varphi\widetilde{\varphi}(v) \\ &= \varphi\widetilde{\varphi}\varphi(u) \\ &= \varphi(u) \\ &= v.\end{aligned}$$

It follows that θ is injective.

Now we will show θ is surjective. Let $(u, w) \in L \oplus N$. Since ψ is surjective, we may choose a $v \in M$ such that $\psi(v) = w$. Then $v + \varphi(u - \widetilde{\varphi}(v)) \in M$ and we have

$$\begin{aligned}\theta(v + \varphi(u - \widetilde{\varphi}(v))) &= (\widetilde{\varphi}(v + \varphi(u - \widetilde{\varphi}(v))), \psi(v + \varphi(u - \widetilde{\varphi}(v))) \\ &= (\widetilde{\varphi}(v) + \widetilde{\varphi}\varphi(u) - \widetilde{\varphi}\varphi\widetilde{\varphi}(v), \psi(v) + \psi\varphi(u) - \psi\varphi\widetilde{\varphi}(v)) \\ &= (\widetilde{\varphi}(v) + u - \widetilde{\varphi}(v), \psi(v)) \\ &= (u, w).\end{aligned}$$

It follows that θ is surjective. □

We want to stress that being split is not just saying that there is an isomorphism $M \to L \oplus N$ of R-modules, but *how* the isomorphism works with the maps f and g in the exact sequence: The commutativity of the diagram says $\varphi \colon L \to M$ behaves like the standard embedding $\iota_1 \colon L \to L \oplus N$ and $\psi \colon M \to N$ behaves like the standard projection $\pi_2 \colon L \oplus N \to N$. Here is an example of a short exact sequece which does not split, even though we have $M \cong L \oplus N$.

Example 42.2. Define $\varphi \colon \mathbb{Z} \to \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ by

$$\varphi(a) = (2a, 0)$$

for all $a \in \mathbb{Z}$ and define $\psi \colon \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ by

$$\psi(a, \overline{a_1}, \overline{a_2}, \dots) = (\overline{a}, \overline{a_1}, \overline{a_2}, \dots)$$

for all $(a, \overline{a_1}, \overline{a_2}, \dots) \in \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. Then

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \xrightarrow{\psi} (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \longrightarrow 0$$

is a short exact sequence which does not split. Indeed, assume for a contradiction that it did split. Then there exists an R-linear map $\widetilde{\psi}\colon (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ such that $\psi\widetilde{\psi} = 1$. Let $\pi_1\colon \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z}$ be and $\pi_2\colon \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ be the natural projection maps and denote $\pi_1 \circ \widetilde{\psi} = \widetilde{\psi}_1$ and $\pi_2 \circ \widetilde{\psi} = \widetilde{\psi}_2$. First note that $\widetilde{\psi}_1\colon (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z}$ must be the zero map since 2 is a nonzerodivisor on $\mathbb{Z}$ and $2 \in \operatorname{Ann}((\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}})$. Indeed, we have

$$\begin{aligned}
2\widetilde{\psi}_1((\overline{a_n})) &= \widetilde{\psi}_1((\overline{2a_n})) \\
&= \widetilde{\psi}_1(0) \\
&= 0
\end{aligned}$$

implies $\widetilde{\psi}_1((\overline{a_n})) = 0$ for all $(\overline{a_n}) \in (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. Now let $(\overline{a_n}) \in (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ with $\overline{a_1} = \overline{1}$ and denote $(b_n) = \widetilde{\psi}_2((\overline{a_n}))$. Then

$$\begin{aligned}
(\overline{a_n}) &= \psi\widetilde{\psi}((\overline{a_n})) \\
&= \psi(\widetilde{\psi}_1((\overline{a_n})), \widetilde{\psi}_2((\overline{a_n}))) \\
&= \psi(0, (b_n)) \\
&= (\overline{0}, \overline{b_1}, \overline{b_2}, \dots).
\end{aligned}$$

This is a contradiction since $\overline{a_1} = \overline{1}$.

Example 42.3. Let I and J be ideals in R such that $I + J = R$. Then the short exact sequence given in Example (42.1) splits. Indeed, choose $x \in I$ and $y \in J$ such that $x + y = 1$. Define $\widetilde{\psi}\colon R \to I \oplus J$ by

$$\widetilde{\psi}(a) = (ax, ay)$$

for all $a \in R$. The map $\widetilde{\psi}$ is easily checked to be an R-linear map. Moreover, we have

$$\begin{aligned}
\psi\widetilde{\psi}(a) &= \psi(ax, ay) \\
&= ax + ay \\
&= a(x + y) \\
&= a
\end{aligned}$$

for all $a \in R$. Therefore $\widetilde{\psi}$ splits this short exact sequence. In particular, we obtain an isomorphism

$$(I \cap J) \oplus R \cong I \oplus J,$$

where the addition map $I \oplus J \to R$ can now be viewed as a projection $(I \cap J) \oplus R \to R$.

If $I \cap J$ happens to be a principal ideal in R, say $I \cap J = \langle x \rangle$, then there is an R-module isomorphism $\mu_x\colon R \to I \cap J$ given by

$$\mu_x(a) = xa$$

for all $a \in R$. In particular, we obtain a sequence of isomorphisms

$$R \oplus R \cong (I \cap J) \oplus R \cong I \oplus J.$$

For example, in $\mathbb{Z}[\sqrt{-5}]$ we have

$$\mathbb{Z}[\sqrt{-5}] \oplus \mathbb{Z}[\sqrt{-5}] \cong \langle 3, 1 + \sqrt{-5} \rangle \oplus \langle 3, 1 - \sqrt{-5} \rangle.$$

42.0.5 Splicing Short Exact Sequences Together

Proposition 42.4. *Suppose for each $i \in \mathbb{Z}$, we are given short exact sequences of the form*

$$0 \longrightarrow K_i \xrightarrow{\phi_i} M_i \xrightarrow{\psi_i} K_{i-1} \longrightarrow 0 \tag{115}$$

Then we can splice these short exact sequences together to get a long exact sequence of the form

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots \tag{116}$$

where $\varphi_i = \phi_{i-1} \circ \psi_i$.

Proof. It follows the short exact sequences (313) that

$$\begin{aligned}\ker\varphi_i &= \ker(\phi_{i-1}\circ\psi_i)\\ &= \ker\psi_i\\ &= \operatorname{im}\phi_i\\ &= \operatorname{im}(\phi_i\circ\psi_{i+1})\\ &= \operatorname{im}\varphi_{i+1}.\end{aligned}$$

It follows that (314) is exact. □

Corollary 33. *Every long exact of R-modules can be formed by splicing together suitable short exact sequences.*

Proof. Let

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots \tag{117}$$

be an exact sequence of R-modules. For each $i \in \mathbb{Z}$, we break (315) into short exact sequences of the form

$$0 \longrightarrow \ker\varphi_i \xrightarrow{\iota_i} M_i \xrightarrow{\widetilde{\varphi}_i} \operatorname{im}\varphi_i \longrightarrow 0 \tag{118}$$

where ι_i is the inclusion map and $\widetilde{\varphi}_i$ is just φ_i but with range $\operatorname{im}\varphi_i$ rather than M_{i-1}. In fact, since $\ker\varphi_{i-1} = \operatorname{im}\varphi_i$, we can rewrite (317) as

$$0 \longrightarrow \ker\varphi_i \xrightarrow{\iota_i} M_i \xrightarrow{\varphi_i} \ker\varphi_{i-1} \longrightarrow 0 \tag{119}$$

Since $\varphi_i = \iota_{i-1}\circ\widetilde{\varphi}_i$, it follows from Proposition (76.2) that splicing these short exact sequences together gives us our original long exact sequence (315) . □

42.1 Pullbacks and Pushouts

Proposition 42.5. *Let M, N, and P be R-modules, let $\psi\colon N \to M$ be an R-linear map, and let $\varphi\colon P \twoheadrightarrow M$ be a surjective R-linear map. Define the* ***pullback of*** $\psi\colon N\to M$ ***and*** $\varphi\colon P\twoheadrightarrow M$ *to be the R-module*

$$N\times_M P = \{(u,v)\in N\times P \mid \psi(u) = \varphi(v)\}$$

equipped with the R-linear maps $\pi_1\colon N\times_M P\to N$ and $\pi_2\colon N\times_M P \to P$ given by

$$\pi_1(u,v) = u \quad \textit{and} \quad \pi_2(u,v) = v$$

for all $(u,v)\in N\times_M P$. Then there exists an isomorphism $\overline{\varphi}\colon P/\pi_1(N\times_M P)\to M/N$ given by

$$\overline{\varphi}(\overline{v}) = \overline{\varphi(v)}$$

for all $\overline{v}\in P/\pi_1(N\times_M P)$. Moreover, the following diagram commutative

$$\begin{tikzcd} N\times_M P \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & P \arrow[r] \arrow[d, "\varphi"] & P/\pi_1(N\times_M P) \arrow[r] \arrow[d, "\overline{\varphi}"] & 0 \\ N \arrow[r, "\psi"] & M \arrow[r] & M/\psi(N) \arrow[r] & 0 \end{tikzcd}$$

Proof. We first need to check that $\overline{\varphi}$ is well-defined. Suppose $v+v'$ is another representative of $\overline{v}$ where $v'\in \operatorname{im}(\pi_2)$. Choose $(u',v')\in N\times_M P$ such that $\pi_1(u',v') = v'$ (so $\varphi(v')=\psi(u')$). Then

$$\begin{aligned}\overline{\varphi}(\overline{v+v'}) &= \overline{\varphi(v+v')}\\ &= \overline{\varphi(v)+\varphi(v')}\\ &= \overline{\varphi(v)+\psi(u')}\\ &= \overline{\varphi(v)}.\end{aligned}$$

Thus $\overline{\varphi}$ is well-defined. Clearly, $\overline{\varphi}$ is a surjective R-linear map since φ is a surjective R-linear map. It remains to show that $\overline{\varphi}$ is injective. Suppose $\overline{v}\in\ker\overline{\varphi}$. Then $\varphi(v)\in\operatorname{im}\psi$. Choose $u\in N$ such that $\psi(u)=\varphi(v)$. Then $(u,v)\in N\times_M P$ and $v = \pi_2(u,v)$. It follows that $\overline{v}=0$ in $P/\pi_2(N\times_M P)$. □

Proposition 42.6. *Let M, N, and E be R-modules, let $\psi\colon M \to N$ be an R-linear map, and let $\varphi\colon M \to E$ be an injective R-linear map. Define the* ***pushout of*** $\psi\colon M \to N$ ***and*** $\varphi\colon M \to E$ *to be the R-module*

$$E +_M N = E \times N / \{(\psi(w), -\varphi(w)) \mid w \in M\}$$

equipped with the R-linear maps $\iota_1\colon E \to E +_M N$ and $\iota_2\colon N \to E +_M N$ given by

$$\iota_1(u) = (u, 0) \quad \text{and} \quad \iota_2(v) = (0, v)$$

for all $u \in E$ and $v \in N$. Then φ restricts to an isomorphism $\varphi|_{\ker\psi}\colon \ker\psi \to \ker\iota_1$. Moreover, the following diagram commutative is commutative

$$\begin{tikzcd}
0 \arrow[r] & \ker\psi \arrow[r] \arrow[d, "\varphi|_{\ker\psi}"] & M \arrow[r, "\psi"] \arrow[d, "\varphi"] & N \arrow[d, "\iota_2"] \\
0 \arrow[r] & \ker\iota_1 \arrow[r] & E \arrow[r, "\iota_1"] & E +_M N
\end{tikzcd}$$

Proof. We first need to check that the restriction of φ to $\ker\psi$ lands in $\ker\iota_1$. Suppose $w \in \ker\psi$. Then observe that

$$\begin{aligned}
\iota_1\varphi(w) &= [\varphi(w), 0] \\
&= [0, -\psi(w)] \\
&= [0, 0],
\end{aligned}$$

where we write $[u, v]$ for the equivalence class of (u, v) in $E +_M N$. It follows that $\varphi(w) \in \ker\iota_1$. Thus the map $\varphi|_{\ker\psi}\colon \ker\psi \to \ker\iota_1$ makes sense.

Clearly, $\varphi|_{\ker\psi}$ is an injective R-linear map since φ is an injective R-linear map. It remains to show that $\varphi|_{\ker\psi}$ is surjective. Suppose $u \in \ker\iota_1$ (so $[u, 0] = [0, 0]$). This implies that there exists a $w \in M$ such that $u = \varphi(w)$ and $\psi(w) = 0$. In other words, this implies the map $\varphi|_{\ker\psi}$ is surjective. □

43 Modules over a PID

43.1 Annihilators and Torsion

Definition 43.1. Let R be an integral domain, let M be an R-module, and let $u \in M$. We define the **annihilator** of u to be

$$0 :_R u = \{a \in R \mid au = 0\}.$$

We say $0 :_R u$ is the set of all elements in R which **kills** u. If $0 :_R u \neq 0$, then we say u is a **torsion element** of M. We denote by M_{tor} to be the set of all torsion elements of M. We say M is **torsion-free** if $M_{\text{tor}} = 0$, that is, the only torsion element of M is 0. We say M is **torsion** if $M_{\text{tor}} = M$, that is, every element in M is a torsion element.

Proposition 43.1. *Let R be an integral domain, let M be an R-module, and let $u \in M$. Then $0 :_R u$ is an ideal of R and M_{tor} is a R-submodule of M.*

Proof. We first show that $0 :_R u$ is an ideal of R. Observe that $0 \in 0 :_R u$ which implies $0 :_R u$ is nonempty. Let $x, y \in 0 :_R u$ and let $a \in R$. Then

$$\begin{aligned}
(ax + y)u &= axu + yu \\
&= 0 + 0 \\
&= 0
\end{aligned}$$

implies $ax + y \in 0 :_R u$. It follows that $0 :_R u$ is an ideal of R.

Now we will show that M_{tor} is an R-submodule of M. Observe that $0 \in M_{\text{tor}}$ which implies M_{tor} is nonempty. Let $u, v \in M_{\text{tor}}$ and let $a \in R$. Choose $x, y \in R \backslash \{0\}$ such that $xu = 0$ and $yv = 0$. Then $xy \neq 0$ since R is an integral domain, and moreover we have

$$\begin{aligned}
xy(au + v) &= xyau + xyv \\
&= ya(xu) + x(yv) \\
&= 0 + 0 \\
&= 0,
\end{aligned}$$

which implies $0 :_R (au + v) \neq 0$. It follows that $au + v \in M_{\text{tor}}$, which implies M_{tor} is an R-submodule of M. □

Proposition 43.2. *Let R be a PID, let p be a prime in R, let M be an R-module, and let $u \in M$. Suppose $p^k u = 0$ for some $k \geq 0$. Then*

$$0 :_R u = \langle p^i \rangle$$

for some $0 \leq i \leq k$.

Proof. Choose $i \geq 0$ to be the smallest integer such that $p^i u = 0$. We claim that $\langle p^i \rangle = 0 :_R u$. Since $p^i \in 0 :_R u$, we certainly have $0 :_R u \supseteq \langle p^i \rangle$. If $0 :_R u \supseteq \langle q^j \rangle$ for some other prime $q \neq p$, then

$$\begin{aligned} 0 :_R u &\supseteq \langle p^i, q^j \rangle \\ &= \langle 1 \rangle \end{aligned}$$

since $\gcd(p^i, q^j) = 1$. In this case, $i = 0$. Otherwise, $i \neq 0$ and $0 :_R u = \langle p^i \rangle$. □

43.2 Embedding finitely generated torsion-free module in R^d

Lemma 43.1. *Every finitely generated torsion-free module M over an integral domain R can be embedded in a finite free R-module. More precisely, if $M \neq 0$, then there is an embedding $M \hookrightarrow R^d$ for some $d \geq 1$ such that the image of M intersects the standard coordinate axis of R^d.*

Proof. Let K be the fraction field of R and $u_1, \dots, u_n$ be a generating set for M as an R-module. We will show n is an upper bounded on the size of any R-linearly independent subset of M. Let $\varphi \colon R^n \to M$ be the linear map given by

$$\varphi(e_i) = u_i$$

for all $1 \leq i \leq n$. Let $v_1, \dots, v_k$ be linearly independent in M. Choose $\widetilde{v}_1, \dots, \widetilde{v}_k \in R^n$ such that

$$\varphi(\widetilde{v}_j) = v_j$$

for all $1 \leq j \leq k$. We claim that $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is linearly independent. Indeed, suppose

$$a_1 \widetilde{v}_1 + \cdots + a_k \widetilde{v}_k = 0 \tag{120}$$

for some $a_1, \dots, a_k \in R$. Then applying φ to both sides of (120) gives us

$$a_1 v_1 + \cdots + a_k v_k = 0$$

which implies $a_1 = \cdots = a_k = 0$ since $\{v_1, \dots, v_k\}$ is linearly independent. Therefore $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is linearly independent. In fact, we claim that $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is K-linearly independent in K^n. Indeed, suppose

$$x_1 \widetilde{v}_1 + \cdots + x_k \widetilde{v}_k = 0 \tag{121}$$

for some $x_1 \dots, x_k \in K$. Let $d \in R$ be the common denominator of $x_1, \dots, x_k$. Then multiplying d to both sides of (121) gives us

$$(dx_1) \widetilde{v}_1 + \cdots + (dx_k) \widetilde{v}_k = 0$$

which implies $dx_1 = \cdots = dx_k = 0$ since $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is R-linearly independent. This further implies $x_1 = \cdots = x_k = 0$ since $d \neq 0$ and R is an integral domain. Thus $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is K-linearly independent in K^n. Now it follows from linear algebra over fields that $k \leq n$.

From the bound $k \leq n$, there is a linearly independent subset of M with maximal size, say $w_1, \dots, w_d$. Then

$$\sum_{j=1}^{d} R w_j \cong R^d.$$

We will find a scalar multiple of M inside of this. For any $u \in M$, the set $\{u, w_1, \dots, w_d\}$ is linearly independent by maximality of d, so there is a nontrivial relation

$$au + \sum_{i=1}^{d} a_i w_i = 0,$$

where $a, a_1, \dots, a_d \in R$, necessarily with $a \neq 0$. Thus

$$au \in \sum_{j=1}^{d} R w_j.$$

In particular, for each $1 \le i \le n$, there exists a nonzero $a_i \in R$ such that

$$a_i u_i \in \sum_{j=1}^{d} R w_j.$$

Setting $a = a_1 \cdots a_n$ and using the fact that R is an integral domain and M is torsion free, we see that

$$a u_i \in \sum_{j=1}^{d} R w_j$$

for all i. So $aM \subseteq \sum_{j=1}^{d} R w_j$. Since R is an integral domain, multiplying by a is an isomorphism of M with aM, so we have the sequence of R-linear maps

$$\begin{aligned} M &\to aM \\ &\hookrightarrow \sum_{j=1}^{d} R w_j \\ &\to R^d \end{aligned}$$

where the last map is an isomorphism. □

43.3 Submodules of a finite free module over a PID

Theorem 43.2. *When R is a PID, any submodule of a free R-module of rank n is free of rank $\le n$.*

Proof. We may assume the free R-module is literally R^n and will induct on n. The case where $n = 1$ is true since R is a PID: every R-submodule of R is an ideal, hence of the form Ra since all ideals in R are principal, and $Ra \cong R$ as R-modules when $a \neq 0$ since R is an integral domain. Say $n \ge 1$ and the theorem is proved for R^n. Let $M \subseteq R^{n+1}$ be a submodule. We want to show M is free of rank $\le n+1$. View

$$M \subseteq R^{n+1} = R \oplus R^n$$

and let $\pi \colon R \oplus R^n \to R^n$ be the projection to the second component of this direct sum. Then

$$N = \pi(M) \subseteq R^n$$

is free of rank $\le n$ by the induction hypothesis. Since π maps M onto N and N is free (and hence projective), we have

$$M \cong N \oplus \ker \pi|_M$$

and $\ker \pi|_M = M \cap (R \oplus 0)$. All submodules of $R \oplus 0 \cong R$ are free of rank ≤ 1. Thus $N \oplus \ker \pi|_M$ is free of rank $\le n+1$, so M is as well. □

Remark 60. Using Zorn's Lemma, one can show that Theorem (43.2) holds for non-finitely generated free modules too: any submodule of a free module over a PID is free.

Corollary 34. *When R is a PID, every finitely generated torsion-free R-module is a finite free R-module.*

Proof. By Lemma (43.1), such a module embeds into a finite free R-module, so it is finite free too by Theorem (43.2). □

Corollary 35. *Let R be a PID. Let M, M', M'' be R-modules such that*

$$M'' \subseteq M' \subseteq M$$

and such that $M \cong R^n \cong M''$. Then $M' \cong R^n$.

Proof. Since M is free of rank n and M' is a submodule, Theorem (43.2) tells us that $M' \cong A^m$ with $m \le n$. Using Theorem (43.2) again on M'' as a submodule of M', we see that $M'' \cong R^k$ with $k \le m$. By hypothesis, $M'' \cong R^k$. Therefore $k = n$ since R is commutative and hence $m = n$. □

43.4 Finitely generated modules over PID is isomorphic to free + torsion

Corollary 36. *Let R be a PID and let M be a finitely generated R-module. Then*

$$M \cong F \oplus M_{\text{tor}}$$

where F is free.

Proof. Observe that M/M_{tor} is torsion-free and finitely generated as an R-module. Indeed, it is torsion-free since if $au \in M_{\text{tor}}$ for some $a \neq 0$, then $u \in M_{\text{tor}}$ since R is an integral domain. It is finitely generated since it is the homomorphic image of a finitely generated module. Therefore by the previous theorem, M/M_{tor} is free. Therefore the short exact sequence

$$0 \longrightarrow M_{\text{tor}} \longrightarrow M \longrightarrow M/M_{\text{tor}} \longrightarrow 0$$

splits. Thus $M \cong F \oplus M_{\text{tor}}$ where $F = M/M_{\text{tor}}$ is free. $\square$

Theorem 43.3. *Let R be a PID and let M be a torsion R-module. For any prime p in R, set*

$$\Gamma_p(M) = \bigcup_{k \geq 0} (0 :_M p^k) = \{u \in M \mid p^k u = 0 \text{ for some } k \geq 0\}.$$

Then

$$M \cong \bigoplus_{p \text{ prime}} \Gamma_p(M).$$

Furthermore, if M is finitely-generated, then $\Gamma_p(M) = 0$ for all but finitely many p.

Proof. Suppose $0 \neq a \in A$. Then there exists $0 \neq r \in R$ such that $ra = 0$. Write

$$r = p_1^{b_1} \cdots p_k^{b_k}.$$

Now observe that

$$\begin{aligned} (p_2^{b_2} p_3^{b_3} \cdots p_k^{b_k})a &\in A_{p_2} \\ (p_1^{b_2} p_3^{b_3} \cdots p_k^{b_k})a &\in A_{p_3} \\ &\vdots \\ (p_1^{b_2} p_2^{b_3} \cdots p_{k-1}^{b_{k-1}})a &\in A_{p_k} \end{aligned}$$

We claim that $a \in A_{p_1} + A_{p_2} \cdots + A_{p_k}$. Indeed,

$$\gcd(p_2^{b_2} p_3^{b_3} \cdots p_k^{b_k}, p_1^{b_2} p_3^{b_3} \cdots p_k^{b_k}, \ldots, p_1^{b_2} p_2^{b_3} \cdots p_{k-1}^{b_{k-1}}) = 1.$$

Thus there exists $r_1, r_2, \ldots, r_k$ such that

$$\sum r_i p_1^{b_1} \cdots \widehat{p_i^{b_i}} \cdots p_k^{b_k} = 1.$$

Therefore

$$\begin{aligned} a &= \sum r_i p_1^{b_1} \cdots \widehat{p_i^{b_i}} \cdots p_k^{b_k} a \\ &\in A_{p_1} + A_{p_2} \cdots + A_{p_k}. \end{aligned}$$

To see that the sum is direct, suppose $a \in A_p \cap \sum_{q \neq p} A_q$. Choose $k \in \mathbb{N}$ such that $p^k a = 0$ and choose $a_{q_i} \in A_{q_i}$ with $q_i^{k_i} a = 0$ such that

$$a = a_{q_1} + \cdots + a_{q_m}.$$

If $\alpha = \prod_{i=1}^m q_i^{k_i}$, then $p^k a = 0$ and $\alpha a = 0$. Since $\gcd(\alpha, p^k) = 1$, we see that a is killed by all of R. Thus $a = 0$ since $1 \in R$. $\square$

43.5 Aligned Bases

There is a convenient way of picturing any submodule of a finite free module over a PID: bases can be chosen for the module and submodule that are aligned nicely, as follows.

Definition 43.2. Let R be a PID, let M be a finite free R-module, and let M' be a submodule of M. A basis $\{u_1, \dots, u_n\}$ of M and a basis $\{a_1u_1, \dots, a_mu_m\}$ of M' with $a_i \in R\backslash\{0\}$ and $m \leq n$ is called a pair of **aligned** bases.

Theorem 43.4. *Any finite free R-module M of rank $n \geq 1$ and nonzero submodule M' of rank $m \leq n$ admit a pair of aligned bases: there is a basis $u_1, \dots, u_n$ of M and nonzero $a_1, \dots, a_m \in R$ such that*

$$M = \bigoplus_{i=1}^{n} Ru_i \quad \textit{and} \quad M' = \bigoplus_{j=1}^{m} Ra_ju_j.$$

Proof. Define S to be the set of ideals $\varphi(M')$ where $\varphi\colon M \to R$ is R-linear. This includes nonzero ideals; for example, let M have R-basis $\{e_1, \dots, e_n\}$. Choose any nonzero $u' \in M'$ and write

$$u' = a_1e_1 + \cdots + a_ne_n.$$

Then since $u' \neq 0$, we must have $a_i \neq 0$ for some i, and so $e_i^\star(u') = a_i$ is nonzero. Hence $e_i^\star(M') \neq 0$.

Any nonzero ideal in R is contained in only finitely many ideals since R is a PID, so S contains maximal members with respect to inclusion. Call one of these maximal members Ra_1, so $a_1 \neq 0$. Thus $Ra_1 = \varphi_1(M')$ for some linear map $\varphi_1\colon M \to R$. There exists some $v' \in M'$ such that

$$a_1 = \varphi_1(v').$$

Eventually we are going to show that φ_1 takes the value 1 on M.

We claim that for any linear map $\varphi\colon M \to R$, we have $a_1 \mid \varphi(v')$. To show this, set $\varphi(v') = a_\varphi \in R$. Since R is a PID, we have $Ra_1 + Ra_\varphi = Rd$ for some d, so $Ra_1 \subseteq Rd$. Then there exists $x, y \in R$ such that $d = xa_1 + ya_\varphi$. Thus

$$\begin{aligned} d &= xa_1 + ya_\varphi \\ &= x\varphi_1(v') + y\varphi(v') \\ &= (x\varphi_1 + y\varphi)(v'), \end{aligned}$$

and so $dR \subseteq (x\varphi_1 + y\varphi)(M') \in S$. Hence

$$\begin{aligned} \varphi_1(M') &= Ra_1 \\ &\subseteq Rd \\ &\subseteq (x\varphi_1 + y\varphi)(M'). \end{aligned}$$

Since $x\varphi_1 + y\varphi$ is a linear map $M \to R$, it belongs to S, so maximality of $\varphi_1(M')$ in S implies

$$\begin{aligned} \varphi_1(M') &= (x\varphi_1 + y\varphi)(M') \\ &= Rd. \end{aligned}$$

Hence

$$\begin{aligned} Ra_1 &= Rd \\ &= Ra_1 + Ra_\varphi, \end{aligned}$$

which implies $a_\varphi \in R$, and so $a_1 \mid a_\varphi$.

With the claim proved, we are ready to build aligned bases in M and M'. Letting $\{e_1, \dots, e_n\}$ be a basis for M, we have

$$v' = c_1e_1 + \cdots + c_ne_n$$

for some $c_i \in R$. The ith coordinate function for this basis is a linear map $M \to R$ taking the value c_i at v', and so c_i is a multiple of a_1 by our claim. Writing $c_i = a_1b_i$, we have

$$\begin{aligned} v' &= \sum_{i=1}^{n} c_ie_i \\ &= \sum_{i=1}^{n} a_1b_ie_i \\ &= a_1\left(b_1e_1 + \cdots + b_ne_n\right) \\ &= a_1v_1, \end{aligned}$$

say. Then

$$\begin{aligned} a_1 &= \varphi_1(v') \\ &= \varphi_1(a_1 v_1) \\ &= a_1 \varphi_1(v_1), \end{aligned}$$

and so $\varphi_1(v_1) = 1$. We have found an element of M at which φ_1 takes the value 1.

The module M can be written as $Rv_1 + \ker\varphi_1$ since any $v \in M$

$$v = \varphi_1(v)v_1 + (v - \varphi_1(v))v_1.$$

Also $Rv_1 \cap \ker\varphi_1$. Thus $M = Rv_1 \oplus \ker\varphi_1$. Since M is free of rank n its submodule $\ker\varphi_1$ is free and necessarily of rank $n-1$.

How does M' fit in this decomposition of M? For any $w \in M'$ we have

$$w = \varphi_1(w)v_1 + (w - \varphi_1(w)v_1)$$

and the first term is

$$\begin{aligned} \varphi_1(w)v_1 &\in \varphi_1(M')v_1 \\ &= (Ra_1)v_1 \\ &= Ra_1v_1 \\ &= Rv' \\ &\subseteq M', \end{aligned}$$

so $w - \varphi_1(w)v_1 \in M'$ too. Therefore

$$M' = (M' \cap Rv_1) \oplus (M' \cap \ker\varphi_1).$$

So $M = Rv_1 \oplus \ker\varphi_1$ and $M' = Ra_1v_1 \oplus (M' \cap \ker\varphi_1)$. The last equation tells us $M' \cap \ker\varphi_1$ is free of rank $m-1$ since M' is free of rank m. If $m = 1$ then we're done. If $m > 1$, then we can describe how $M' \cap \ker\varphi_1$ sits in $\ker\varphi_1$ by induction on the rank: we have a basis $v_2, \dots, v_n$ of $\ker\varphi_1$ and $a_2, \dots, a_m \in R\backslash\{0\}$ such that $a_2v_2, \dots, a_mv_m$ is a basis of $M' \cap \ker\varphi_1$. □

44 Tensor

44.1 Definition of Tensor Products via UMP

Definition 44.1. Let M and N be R-modules. The **tensor product** $M \otimes_R N$ is an R-module equipped with a bilinear map $\otimes\colon M \times N \to M \otimes_R N$ such that for each bilinear map $B\colon M \times N \to P$ there is a unique linear map $L\colon M \otimes_R N \to P$ making the following diagram commute.

$$\begin{tikzcd} & M \otimes_R N \arrow[dd, dotted, "L"] \\ M \times N \arrow[ur, "\otimes"] \arrow[dr, "B"'] & \\ & P \end{tikzcd}$$

Let R-modules T and T', and bilinear maps $b\colon M \times N \to T$ and $b'\colon M \times N \to T'$, satisfy the universal mapping property of the tensor product. From universality of $b\colon M \times N \to T$, the map $b'\colon M \times N \to T'$ factors uniquely through T: there exists a unique linear map $f\colon T \to T'$ making

$$\begin{tikzcd} & T \arrow[dd, dotted, "f"] \\ M \times N \arrow[ur, "b"] \arrow[dr, "b'"'] & \\ & T' \end{tikzcd} \tag{122}$$

commute. From universality of $b' \colon M \times N \to T'$, the map $b \colon M \times N \to T$ factors uniquely through T': there exists a unique linear map $f' \colon T' \to T$ making

$$\begin{tikzcd} & T' \arrow[dd, dotted, "f'"] \\ M \times N \arrow[ur, "b'"] \arrow[dr, "b"'] & \\ & T \end{tikzcd} \tag{123}$$

commute. We combine (124) and (123) into the commutative diagram

$$\begin{tikzcd} & T \arrow[d, "f"] \\ M \times N \arrow[ur, "b"] \arrow[r, "b'"] \arrow[dr, "b"'] & T' \arrow[d, "f'"] \\ & T \end{tikzcd} \tag{124}$$

Removing the middle, we have the commutative diagram

$$\begin{tikzcd} & T \arrow[dd, "f' \circ f"] \\ M \times N \arrow[ur, "b"] \arrow[dr, "b"'] & \\ & T \end{tikzcd} \tag{125}$$

From universality of (T, b), a unique linear map $T \to T$ fits in (125). The identity map works, so $f' \circ f = 1_T$. Similarly, $f \circ f' = 1_{T'}$ by stacking (124) and (123) in the other order. Thus T and T' are isomorphic R-modules by f and also $f \circ b = f'$, which means f identifies b with b'. So two tensor products of M and N can be identified with each other in a unique way compatible with the distinguished bilinear maps to them from $M \times N$.

44.2 Construction of Tensor Product

Theorem 44.1. *A tensor product of M and N exists.*

Proof. Consider $M \times N$ simply as a set. We form the free R-module on this set:

$$F_R(M \times N) = \bigoplus_{(u,v) \in M \times N} R\delta_{(u,v)}.$$

Let D be the submodule of $F_R(M \times N)$ $\square$

44.3 The Covariant Functor $- \otimes_R N$

Proposition 44.1. *Let N be an R-module. We obtain a covariant functor*

$$- \otimes_R N \colon \mathbf{Mod}_R \to \mathbf{Mod}_R$$

from the category of R-modules to itself, where the R-module M is assigned to the R-module $M \otimes_R N$ and where the R-linear map $\varphi \colon M \to M'$ is assigned to the R-linear map $\varphi \otimes 1 \colon M \otimes_R N \to M' \otimes_R N$, where $\varphi \otimes 1$ is defined by

$$(\varphi \otimes 1)(u \otimes v) = \varphi(u) \otimes v$$

for all elementary tensors $u \otimes v \in M \otimes_R N$.

Proof. We need to check that $- \otimes_R N$ preserves compositions and identities. We first check that it preserves compositions. Let $\varphi \colon M \to M'$ and $\varphi' \colon M' \to M''$ be two R-linear maps and let $u \otimes v$ be an elementary tensor in

$M \otimes_R N$. Then

$$\begin{aligned}((\varphi' \otimes 1)(\varphi \otimes 1))(u \otimes v) &= (\varphi' \otimes 1)((\varphi \otimes 1)(u \otimes v)) \\ &= (\varphi' \otimes 1)(\varphi(u) \otimes v) \\ &= (\varphi'(\varphi(u)) \otimes v \\ &= (\varphi'\varphi)(u) \otimes v \\ &= (\varphi'\varphi \otimes 1)(u \otimes v).\end{aligned}$$

It follows that $(\varphi' \otimes 1)(\varphi \otimes 1) = \varphi'\varphi \otimes 1$. Hence $- \otimes_R N$ preserves compositions. Next we check that $- \otimes_R N$ preserves identities. Let M be an R-module and $u \otimes v$ be an elementary tensor in $M \otimes_R N$. Then we have

$$\begin{aligned}(1_M \otimes 1)(u \otimes v) &= 1_M(u) \otimes v \\ &= u \otimes v \\ &= 1_{M \otimes_R N}(u \otimes v).\end{aligned}$$

It follows that $1_M \otimes 1 = 1_{M \otimes_R N}$. Hence $- \otimes_R N$ preserves identities. □

44.3.1 Right exactness of $- \otimes_R N$

Proposition 44.2. *The sequence of R-modules and R-linear maps*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0 \tag{126}$$

is exact if and only if for all R-modules N the induced sequence

$$M_1 \otimes_R N \xrightarrow{\varphi_1 \otimes N} M_2 \otimes_R N \xrightarrow{\varphi_2 \otimes N} M_3 \otimes_R N \longrightarrow 0 \tag{127}$$

is exact.

Proof. The sequence

$$M_1 \otimes_R N \longrightarrow M_2 \otimes_R N \longrightarrow M_3 \otimes_R N \longrightarrow 0 \tag{128}$$

is exact for all R-modules N if and only if for all R-modules N and P the induced sequence

$$0 \longrightarrow \mathrm{Hom}_R(M_3 \otimes_R N, P) \longrightarrow \mathrm{Hom}_R(M_2 \otimes_R N, P) \longrightarrow \mathrm{Hom}_R(M_1 \otimes_R N, P) \tag{129}$$

is exact by Proposition (46.4). Then (129) is exact for all R-modules N and P if and only the sequence

$$0 \longrightarrow \mathrm{Hom}_R(M_3, \mathrm{Hom}_R(N, P)) \longrightarrow \mathrm{Hom}_R(M_2, \mathrm{Hom}_R(N, P)) \longrightarrow \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(N, P)) \tag{130}$$

is exact for all R-modules N and P, by tensor-hom adjointness. Then (130) is exact for all R-modules N and P if and only if for all R-modules K

$$0 \longrightarrow \mathrm{Hom}_R(M_3, K) \longrightarrow \mathrm{Hom}_R(M_2, K) \longrightarrow \mathrm{Hom}_R(M_1, K) \tag{131}$$

is exact since any R-module K is isomorphic to an R-module of the form $\mathrm{Hom}_R(N, P)$ (take $N = R$ and $P = K$) and because of naturality of Hom as in (46.5). Finally, (132) is exact if and only if

$$M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{132}$$

is exact again by Proposition (**??**). □

44.4 Tensor Product Properties

44.4.1 Tensor product of finitely presented R-modules is finitely presented

Proposition 44.3. *Let M be an N be finitely presented R-modules with presentations*

$$F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0 \quad \text{and} \quad G_1 \xrightarrow{\psi_1} G_0 \xrightarrow{\psi_0} N \to 0.$$

Then

$$(F_1 \otimes_R G_0) \oplus (F_0 \otimes_R G_1) \xrightarrow{\phi_1} F_0 \otimes_R G_0 \xrightarrow{\phi_0} M \otimes_R N \to 0 \tag{133}$$

is a presentation of $M \otimes_R N$, where ϕ_0 is defined by

$$\phi_0(u_0 \otimes v_0) = \varphi_0(u_0) \otimes v_0 - u_0 \otimes \psi_0(v_0)$$

for all elementary tensors $u_0 \otimes v_0 \in F_0 \otimes_R G_0$, and where ϕ_1 is defined by

$$\phi_1(u_1 \otimes v_0) = \varphi_1(u_1) \otimes v_0 \quad \text{and} \quad \phi_1(u_0 \otimes v_1) = u_0 \otimes \psi_1(v_1)$$

for all $u_1 \otimes v_0 \in F_1 \otimes_R G_0$ and $u_0 \otimes v_1 \in F_0 \otimes_R G_1$.

Proof. The assignment

$$(u_0, v_0) \mapsto \varphi_0(u_0) \otimes v_0 - u_0 \otimes \psi_0(v_0)$$

is R-bilinear and thus ϕ_0 is a well-defined R-linear map. Similarly, the assignments

$$(u_1, v_0) \mapsto \varphi_0(u_0) \otimes v_0 \quad \text{and} \quad (u_0, v_1) \mapsto u_0 \otimes \psi_1(v_1)$$

are R-bilinear and thus ϕ_1 is a well-defined R-linear map. Let us check that (**??**) is exact. □

44.4.2 Tensor product commutes with direct sums

Proposition 44.4. *Let M be an R module and let $\{L_i\}$ be a collection of R-modules indexed over a set I. Then*

$$\left(\bigoplus_{i \in I} L_i\right) \otimes_R M \cong \bigoplus_{i \in I} (L_i \otimes_R M).$$

Proof. For all R-modules N, we have

$$\begin{aligned}
\mathrm{Hom}_R\left(\left(\bigoplus_{i \in I} L_i\right) \otimes_R M, N\right) &\cong \mathrm{Hom}_R\left(\bigoplus_{i \in I} L_i, \mathrm{Hom}_R(M, N)\right) \\
&\cong \prod_{i \in I} \mathrm{Hom}_R(L_i, \mathrm{Hom}_R(M, N)) \\
&\cong \prod_{i \in I} \mathrm{Hom}_R(L_i \otimes_R M, N) \\
&\cong \mathrm{Hom}_R\left(\bigoplus_{i \in I} (L_i \otimes_R M), N\right).
\end{aligned}$$

It follows that

$$\left(\bigoplus_{i \in I} L_i\right) \otimes_R M \cong \bigoplus_{i \in I} (L_i \otimes_R M).$$

□

44.5 Tensor-Hom Adjointness and its Applications

Let B be an A-algebra, let X and Y be B-modules, and let Z be an A-module. Define a map

$$(-)^\diamond \colon \mathrm{Hom}_B(X, \mathrm{Hom}_A(Y, Z)) \to \mathrm{Hom}_A(X \otimes_B Y, Z)$$

as follows: for all $\varphi \in \mathrm{Hom}_B(X, \mathrm{Hom}_A(Y, Z))$ we set $\varphi^\diamond$ to be the unique linear map defined on elementary tensors by $x \otimes y \in X \otimes_B Y$ by

$$\varphi^\diamond(x \otimes y) := (\varphi x) y, \tag{134}$$

where we are using the notational convention $\varphi x = \varphi(x)$ in order to simplify our notation in what follows. Note that (136) is well-defined since the map $(x, y) \mapsto (\varphi x) y$ is B-bilinear. Indeed, additivity in one argument while the other is fixed is obvious. Also φ is B-linear by assumption, so $(\varphi(bx))y = (b(\varphi x))y$, and φx is B-linear because $\mathrm{Hom}_A(Y, Z)$ is given the structure of a B-module using the fact that Y is a B-module; namely $(b(\varphi x))y := (\varphi x)(by)$. Finally $(-)^\diamond$ is B-linear because both φ and φx are B-linear and because $\mathrm{Hom}_A(X \otimes_B Y, Z)$ is given the structure of a B-module using the fact that Y is a B-module; namely

$$(b(\varphi^\diamond))(x \otimes y) := \varphi^\diamond(x \otimes by) = (\varphi x)(by) = (b(\varphi x))y = (\varphi(bx))y = ((b\varphi)x)y =: (b\varphi)^\diamond(x \otimes y). \tag{135}$$

Notice that b never appeared outside all of the parenthesis in (135): every term in (135) is an element of Z, which is an A-module! Next we define a map

$$(-)_\diamond \colon \mathrm{Hom}_A(X \otimes_B Y, Z) \to \mathrm{Hom}_B(X, \mathrm{Hom}_A(Y, Z))$$

as follows: for all $\psi \in \mathrm{Hom}_A(X \otimes_B Y, Z)$ we set $\psi_\diamond$ to be the unique B-linear map such that for all $x \in X$ and $y \in Y$ we have

$$(\psi_\diamond x)y := \psi(x \otimes y) \tag{136}$$

Note that (136) is well-defined since the map $(x, y) \mapsto (\psi_\diamond x)y$ is B-bilinear. Thus for instance, the following is a perfectly legitimate computation:

$$\begin{aligned} ((b\psi + \widetilde{\psi})_\diamond x)y &= (b\psi + \widetilde{\psi})(x \otimes y) \\ &= (b\psi)(x \otimes y) + \widetilde{\psi}(x \otimes y) \\ &= \psi(x \otimes by) + \widetilde{\psi}(x \otimes y) \\ &= (\psi_\diamond x)(by) + (\widetilde{\psi}_\diamond x)y \\ &= (b(\psi_\diamond x)y + (\widetilde{\psi}_\diamond x)y \\ &= ((b\psi)_\diamond x)y + (\widetilde{\psi}_\diamond x)y. \end{aligned}$$

Again, b never appears outside the parenthesis in the computation above because each of these elements belongs to Z. Thus $(-)_\diamond$ and $(-)^\diamond$ are both B-module homomorphisms. In fact, we get something much stronger!

Theorem 44.2. *The map $(-)^\diamond$ is an isomorphism which is natural in X, Y, and Z, with the map $(-)_\diamond$ being its inverse. In particular, the functor $- \otimes_B Y$ is left adjoint to the functor $\mathrm{Hom}_B(X, -)$, and thus $- \otimes_B X$ preserves all colimits and $\mathrm{Hom}_A(X, -)$ preserves all limits.*

Intuitively, one thinks of $\varphi^\diamond(x \otimes y) = (\varphi x)y$ as applying the "associative law" where the diamond in the superscript tells us that we can "pull back" the parenthesis. Similarly, one thinks of $(\psi_\diamond x)y = \psi(x \otimes y)$ as applying the "associative law" where the diamond in the subscript tells us that we can "push forward" the parenthesis. With this in in mind, it is very easy to see why $(-)^\diamond$ and $(-)_\diamond$ are inverse to each other: we are just applying the associative law! Indeed, we have

$$((\varphi^\diamond)_\diamond x)y = \varphi^\diamond(x \otimes y) = (\varphi x)y \quad \text{and} \quad (\psi_\diamond)^\diamond(x \otimes y) = (\psi_\diamond x)y = \psi(x \otimes y). \tag{137}$$

In particular, one should note that the reason why $(-)_\diamond$ and $(-)^\diamond$ are inverse to each other is precisely due to the way we defined them in the first place. Another added benefit that we get when using this notation is that when we write an interpretable string using the symbols $\{\diamond, (,), \varphi, \psi, \phi, x, y, z\}$, then it becomes visibly clear how we could interpret this string, where we consider a string interpretable if we can obtain a new string without any diamond symbols by applying the associative law a finite number of times to the original string. For instance, the string $\varphi_\diamond(x \otimes y)$ is uninterpretable in our language since we can't "pullback" the parenethesis and remove the diamond in the subscript. On the other hand, the string $\phi^\diamond(\psi x \otimes (\varphi_\diamond x)y)$ is interpretable: if we apply the associative law one time, we can remove the subscript diamond and obtain $\phi^\diamond(\psi x \otimes \varphi(x \otimes y))$. If we apply the associative law again, we can remove the superscript diamond and obtain $(\psi(\varphi x))\phi(x \otimes y)$. Since this string doesn't contain any diamonds, we can give a reasonable interpretation to it. For instance, ψ can be thought of as a map in $\mathrm{Hom}_B(L, \mathrm{Hom}_A(M, N))$, which maps the element $\varphi x \in L$ to the map $\psi(\varphi x) \in \mathrm{Hom}_A(M, N)$ whose value at $\phi(x \otimes y)$ is $(\psi(\varphi x))\phi(x \otimes y)$.

Proof. We've have already shown that $(-)^\diamond$ is a B-linear isomorphism with $(-)_\diamond$ being its inverse. It remains to show that $(-)^\diamond$ (or equivalently $(-)_\diamond$) is natural in X, Y, and Z. But our simple description of $(-)^\diamond$ makes this completely obvious! For instance, naturality in X means that if we have an R-module homomorphism $\lambda \colon X \to X'$, then the following diagram commutes:

$$\begin{tikzcd} \mathrm{Hom}_B(X, \mathrm{Hom}_A(Y, Z)) \arrow[r, "(-)^\diamond"] \arrow[d, "\lambda^*"'] & \mathrm{Hom}_A(X \otimes_B Y, Z) \arrow[d, "(\lambda \otimes 1)^*"] \\ \mathrm{Hom}_B(X, \mathrm{Hom}_A(Y, Z)) \arrow[r, "(-)^\diamond"] & \mathrm{Hom}_A(X \otimes_B Y, Z) \end{tikzcd}$$

Where $(-)^\diamond$ is defined on $\mathrm{Hom}_B(X', \mathrm{Hom}_A(Y, Z))$ essentially the same way that it was defind on $\mathrm{Hom}_B(X, \mathrm{Hom}_A(Y, Z))$. Furthermore, the diagram above commutes since if $\varphi \in \mathrm{Hom}_B(X', \mathrm{Hom}_A(Y, Z))$, then we have

$$\begin{aligned}(\lambda^*\varphi)^\diamond(x \otimes y) &= ((\lambda^*\varphi)x)y \\ &= (\varphi(\lambda x))y \\ &= \varphi^\diamond(\lambda x \otimes y) \\ &= ((\lambda \otimes 1)^*(\varphi^\diamond))(x \otimes y).\end{aligned}$$

The point to remember in the computation above is that all we are doing here is applying universal algrebraic rules like "commutativity" and "associativity", so it's perfectly reasonable that these become natural isomorphisms. □

44.5.1 General Version of Tensor-Hom Adjunction

Let B be an A-algebra, let X be an A-module and let Y and Z be B-modules. Note that Y and Z are given the structure of an A-module using the ring homomorphim $A \to B$, thus they are naturally A-modules. There is another version of tensor-hom which we would like to describe now. We claim that exists a canonical isomorphisms

$$(-)^\diamond \colon \mathrm{Hom}_A(X, \mathrm{Hom}_B(Y, Z)) \to \mathrm{Hom}_B(X \otimes_A Y, Z) \quad \text{and} \quad (-)_\diamond \colon \mathrm{Hom}_B(X \otimes_A Y, Z) \to \mathrm{Hom}_A(X, \mathrm{Hom}_B(Y, Z))$$

as B-modules, both of which are natural in X, Y, and Z. Notice that the rings have swapped positions this time. We give $\mathrm{Hom}_B(Y, Z)$ the structure of an A-module using the fact that Y and Z are A-modules; namely $(a\varphi)y := \varphi(ay) := a(\varphi y)$. Similarly we give $\mathrm{Hom}_A(X, \mathrm{Hom}_B(Y, Z))$ the structure of a B-module using the fact $\mathrm{Hom}_B(Y, Z)$ and Z are B-modules; namely $((b\psi)x)y := (b(\psi x))y = (\psi x)(by) = b((\psi x)y)$. Finally we give $X \otimes_A Y$ the structure of a B-module using the fact that Y is a B-module. With all of this in mind, we define

$$\varphi^\diamond(x \otimes y) = (\varphi x)y \quad \text{and} \quad (\psi_\diamond x)y = \psi(x \otimes y).$$

These maps still work since all maps involved are B-linear maps. Here is a much more general version of the tensor-hom adjunction:

Theorem 44.3. *Let A, B, and C be three different rings (each of which is not necessarily-commutative). Let X be an (A, B)-bimodule (so A acts on the left of X and B acts on the right of X), let Y be a (B, C)-bimodule, and let Z be an (A, C)-bimodule.*

1. *We have canonical isomorphisms*

$$(-)^\diamond \colon \mathrm{Hom}_B(X, \mathrm{Hom}_C(Y, Z)) \to \mathrm{Hom}_C(X \otimes_B Y, Z) \quad \textit{and} \quad (-)_\diamond \colon \mathrm{Hom}_C(X \otimes_B Y, Z) \simeq \mathrm{Hom}_B(X, \mathrm{Hom}_C(Y, Z))$$

as (A, A)-bimodules, natural in X, Y, and Z, defined by

$$(\psi^\diamond x)y = \psi(x \otimes y) \quad \textit{and} \quad (\varphi_\diamond x)y = \varphi(x \otimes y).$$

2. *We have canonical isomorphisms*

$$(-)^\diamond \colon \mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z)) \to \mathrm{Hom}_A(X \otimes_B Y, Z) \quad \textit{and} \quad (-)_\diamond \colon \mathrm{Hom}_A(X \otimes_B Y, Z) \simeq \mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z))$$

as (C, C)-bimodules, natural in X, Y, and Z, defined by

$$(\psi^\diamond y)x = \psi(x \otimes y) \quad \textit{and} \quad (\varphi_\diamond x)y = \varphi(x \otimes y)$$

Note that first tensor-hom adjunction has the form $\mathrm{Hom}(X \otimes Y, Z) \simeq \mathrm{Hom}(X, \mathrm{Hom}(Y, Z))$ whereas the second tensor-hom adjunction has the form $\mathrm{Hom}(X \otimes Y, Z) \simeq \mathrm{Hom}(Y, \mathrm{Hom}(X, Z))$ where we note the letters X and Y getting swapped. In the case where we are working over commutative rings, then we have $X \otimes Y \simeq Y \otimes X$, so we swapping can be fixed by just relabeling things. The important to remember, is that tensor-hom should look something like $\mathrm{Hom}_{(-)}(X \otimes_{(-)} Y, Z) \simeq \mathrm{Hom}_{(-)}(X, \mathrm{Hom}_{(-)}(Y, Z))$ where we place a ring in the spots $(-)$ only where they make sense. For instance, $\mathrm{Hom}_C(X, \mathrm{Hom}_B(Y, Z))$ doesn't make sense because X is not a (left or right) C-module and there's no canonical way to give it the structure of a C-module, so it doens't make sense to talk about C-linear maps from X to $\mathrm{Hom}_B(Y, Z)$. Another thing to consider is that there are two ways of giving $\mathrm{Hom}_A(X, Z)$ an A-module structure: we can give it a left A-module structure via $(a\varphi)x := \varphi(ax)$ and we can also give it a right A-module structure via $(\varphi a)(x) := (\varphi x)a$, so $\mathrm{Hom}_A(X, Z)$ can be viewed as an (A, A)-bimodule. Also, $\mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z))$ is a (C, C)-bimodule via $((c\psi)y)x := c((\psi y)x)$ and $((\psi c)y)x = (\psi(yc))x$.

44.5.2 Transporting Projective/Injective Modules over one Ring to Another

Let B be an A-algebra. We can use the tensor-hom adjunction to transport injective A-modules to injective B-modules as follows:

Proposition 44.5. *Let E be an injective A-module, and let F a flat B-module. Then $\mathrm{Hom}_A(F,E)$ is an injective B-module.*

Proof. The functor $\mathrm{Hom}_B(-,\mathrm{Hom}_A(F,E))$ is exact if and only if the functor $\mathrm{Hom}_A(-\otimes_B F, E)$ is exact by tensor-hom adjunction. Now notice that the functor $-\otimes_B F$ is exact since F is a flat B-module, and the functor $\mathrm{Hom}_A(-,E)$ is exact since E is an injective A-module. Thus $\mathrm{Hom}_A(-\otimes_B F, E)$ is a composition of exact functors, and so it must be exact too. $\square$

We can also transport injective B-modules down to injective A-modules:

Proposition 44.6. *Let E be an injective B-module and let F be a B-module which is projective as an A-module. Then $\mathrm{Hom}_B(F,E)$ is an injective A-module.*

Proof. The functor $\mathrm{Hom}_A(-,\mathrm{Hom}_B(F,E))$ is exact if and only if the functor $\mathrm{Hom}_B(-\otimes_A F, E)$ is exact by tensor-hom adjunction. Now notice that the functor $-\otimes_A F$ is exact since F is a flat A-module, and the functor $\mathrm{Hom}_B(-,E)$ is exact since E is an injective B-module. Thus $\mathrm{Hom}_A(-\otimes_B F, E)$ is a composition of exact functors, and so it must be exact too. $\square$

Now let's see how to transport projective modules; namely if we have a projective A-module and a projective B-module, then we can tensor them together to obtain another projective B-module.

Proposition 44.7. *Let P be a projective A-module and let Q be a projective B-module. Then $P\otimes_A Q$ is a projective B-module.*

Proof. It suffices to show that $\mathrm{Hom}_B(P\otimes_A Q,-)$ is exact. Let

$$M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be a short exact sequence of B-modules. Then since Q is a projective B-module, the induced sequence

$$0 \longrightarrow \mathrm{Hom}_B(Q,M_1) \longrightarrow \mathrm{Hom}_B(Q,M_2) \longrightarrow \mathrm{Hom}_B(Q,M_3) \longrightarrow 0$$

is exact. Then since P is a projective A-module, the induced sequence

$$0 \longrightarrow \mathrm{Hom}_A(P,\mathrm{Hom}_B(Q,M_1)) \longrightarrow \mathrm{Hom}_A(P,\mathrm{Hom}_B(Q,M_2)) \longrightarrow \mathrm{Hom}_A(P,\mathrm{Hom}_B(Q,M_3)) \longrightarrow 0$$

is exact. By naturality of tensor-hom adjointness, we have a commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_A(P,\mathrm{Hom}_B(Q,M_1)) \arrow[r] \arrow[d, "\simeq"] & \mathrm{Hom}_A(P,\mathrm{Hom}_B(Q,M_2)) \arrow[r] \arrow[d, "\simeq"] & \mathrm{Hom}_A(P,\mathrm{Hom}_B(Q,M_3)) \arrow[r] \arrow[d, "\simeq"] & 0 \\
0 \arrow[r] & \mathrm{Hom}_B(P\otimes_A Q,M_1) \arrow[r] & \mathrm{Hom}_B(P\otimes_A Q,M_2) \arrow[r] & \mathrm{Hom}_B(P\otimes_A Q,M_3) \arrow[r] & 0
\end{tikzcd}$$

where the columns are isomorphisms and where the top row is exact. It follows from the 3×3 lemma that the bottom row is exact too. $\square$

Essentially by the same argument works in the reverse direction too (though under more restrictions):

Proposition 44.8. *Let Q be a projective B-module and let P be a B-module which is projective as an A-module. Then $P\otimes_B Q$ is projective as an A-module.*

44.5.3 Base Change in Ext

Let B be an A-algebra. We are often presented with the situation where we are working over the ring A and would like to change our base ring to B (and vice-versa). For instance, perhaps we know something about Ext_A and would like to use this information to obtain something about Ext_B. One way we can do this is to use tensor-hom adjointness:

Proposition 44.9. *Assume B is a flat A-algebra. Then there is a canonical isomorphism of graded B-modules*

$$\mathrm{Ext}_B(M\otimes_A B, N) \to \mathrm{Ext}_A(M,N) \tag{138}$$

which is natural in M and N.

Proof. Let F be a projective resolution of M over A. Then $F \otimes_A B$ is a B-complex whose underlying graded module is projective. Furthermore, since B is flat, we have $\mathrm{H}_+(F \otimes B) = 0$ and $\mathrm{H}_0(F \otimes B) = M \otimes B$. Therefore $F \otimes B$ is a projective resolution of $M \otimes B$ over B (note that if B were not a flat A-algebra, then we'd have $\mathrm{H}_+(F \otimes B) = \mathrm{Ext}_A^+(M, B)$ which doesn't necessarily vanish). So to define the map (138), it suffices to define a quasiisomorphism

$$\mathrm{Hom}_B(F \otimes_A B, N) \to \mathrm{Hom}_A(F, N) \tag{139}$$

of B-complexes natural in F and N. Once this chain map is defined, we can then pass it through homology to get the map (138). In fact, we will construct an isomorphism (139) of B-complexes! This is much *stronger* than merely being a quasiisomoprhism. Consider the composition

$$\mathrm{Hom}_B(F \otimes_A B, N) \xrightarrow[\simeq]{(-)_\diamond} \mathrm{Hom}_A(F, \mathrm{Hom}_B(B, N)) \xrightarrow[\simeq]{[-]} \mathrm{Hom}_A(F, N).$$

The way the composite of this map looks on the elements can be seen as follows: let $\varphi\colon F \otimes_A B \to N$ be an i-chain B-map (that is, a chain map of degree i of B-complexes). From φ, we obtain the i-chain B-map $\varphi_\diamond\colon F \to \mathrm{Hom}_B(B, N)$ where $\varphi_\diamond$ is defined on elements by $(\varphi_\diamond \alpha)b = \varphi(\alpha \otimes b)$ where $\alpha \in F$ and $b \in B$. From $\varphi_\diamond$ we obtain the i-chain A-map $[\varphi_\diamond]\colon F \to N$ where $[\varphi_\diamond]$ is defined on elements by $[\varphi_\diamond](\alpha) = (\varphi_\diamond \alpha)1$ for all $\alpha \in F$. We then extend $[\varphi_\diamond]$ to a B-linear map using the fact that N is a B-module; namely

$$(b[\varphi_\diamond])(\alpha) := b([\varphi]_\diamond \alpha) = b((\varphi\alpha)1) = b\varphi(\alpha \otimes 1) = \varphi(\alpha \otimes b).$$

Composing these maps gives us a chain map of B-complexes (139). We already know that $(-)_\diamond$ is isomorphism of B-complexes, natural in F and M. It is easy to see that $[\cdot]$ is also an isomorphism of B-complexes, natural in F and N. Thus their composite, denoted $\varphi \mapsto [\varphi_\diamond]$, is an isomorphism of B-complexes, natural in F and N.

Finally, we need to discuss why naturality is important. Suppose we have an A-linear map $\lambda\colon M \to M'$. Let F' be a projective resolution of M' over A and lift λ to a comparison map $\lambda\colon F \to F'$. We obtain a diagram

$$\begin{tikzcd} \mathrm{Hom}(F' \otimes B, N) \arrow[r, "{[(-)_\diamond]}"] & \mathrm{Hom}(F', N) \\ \mathrm{Hom}(F \otimes B, N) \arrow[u, "(\lambda \otimes 1)^*"] \arrow[r, "{[(-)_\diamond]}"] & \mathrm{Hom}(F, N) \arrow[u, "\lambda^*"'] \end{tikzcd} \tag{140}$$

which is commutative on the nose since $[(-)_\diamond]$ is a natural isomorphism. Thus when we take this diagram in homology, we obtain

$$\begin{tikzcd} \mathrm{Ext}_B(M' \otimes B, N) \arrow[r] & \mathrm{Ext}_A(M', N) \\ \mathrm{Ext}_B(M \otimes B, N) \arrow[u] \arrow[r] & \mathrm{Ext}_A(M, N) \arrow[u] \end{tikzcd}$$

which is again commutative on the nose. Thus the isomorphism $\mathrm{Ext}_B(M \otimes_A B, N) \to \mathrm{Ext}_A(M, N)$ is natural in M (and similarly in N), but keep in mind that we only required the diagram (140) to be commutative up to homotopy in order to bet naturality in M for Ext. □

Proposition 44.10. *Let B be an A-algebra, let Q be a projective B-module which is flat as an A-module, and let N be a B-module. Then we have*

$$\mathrm{Ext}_B(M \otimes_A Q, N) \to \mathrm{Ext}_A(M, \mathrm{Ext}_B(Q, N)) \tag{141}$$

which is natural in M and N.

Proof. Note that since Q is a projective B-module, we have $\mathrm{Ext}_B(Q, N) = \mathrm{Hom}_B(Q, N)$ as graded modules. Let X be a projective resolution of M over A. Then $X \otimes_A Q$ is a B-complex whose underlying graded module is projective (by the base change formula) and such that $\mathrm{H}_+(X \otimes Q) = \mathrm{H}_+(X) = 0$ and $\mathrm{H}_+(X \otimes Q) = M \otimes_A Q$. Thus $X \otimes_A Q$ is a projective resolution of $M \otimes_A Q$ over B. So to define the map (141), it suffices to define a quasiisomorphism

$$\mathrm{Hom}_B(F \otimes_A Q, N) \to \mathrm{Hom}_A(M, \mathrm{Hom}_B(Q, N)) \tag{142}$$

of B-complexes natural in F, Q, and N. Once this chain map is defined, we can then pass it through homology to get the map (138). In fact, we will construct an isomorphism (139) of B-complexes! This is much *stronger* than merely being a quasiisomoprhism. Consider the composition

$$\mathrm{Hom}_B(F \otimes_A Q, N) \to \mathrm{Hom}_A(F, \mathrm{Hom}_B(Q, N)).$$

The way the composite of this map looks on the elements can be seen as follows: let $\varphi\colon F\otimes_A Q\to N$ be an i-chain B-map. From φ, we obtain the i-chain B-map $\varphi_\diamond\colon F\to \mathrm{Hom}_B(Q,N)$ where $\varphi_\diamond$ is defined on elements by $(\varphi_\diamond\alpha)q=\varphi(\alpha\otimes q)$ where $\alpha\in F$ and $q\in Q$. We already know that $(-)_\diamond$ is isomorphism of B-complexes, natural in F, Q, and M, so we are done. □

44.5.4 Tensor Product of Projective is Projective

Let B be an A-algebra, let X be an A-module and let Y and Z be B-modules. Note that Y and Z are given the structure of an A-module using the ring homomorphim $A\to B$, thus they are naturally A-modules. There is another version of tensor-hom which we would like to describe. We claim that exists an isomorphism of B-modules

$$\mathrm{Hom}_A(X,\mathrm{Hom}_B(Y,Z))\to \mathrm{Hom}_B(X\otimes_A Y,Z)$$

which is natural in X, Y, and Z. Notice that the rings have swapped positions this time. We give $\mathrm{Hom}_B(Y,Z)$ the structure of an A-module using the fact that Y and Z are A-modules; namely $(a\varphi)y:=\varphi(ay):=a(\varphi y)$. Similarly we give $\mathrm{Hom}_A(X,\mathrm{Hom}_B(Y,Z))$ the structure of a B-module using the fact $\mathrm{Hom}_B(Y,Z)$ and Z are B-modules; namely $((b\psi)x)y:=(\psi x)(by)=b((\psi x)y)$. Finally we give $X\otimes_A Y$ the structure of a B-module using the fact that Y is a B-module. With all of this in mind, we could try to define this map via $(-)^\diamond$ again and set

$$\varphi^\diamond(x\otimes y)=(\varphi x)y$$

for all $\varphi\in\mathrm{Hom}_A(X,\mathrm{Hom}_B(Y,Z))$ and for all $x\in X$ and $y\in Y$. This map still works since all maps involved are B-linear maps. Here's the most general version:

Theorem 44.4. *Let A, B, and C be three different rings (each of which is not necessarily-commutative). Let X be an (A,B)-bimodule (so A acts on the left of X and B acts on the right of X), let Y be a (B,C)-bimodule, and let Z be an (A,C)-bimodule.*

1. *We have canonical isomorphisms*

$$(-)^\diamond\colon \mathrm{Hom}_B(X,\mathrm{Hom}_C(Y,Z))\to\mathrm{Hom}_C(X\otimes_B Y,Z)\quad \textit{and}\quad (-)_\diamond\colon \mathrm{Hom}_C(X\otimes_B Y,Z)\simeq\mathrm{Hom}_B(X,\mathrm{Hom}_C(Y,Z))$$

as (A,A)-bimodules, natural in X, Y, and Z, defined by

$$(\psi^\diamond x)y=\psi(x\otimes y)\quad \textit{and}\quad (\varphi_\diamond x)y=\varphi(x\otimes y).$$

2. *We have canonical isomorphisms*

$$(-)^\diamond\colon \mathrm{Hom}_B(Y,\mathrm{Hom}_A(X,Z))\to\mathrm{Hom}_A(X\otimes_B Y,Z)\quad \textit{and}\quad (-)_\diamond\colon \mathrm{Hom}_A(X\otimes_B Y,Z)\simeq\mathrm{Hom}_B(Y,\mathrm{Hom}_A(X,Z))$$

as (C,C)-bimodules, natural in X, Y, and Z, defined by

$$(\psi^\diamond y)x=\psi(x\otimes y)\quad \textit{and}\quad (\varphi_\diamond x)y=\varphi(x\otimes y)$$

Note that first tensor-hom adjunction has the form $\mathrm{Hom}(X\otimes Y,Z)\simeq\mathrm{Hom}(X,\mathrm{Hom}(Y,Z))$ whereas the second tensor-hom adjunction has the form $\mathrm{Hom}(X\otimes Y,Z)\simeq\mathrm{Hom}(Y,\mathrm{Hom}(X,Z))$ where we note the letters X and Y getting swapped. In the case where we are working over commutative rings, then we have $X\otimes Y\simeq Y\otimes X$, so we swapping can be fixed by just relabeling things. The important to remember, is that tensor-hom should look something like $\mathrm{Hom}_{(-)}(X\otimes_{(-)}Y,Z)\simeq\mathrm{Hom}_{(-)}(X,\mathrm{Hom}_{(-)}(Y,Z))$ where we place a ring in the spots $(-)$ only where they make sense. For instance, $\mathrm{Hom}_C(X,\mathrm{Hom}_B(Y,Z))$ doesn't make sense because X is not a (left or right) C-module and there's no canonical way to give it the structure of a C-module, so it doens't make sense to talk about C-linear maps from X to $\mathrm{Hom}_B(Y,Z)$. Another thing to consider is that there are two ways of giving $\mathrm{Hom}_A(X,Z)$ an A-module structure: we can give it a left A-module structure via $(a\varphi)x:=\varphi(ax)$ and we can also give it a right A-module structure via $(\varphi a)(x):=(\varphi x)a$, so $\mathrm{Hom}_A(X,Z)$ can be viewed as an (A,A)-bimodule. Also, $\mathrm{Hom}_B(Y,\mathrm{Hom}_A(X,Z))$ is a (C,C)-bimodule via $((c\psi)y)x:=c((\psi y)x)$ and $((\psi c)y)x=(\psi(yc))x$.

44.5.5 Tensor-Hom Adjointness for Complexes

Tensor-hom adjointness continues to make sense in categories of chain complexes as well. We just need to check that the tensor-hom isomorphism $(-)_\diamond\colon\mathrm{Hom}_A(X\otimes_B Y,Z)\to\mathrm{Hom}_B(X,\mathrm{Hom}_A(Y,Z))$ commutes with the differentials, that is

$$\mathrm{d}^\star(\varphi_\diamond)=(\mathrm{d}^\star\varphi)_\diamond$$

for all $\varphi \in \mathrm{Hom}_A(X \otimes_B Y, Z)$. Indeed, for all such φ and for all homogeneous $x \in X$ and $y \in Y$, we have

$$\begin{aligned}((\mathrm{d}^\star(\varphi_\diamond))x)y &= ((\mathrm{d}\varphi_\diamond - (-1)^{|\varphi|}\varphi_\diamond \mathrm{d})x)y \\ &= (\mathrm{d}(\varphi_\diamond x))y - (-1)^{|\varphi|}(\varphi_\diamond \mathrm{d}x)y \\ &= \mathrm{d}((\varphi_\diamond x)y) - (-1)^{|\varphi|+|x|}(\varphi_\diamond x)\mathrm{d}y - (-1)^{|\varphi|}(\varphi_\diamond \mathrm{d}x)y \\ &= \mathrm{d}\varphi(x \otimes y) - (-1)^{|\varphi|+|x|}\varphi(x \otimes \mathrm{d}y) - (-1)^{|\varphi|}\varphi(\mathrm{d}x \otimes y) \\ &= \mathrm{d}\varphi(x \otimes y) - (-1)^{|\varphi|}(\varphi(\mathrm{d}x \otimes y) + (-1)^{|x|}\varphi(x \otimes \mathrm{d}y)) \\ &= \mathrm{d}\varphi(x \otimes y) - (-1)^{|\varphi|}\varphi \mathrm{d}(x \otimes y) \\ &= ((\mathrm{d}\varphi)_\diamond x)y - (-1)^{|\varphi|}((\varphi \mathrm{d})_\diamond x)y \\ &= ((\mathrm{d}^\star \varphi)_\diamond x)y.\end{aligned}$$

45 Localization

Throughout this section, all rings are assumed to be commutative. A notion of localization can still be defined for noncommutative rings, however we will not take this route.

45.1 Multiplicatively Closed Sets

Definition 45.1. Let R be a ring. A subset $S \subset R$ is called **multiplicatively closed** if $1 \in S$ and $s, t \in S$ implies $st \in S$.

Remark 61. One can also say that a subset $S \subset R$ is called multiplicatively closed if it is closed under products of elements, where the "empty product" is understood to be 1.

45.1.1 Examples of multiplicatively closed sets

Example 45.1. Let $\mathfrak{p} \subset R$ be a prime ideal. Then $R \setminus \mathfrak{p}$ is a multiplicatively closed set.

Example 45.2. Let R be a ring and let $a \in R$. Then the set $\{a^n \mid n \in \mathbb{Z}_{\geq 0}\}$ is a multiplicatively closed set.

Example 45.3. The set of all nonzero homogeneous polynomials in the polyomial ring $R[x_1, \dots, x_n]$ is a multiplicatively closed set.

45.1.2 Image of multiplicatively closed set is multiplicatively closed

Proposition 45.1. *Let $\varphi \colon A \to B$ be a ring homomorphism and let S be a multiplicatively closed subset of A. Then $\varphi(S)$ is a multiplicatively closed subset of B.*

Proof. Since φ is a ring homomorphism, it takes the identity to the identity, and so $1 \in \varphi(S)$. Also, if $\varphi(s), \varphi(t) \in \varphi(S)$, then

$$\begin{aligned}\varphi(s)\varphi(t) &= \varphi(st) \\ &\in \varphi(S).\end{aligned}$$

Thus $\varphi(S)$ is multiplicatively closed. □

45.1.3 Inverse image of multiplicatively closed set is multiplicatively closed

Proposition 45.2. *Let $\varphi \colon A \to B$ be a ring homomorphism and let T be a multiplicatively closed subset of B. Then $\varphi^{-1}(T)$ is a multiplicatively closed subset of A.*

Proof. Since φ is a ring homomorphism, it takes the identity to the identity, and so $1 \in \varphi^{-1}(T)$. Also, if $s, t \in \varphi^{-1}(T)$, then $\varphi(s), \varphi(t) \in T$, and so

$$\begin{aligned}\varphi(st) &= \varphi(s)\varphi(t) \\ &\in T\end{aligned}$$

implies $st \in \varphi^{-1}(T)$. Thus $\varphi^{-1}(T)$ is multiplicatively closed. □

45.2 Localization of ring with respect to multiplicatively closed set

Definition 45.2. We define the **localization of** R **with respect to** S, denoted R_S or $S^{-1}R$, as follows: as a set R_S is given by

$$R_S := \left\{ \frac{a}{s} \mid a \in R, s \in S \right\}$$

where a/s denotes the equivalence class of $(a, s) \in R \times S$ with respect to the following equivalence relation:

$$(a, s) \sim (a', s') \text{ if and only if there exists } s'' \in S \text{ such that } s''s'a = s''sa'. \tag{143}$$

We give R_S a ring structure by defining addition and multiplication on R_S by

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2a_1 + s_1a_2}{s_1s_2} \quad \text{and} \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1a_2}{s_1s_2}, \tag{144}$$

for a_1/s_1 and a_2/s_2 in R_S, where $1/1$ serves as the multiplicative identity element in R_S and $0/0$ serves as the additive identity in R_S. The ring R_S comes equipped with a natural ring homomoprhism $\rho_S \colon R \to R_S$, given by

$$\rho_S(a) = \frac{a}{1}$$

for all $a \in R$.

Proposition 45.3. *With the notation as above, R_S is a ring. Furthermore, $\rho_S \colon R \to R_S$ is a ring homomorphism.*

Proof. There are several things we need to check. We will break this into steps

Step 1: We show that the relation (143) is in fact a equivalence relation. First we show reflexivity of $\sim$. Let $(a, s) \in R \times S$. Then since $1 \in S$ and $1 \cdot sa = 1 \cdot sa$, we have $(a, s) \sim (a, s)$. Next we show symmetry of $\sim$. Suppose $(a, s) \sim (a', s')$. Choose $s'' \in S$ such that $s''s'a = s''sa'$. Then by symmetry of equality, we have $s''sa' = s''s'a$. Therefore $(a', s') \sim (a, s)$. Finally, we show transitivity of $\sim$. Suppose $(a_1, s_1) \sim (a_2, s_2)$ and $(a_2, s_2) \sim (a_3, s_3)$. Choose $s_{12}, s_{23} \in S$ such that

$$s_{12}s_2a_1 = s_{12}s_1a_2 \quad \text{and} \quad s_{23}s_3a_2 = s_{23}s_2a_3$$

Then $s_{23}s_{12}s_2 \in S$ and

$$\begin{aligned}
(s_{23}s_{12}s_2)(s_3a_1) &= s_{23}(s_{12}s_2a_1)s_3 \\
&= s_{23}(s_{12}s_1a_2)s_3 \\
&= s_{12}s_1(s_{23}s_3a_2) \\
&= s_{12}s_1(s_{23}s_2a_3) \\
&= (s_{12}s_{23}s_2)(s_1a_3).
\end{aligned}$$

Thus $\sim$ is in fact an equivalence relation.

Step 2: Addition and multiplication defined in (144) are well-defined. Suppose $a_1/s_1 = a_1'/s_1'$ and $a_2/s_2 = a_2'/s_2'$. Choose $s_1'', s_2'' \in S$ such that

$$s_1''s_1'a_1 = s_1''s_1a_1' \quad \text{and} \quad s_2''s_2'a_2 = s_2''s_2a_2'.$$

Then $s_1''s_2'' \in S$ and

$$\begin{aligned}
s_1''s_2''(s_2a_1 + s_1a_2)s_1's_2' &= s_2''s_2(s_1''s_1'a_1)s_2' + s_1''s_1(s_2''s_2'a_2)s_1' \\
&= s_2''s_2(s_1''s_1a_1')s_2' + s_1''s_1(s_2''s_2a_2')s_1' \\
&= s_2''s_2(s_1''s_1a_1')s_2' + s_1''s_1(s_2''s_2a_2')s_1' \\
&= s_1''s_2''(s_2'a_1' + s_1'a_2')s_1s_2
\end{aligned}$$

implies

$$\frac{s_2a_1 + s_1a_2}{s_1s_2} = \frac{s_2'a_1' + s_1'a_2'}{s_1's_2'}.$$

Similarly, $s_1''s_2''$ and

$$\begin{aligned}
s_1''s_2''a_1a_2s_1's_2' &= (s_1''s_1'a_1)(s_2''s_2'a_2) \\
&= (s_1''s_1a_1')(s_2''s_2a_2') \\
&= s_1''s_2''a_1'a_2's_1s_2
\end{aligned}$$

implies

$$\frac{a_1a_2}{s_1s_2} = \frac{a_1'a_2'}{s_1's_2'}.$$

Thus we have shown that addition and multiplication in (144) are well-defined.

Step 3: Now we check that addition and multiplication in (144) gives us a ring structure. First let us show that addition in (144) gives us an abelian group with $0/1$ being the additive identity. We begin by checking associativity. Let $a_1/s_1, a_2/s_2, a_3/s_3 \in R_S$. Then

$$\begin{aligned}
\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}\right) + \frac{a_3}{s_3} &= \frac{s_2a_1 + s_1a_2}{s_1s_2} + \frac{a_3}{s_3} \\
&= \frac{s_3(s_2a_1 + s_1a_2) + (s_1s_2)a_3}{(s_1s_2)s_3} \\
&= \frac{s_3(s_2a_1) + s_3(s_1a_2) + (s_1s_2)a_3}{s_1(s_2s_3)} \\
&= \frac{(s_2s_3)a_1 + s_1(s_3a_2) + s_1(s_2a_3)}{s_1(s_2s_3)} \\
&= \frac{(s_2s_3)a_1 + s_1(s_3a_2 + s_2a_3)}{s_1(s_2s_3)} \\
&= \frac{a_1}{s_1} + \frac{s_3a_2 + s_2a_3}{s_2s_3} \\
&= \frac{a_1}{s_1} + \left(\frac{a_2}{s_2} + \frac{a_3}{s_3}\right).
\end{aligned}$$

Thus addition in (144) is associative. Now we check commutativity. Let $a_1/s_1, a_2/s_2 \in R_S$. Then

$$\begin{aligned}
\frac{a_1}{s_1} + \frac{a_2}{s_2} &= \frac{s_2a_1 + s_1a_2}{s_1s_2} \\
&= \frac{s_1a_2 + s_2a_1}{s_2s_1} \\
&= \frac{a_2}{s_2} + \frac{a_1}{s_1}.
\end{aligned}$$

Thus addition in (144) is commutative. Now we check that $0/1$ is the identity. Let $a/s \in R_S$. Then

$$\begin{aligned}
\frac{0}{1} + \frac{a}{s} &= \frac{s \cdot 0 + 1 \cdot a}{1 \cdot s} \\
&= \frac{0 + a}{s} \\
&= \frac{a}{s}.
\end{aligned}$$

Thus addition in (144) is commutative. Thus $0/1$ is the identity. Finally we check that every element has an inverse. Let $a/s \in R_S$. Then

$$\begin{aligned}
\frac{a}{s} + \frac{-a}{s} &= \frac{a - a}{s} \\
&= \frac{0}{s} \\
&= \frac{0}{1}.
\end{aligned}$$

implies $-a/s$ is the inverse to a/s. Therefore $(R_S, +)$ forms an abelian group with $0/1$ being identity element.

Now let us show that $(R_S, +, \cdot)$ is a ring. We first check that multiplication in (144) is associative. Let

$a_1/s_1, a_2/s_2, a_3/s_3 \in R_S$. Then

$$\begin{aligned}\left(\frac{a_1}{s_1}\frac{a_2}{s_2}\right)\frac{a_3}{s_3} &= \frac{a_1a_2}{s_1s_2}\frac{a_3}{s_3} \\ &= \frac{(a_1a_2)a_3}{(s_1s_2)s_3} \\ &= \frac{a_1(a_2a_3)}{s_1(s_2s_3)} \\ &= \frac{a_1}{s_1}\frac{a_2a_3}{s_2s_3} \\ &= \frac{a_1}{s_1}\left(\frac{a_2}{s_2}\frac{a_3}{s_3}\right).\end{aligned}$$

Therefore multiplication in (144) is associative. Next we check that multiplication in (144) distributes over addition. Let $a_1/s_1, a_2/s_2, a_3/s_3 \in R_S$. Then

$$\begin{aligned}\frac{a_1}{s_1}\left(\frac{a_2}{s_2}+\frac{a_3}{s_3}\right) &= \frac{a_1}{s_1}\left(\frac{s_3a_2+s_2a_3}{s_2s_3}\right) \\ &= \frac{a_1(s_3a_2+s_2a_3)}{s_1s_2s_3} \\ &= \frac{a_1s_3a_2+a_1s_2a_3}{s_1s_2s_3} \\ &= \frac{s_3a_1a_2+s_2a_1a_3}{s_1s_2s_3} \\ &= \frac{s_3a_1a_2}{s_1s_2s_3}+\frac{s_2a_1a_3}{s_1s_2s_3} \\ &= \frac{a_1a_2}{s_1s_2}+\frac{a_1a_3}{s_1s_3} \\ &= \frac{a_1}{s_1}\frac{a_2}{s_2}+\frac{a_1}{s_1}\frac{a_3}{s_3}\end{aligned}$$

Thus multiplication in (144) distributes over addition. Finally, let us check that $1/1$ is the identity element in R_S under multplication. Let $a/s \in R_S$. Then

$$\begin{aligned}\frac{1}{1}\cdot\frac{a}{s} &= \frac{1\cdot a}{1\cdot s} \\ &= \frac{a}{s}.\end{aligned}$$

Thus $1/1$ is the identity element in R_S under multiplication.

Step 4: For the final step, we prove that $\rho_S \colon R \to R_S$ is a ring homomorphism. First note that it sends the identity to the identity. Next, let $a, b \in R$. Then

$$\begin{aligned}\rho_S(a+b) &= \frac{a+b}{1} \\ &= \frac{1\cdot a+1\cdot b}{1\cdot 1} \\ &= \frac{a}{1}+\frac{b}{1} \\ &= \rho_S(a)+\rho_S(b)\end{aligned}$$

and

$$\begin{aligned}\rho_S(ab) &= \frac{ab}{1} \\ &= \frac{ab}{1\cdot 1} \\ &= \frac{a}{1}\cdot\frac{b}{1} \\ &= \rho_S(a)\rho_S(b).\end{aligned}$$

Thus ρ_S is a ring homomorphism. $\square$

45.2.1 Universal Mapping Property of Localization

Proposition 45.4. *Let S be a multiplicatively closed subset of a ring A and let $\varphi\colon A \to B$ be a ring homomorphism such that $\varphi(S) \subseteq B^\times$. Then there exists a unique ring homomorphism $\widetilde{\varphi}\colon A_S \to B$ such that $\widetilde{\varphi}\rho_S = \varphi$.*

Proof. We define $\widetilde{\varphi}\colon A_S \to B$ by

$$\widetilde{\varphi}\left(\frac{a}{s}\right) = \varphi(a)\varphi(s)^{-1} \tag{145}$$

for all $a/s \in A_S$. We need to verify that (145) is well-defined. Suppose $a'/s' = a/s$. Choose $s'' \in S$ such that $s''sa' = s''s'a$. Then $\varphi(a') = \varphi(s'')\varphi(s')\varphi(s'')^{-1}\varphi(s)^{-1}\varphi(a)$ in B, and so

$$\begin{aligned}
\widetilde{\varphi}\left(\frac{a'}{s'}\right) &= \varphi(a')\varphi(s')^{-1} \\
&= \varphi(s'')\varphi(s')\varphi(s'')^{-1}\varphi(s)^{-1}\varphi(a)\varphi(s')^{-1} \\
&= \varphi(a)\varphi(s)^{-1} \\
&= \widetilde{\varphi}\left(\frac{a}{s}\right).
\end{aligned}$$

Thus (145) is well-defined. It is also easily seen to be a ring homomorphism which satisfies

$$\begin{aligned}
(\widetilde{\varphi}\rho_S)(a) &= \widetilde{\varphi}(\rho_S(a)) \\
&= \widetilde{\varphi}\left(\frac{a}{1}\right) \\
&= \frac{\varphi(a)}{\varphi(1)} \\
&= \frac{\varphi(a)}{1} \\
&= \varphi(a).
\end{aligned}$$

for all $a \in A$. Thus $\widetilde{\varphi}\rho_S = \varphi$. This shows existence.

For uniqueness, suppose $\widetilde{\varphi}$ and $\widetilde{\varphi}'$ are two such maps. Then we have

$$\begin{aligned}
\widetilde{\varphi}\left(\frac{a}{s}\right) &= \widetilde{\varphi}\left(\frac{1}{s}\cdot\frac{a}{1}\right) \\
&= \widetilde{\varphi}\left(\frac{1}{s}\right)\widetilde{\varphi}\left(\frac{a}{1}\right) \\
&= \left(\widetilde{\varphi}\left(\frac{s}{1}\right)\right)^{-1}\widetilde{\varphi}\left(\frac{a}{1}\right) \\
&= \left(\widetilde{\varphi}'\left(\frac{s}{1}\right)\right)^{-1}\widetilde{\varphi}'\left(\frac{a}{1}\right) \\
&= \widetilde{\varphi}'\left(\frac{1}{s}\right)\widetilde{\varphi}'\left(\frac{a}{1}\right) \\
&= \widetilde{\varphi}'\left(\frac{1}{s}\cdot\frac{a}{1}\right) \\
&= \widetilde{\varphi}'\left(\frac{a}{s}\right)
\end{aligned}$$

for all $a/s \in A_S$. Thus $\widetilde{\varphi} = \widetilde{\varphi}'$. □

45.2.2 Properties of ρ_S

Proposition 45.5. *Let S be a multiplicatively closed subset of R. Then*

1. *ρ_S is injective if and only if S does not contain any zero divisors;*
2. *ρ_S is an isomorphism if and only if S consists of units.*

Proof. 1. Suppose ρ_S is injective and assume for a contradiction that S contains a zero divisor, say $s \in S$ with $st = 0$ for some $t \in R\backslash\{0\}$. Then observe that $t \neq 0$ but $t/1 = 0$ since $st = 0$ where $s \in S$. This contradicts the fact that ρ_S is injective.

Conversely, suppose S does not contain any zero divisors and assume for a contradiction that ρ_S is not injective. Choose $t \in R\backslash\{0\}$ such that $t/1 = 0$. Then there exists an $s \in S$ such that $st = 0$. This implies s is a zero divisor, which contradicts the fact that S does not contain any zero divisors.

2. By the universal mapping property of localization applied to the identity map $1_R \colon R \to R$, there exists a ring homomorphism $\psi \colon R_S \to R$ such that $\psi\rho_S = 1_R$. Applying the universal mapping property of localization to the map $\rho_S \colon R \to R_S$, we see that $1_{R_S} \colon R_S \to R_S$ is the *unique* homomorphism which satisfies $1_{R_S}\rho_S = \rho_S$, but observe that we also have

$$\begin{aligned}(\rho_S\psi)\rho_S &= \rho_S(\psi\rho_S) \\ &= \rho_S 1_R \\ &= \rho_S.\end{aligned}$$

Thus by uniqueness, we have $1_{R_S} = \rho_S\psi$. It follows that ρ_S is an isomorphism with ψ being its inverse. □

45.2.3 Prime Ideals in R_S

Recall that we denote by $\operatorname{Spec} R$ to be the set of all prime ideals in R. If S is a multiplicatively closed subset of R, then we can give a simple description of $\operatorname{Spec} R_S$ in terms of a subset of $\operatorname{Spec} R$.

Theorem 45.1. *Let S be a multiplicatively closed subset of R. Then we have a bijection*

$$\Psi \colon \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \varnothing\} \to \operatorname{Spec} R_S$$

given by $\Psi(\mathfrak{p}) = \mathfrak{p}_S$ for all prime ideals $\mathfrak{p}$ in R such that $\mathfrak{p} \cap S = \varnothing$. Then inverse to Ψ, which we denote by

$$\Phi \colon \operatorname{Spec} R_S \to \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \varnothing\}$$

is given by $\Phi(\mathfrak{q}) = \rho^{-1}(\mathfrak{q})$ for all prime ideals $\mathfrak{q}$ in R_S where $\rho \colon R \to R_S$ is the canonical localization map.

Proof. First note that both Ψ and Φ land in their designated target spaces. Indeed, for any prime ideal $\mathfrak{q}$ in $\operatorname{Spec} R_S$, the ideal $\rho^{-1}(\mathfrak{q})$ is easily seen to be prime in R. Also if $\mathfrak{p}$ is a prime ideal in R such that $\mathfrak{p} \cap S = \varnothing$, then $\mathfrak{p}_S$ is a prime ideal in R_S. Indeed, let $x/s, y/t \in \mathfrak{p}_S$, where $x, y \in \mathfrak{p}$ and $s, t \in S$, and suppose $(x/s)(y/t) \in \mathfrak{p}_S$. Then $xy/st \in \mathfrak{p}_S$, which implies $xy \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we have either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Without loss of generality, say $x \in \mathfrak{p}$. Then clearly $x/s \in \mathfrak{p}_S$. This implies $\mathfrak{p}_S$ is prime.

We now want to show that these two maps are inverse to each other. First let us show that Ψ is injective. Let $\mathfrak{p}$ and $\mathfrak{p}'$ be two distinct primes in R such that $\mathfrak{p} \cap S = \mathfrak{p}' \cap S = \varnothing$. Without loss of generality, say $\mathfrak{p} \not\subseteq \mathfrak{p}'$. Choose $x \in \mathfrak{p} \backslash \mathfrak{p}'$. Then observe that $x/1 \in \mathfrak{p}_S$. Furthermore, we also have $x/1 \notin \mathfrak{p}'_S$. Indeed, assume for a contradiction $x/1 \in \mathfrak{p}'_S$. Then $x/1 = y/s$ with $y \in \mathfrak{p}'_S$ and $s \in S$. Then there exists $t \in S$ such that $tsx = ty \in \mathfrak{p}'$. As $\mathfrak{p}'$ is prime and $s, t \notin \mathfrak{p}'$, we must have $x \in \mathfrak{p}'$, which is a contradiction. This shows that $\mathfrak{p}_S$ and $\mathfrak{p}'_S$ are distinct, and hence Ψ is injective.

Now we will show Ψ is surjective. Let $\mathfrak{q} \in \operatorname{Spec} R_S$. We claim that $\mathfrak{q} = \rho^{-1}(\mathfrak{q})_S$. Indeed, we have

$$\begin{aligned}\rho^{-1}(\mathfrak{q})_S &= \{x/s \mid x \in \rho^{-1}(\mathfrak{q}) \text{ and } s \in S\} \\ &= \{x/s \mid x/1 \in \mathfrak{q} \text{ and } s \in S\} \\ &= \mathfrak{q},\end{aligned}$$

where equality in the last line follows from the fact that $\mathfrak{q}$ is prime: if $x/s \in \mathfrak{q}$, then $x/1 \in \mathfrak{q}$ since $1/s \notin \mathfrak{q}$ and $x/s = (x/1)(1/s)$. Thus Ψ is surjective and hence a bijection. In proving that Ψ is surjective, we also see that the inverse of Ψ is Φ. □

45.3 Localization of module with respect to multiplicatively closed set

Definition 45.3. Let S be a multiplicatively closed subset of R and let M be an R-module. We define the **localization of M with respect to S**, denoted M_S or $S^{-1}M$, as follows: as a set M_S is given by

$$M_S := \left\{ \frac{u}{s} \mid u \in M, s \in S \right\}$$

where u/s denotes the equivalence class of $(u, s) \in M \times S$ with respect to the following equivalence relation:

$$(u, s) \sim (u', s') \text{ if and only if there exists } s'' \in S \text{ such that } s''s'u = s''su'. \tag{146}$$

We give M_S an R_S-module structure by ring defining addition and scalar multiplication on M_S by

$$\frac{u_1}{s_1} + \frac{u_2}{s_2} = \frac{s_2u_1 + s_1u_2}{s_1s_2} \quad \text{and} \quad \frac{a}{s}\frac{u}{t} = \frac{au}{st}, \tag{147}$$

for $u_1/s_1, u_2/s_2, u/t \in M_S$ and $a/s \in R_S$, with $0/0$ being the additive identity in M_S.

Proposition 45.6. *With the notation above, M_S is an R_S-module. By restricting scalars via the ring the homomoprhism $\rho_S\colon R \to R_S$, it is also an R-module. More specifically, the R-module scalar multiplication is given by*

$$a \cdot \frac{u}{s} = \frac{au}{s}$$

for all $a \in R$ and $u/s \in M_S$.

Proof. The proof of this is similar to the proof of (78.1), but we include it here for completeness. Again, there are several things we need to check, so we break it up into steps.

Step 1: We show that the relation (143) is in fact a equivalence relation. First we show reflexivity of $\sim$. Let $(u,s) \in M \times S$. Then since $1 \in S$ and $1 \cdot su = 1 \cdot su$, we have $(u,s) \sim (u,s)$. Next we show symmetry of $\sim$. Suppose $(u,s) \sim (u',s')$. Choose $s'' \in S$ such that $s''s'u = s''su'$. Then by symmetry of equality, we have $s''su' = s''s'u$. Therefore $(u',s') \sim (u,s)$. Finally, we show transitivity of $\sim$. Suppose $(u_1,s_1) \sim (u_2,s_2)$ and $(u_2,s_2) \sim (u_3,s_3)$. Choose $s_{12}, s_{23} \in S$ such that

$$s_{12}s_2u_1 = s_{12}s_1u_2 \quad \text{and} \quad s_{23}s_3u_2 = s_{23}s_2u_3$$

Then $s_{23}s_{12}s_2 \in S$ and

$$\begin{aligned}
(s_{23}s_{12}s_2)(s_3u_1) &= s_{23}(s_{12}s_2u_1)s_3 \\
&= s_{23}(s_{12}s_1u_2)s_3 \\
&= s_{12}s_1(s_{23}s_3u_2) \\
&= s_{12}s_1(s_{23}s_2u_3) \\
&= (s_{12}s_{23}s_2)(s_1u_3).
\end{aligned}$$

Thus $\sim$ is in fact an equivalence relation.

Step 2: Addition and multiplication in (147) are well-defined. Suppose $u_1/s_1 = u_1'/s_1'$ and $u_2/s_2 = u_2'/s_2'$. Choose $s_1'', s_2'' \in S$ such that

$$s_1''s_1'u_1 = s_1''s_1u_1' \quad \text{and} \quad s_2''s_2'u_2 = s_2''s_2u_2'.$$

Then $s_1''s_2'' \in S$ and

$$\begin{aligned}
s_1''s_2''(s_2u_1 + s_1u_2)s_1's_2' &= s_2''s_2(s_1''s_1'u_1)s_2' + s_1''s_1(s_2''s_2'u_2)s_1' \\
&= s_2''s_2(s_1''s_1u_1')s_2' + s_1''s_1(s_2''s_2u_2')s_1' \\
&= s_2''s_2(s_1''s_1u_1')s_2' + s_1''s_1(s_2''s_2u_2')s_1' \\
&= s_1''s_2''(s_2'u_1' + s_1'u_2')s_1s_2
\end{aligned}$$

implies

$$\frac{s_2u_1 + s_1u_2}{s_1s_2} = \frac{s_2'u_1' + s_1'u_2'}{s_1's_2'}.$$

Similarly, $s_1''s_2'' \in S$ and

$$\begin{aligned}
s_1''s_2''u_1u_2s_1's_2' &= (s_1''s_1'u_1)(s_2''s_2'u_2) \\
&= (s_1''s_1u_1')(s_2''s_2u_2') \\
&= s_1''s_2''u_1'u_2's_1s_2
\end{aligned}$$

implies

$$\frac{a_1a_2}{s_1s_2} = \frac{a_1'a_2'}{s_1's_2'}.$$

Thus we have shown that addition and scalar multiplication in (147) are well-defined.

Step 3: Now we show that addition and multiplication in (147) gives us an R_S-module structure. First let us show that addition in (147) gives us an abelian group with $0/1$ being the additive identity. We begin by checking associativity. Let $u_1/s_1, u_2/s_2, u_3/s_3 \in M_S$. Then

$$\begin{aligned}
\left(\frac{u_1}{s_1}+\frac{u_2}{s_2}\right)+\frac{u_3}{s_3} &= \frac{s_2u_1+s_1u_2}{s_1s_2}+\frac{u_3}{s_3} \\
&= \frac{s_3(s_2u_1+s_1u_2)+(s_1s_2)u_3}{(s_1s_2)s_3} \\
&= \frac{s_3(s_2u_1)+s_3(s_1u_2)+(s_1s_2)u_3}{s_1(s_2s_3)} \\
&= \frac{(s_2s_3)u_1+s_1(s_3u_2)+s_1(s_2u_3)}{s_1(s_2s_3)} \\
&= \frac{(s_2s_3)u_1+s_1(s_3u_2+s_2u_3)}{s_1(s_2s_3)} \\
&= \frac{u_1}{s_1}+\frac{s_3u_2+s_2u_3}{s_2s_3} \\
&= \frac{u_1}{s_1}+\left(\frac{u_2}{s_2}+\frac{u_3}{s_3}\right).
\end{aligned}$$

Thus addition in (147) is associative. Now we check commutativity. Let $u_1/s_1, u_2/s_2 \in M_S$. Then

$$\begin{aligned}
\frac{u_1}{s_1}+\frac{u_2}{s_2} &= \frac{s_2u_1+s_1u_2}{s_1s_2} \\
&= \frac{s_1u_2+s_2u_1}{s_2s_1} \\
&= \frac{u_2}{s_2}+\frac{u_1}{s_1}.
\end{aligned}$$

Thus addition in (147) is commutative. Now we check that $0/1$ is the identity. Let $u/s \in M_S$. Then

$$\begin{aligned}
\frac{0}{1}+\frac{u}{s} &= \frac{s\cdot 0+1\cdot u}{1\cdot s} \\
&= \frac{0+u}{s} \\
&= \frac{u}{s}.
\end{aligned}$$

Thus $0/1$ is the identity. Finally we check that every element has an inverse. Let $u/s \in M_S$. Then

$$\begin{aligned}
\frac{u}{s}+\frac{-u}{s} &= \frac{u-u}{s} \\
&= \frac{0}{s} \\
&= \frac{0}{1}.
\end{aligned}$$

implies $-u/s$ is the inverse to u/s. Therefore $(M_S,+)$ forms an abelian group with $0/1$ being the identity element.

Now let us show that $(M_S,+,\cdot)$ is an R_S-module. We first check that scalar multiplication in (147) is associative. Let $a_1/s_1, a_2/s_2 \in R_S$ and let $u/s \in M_S$. Then

$$\begin{aligned}
\left(\frac{a_1}{s_1}\frac{a_2}{s_2}\right)\frac{u}{s} &= \frac{a_1a_2}{s_1s_2}\frac{u}{s} \\
&= \frac{(a_1a_2)u}{(s_1s_2)s} \\
&= \frac{a_1(a_2u)}{s_1(s_2s)} \\
&= \frac{a_1}{s_1}\frac{a_2u}{s_2s} \\
&= \frac{a_1}{s_1}\left(\frac{a_2}{s_2}\frac{u}{s}\right).
\end{aligned}$$

Therefore scalar multiplication in (147) is associative. Next we check that scalar multiplication in (147) distributes over addition. Let $a/s \in R_S$ and $u_1/s_1, u_2/s_2 \in M_S$. Then

$$\begin{aligned}
\frac{a}{s}\left(\frac{u_1}{s_1}+\frac{u_2}{s_2}\right) &= \frac{a}{s}\left(\frac{s_2u_1+s_1u_2}{s_1s_2}\right)\\
&= \frac{a(s_2u_1+s_1u_2)}{ss_1s_2}\\
&= \frac{as_2u_1+as_1u_2}{ss_1s_2}\\
&= \frac{s_2au_1+sau_2}{ss_1s_2}\\
&= \frac{s_2au_1}{ss_1s_2}+\frac{sau_2}{ss_1s_2}\\
&= \frac{au_1}{ss_1}+\frac{au_2}{ss_2}\\
&= \frac{a}{s}\frac{u_1}{s_1}+\frac{a}{s}\frac{u_2}{s_2}.
\end{aligned}$$

Similarly, let $a_1/s_1, a_2/s_2 \in R_S$ and $u/s \in M_S$. Then

$$\begin{aligned}
\left(\frac{a_1}{s_1}+\frac{a_2}{s_2}\right)\frac{u}{s} &= \left(\frac{s_2a_1+s_1a_2}{s_1s_2}\right)\frac{u}{s}\\
&= \frac{(s_2a_1+s_1a_2)u}{s_1s_2s}\\
&= \frac{s_2a_1u+s_1a_2u}{s_1s_2s}\\
&= \frac{s_2a_1u+s_1a_2u}{s_2s_1s}\\
&= \frac{s_2a_1u}{s_2s_1s}+\frac{s_1a_2u}{s_1s_2s}\\
&= \frac{a_1u}{s_1s}+\frac{a_2u}{s_2s}\\
&= \frac{a_1}{s_1}\frac{u}{s}+\frac{a_2}{s_2}\frac{u}{s}.
\end{aligned}$$

Thus multiplication in (147) distributes over addition. Finally, let us check that $1/1$ fixes M_S. Let $u/s \in M_S$. Then

$$\begin{aligned}
\frac{1}{1}\cdot\frac{u}{s} &= \frac{1\cdot u}{1\cdot s}\\
&= \frac{u}{s}.
\end{aligned}$$

Thus $1/1$ fixes M_S. □

45.4 Localization as a functor

Proposition 45.7. *Let S be a multiplicatively closed subset of R. We obtained a functor*

$$-_S\colon \mathbf{Mod}_R \to \mathbf{Mod}_{R_S}$$

*called **localization** where an R-module M is mapped to the R_S-module M_S and where the R-linear map $\varphi\colon M \to N$ is mapped to the R_S-linear map $\varphi_S\colon M_S \to N_S$ given by*

$$\varphi_S\left(\frac{u}{s}\right) = \frac{\varphi(u)}{s} \tag{148}$$

for all $u/s \in M_S$.

Proof. We first check that (148) is well-defined. Suppose $u/s = u'/s'$. Choose $s'' \in S$ such that $s''s'u = s''su'$. Then $s''s'\varphi(u) = s''s\varphi(u')$ by R-linearity of φ, and hence $\varphi(u)/s = \varphi(u')/s'$. Thus (148) is well-defined.

Now let us check that φ_S is an R_S-linear map. Let $a_1/s_1, a_2/s_2 \in R_S$ and let $u_1/t_1, u_2/t_2 \in M_S$. Then

$$\begin{aligned}
\varphi_S\left(\frac{a_1}{s_1}\frac{u_1}{t_1} + \frac{a_2}{s_2}\frac{u_2}{t_2}\right) &= \varphi_S\left(\frac{s_2t_2a_1u_1 + s_1t_1a_2u_2}{s_1t_1s_2t_2}\right) \\
&= \frac{\varphi(s_2t_2a_1u_1 + s_1t_1a_2u_2)}{s_1t_1s_2t_2} \\
&= \frac{s_2t_2a_1\varphi(u_1) + s_1t_1a_2\varphi(u_2)}{s_1t_1s_2t_2} \\
&= \frac{a_1}{s_1}\frac{\varphi(u_1)}{t_1} + \frac{a_2}{s_2}\frac{\varphi(u_2)}{t_2} \\
&== \frac{a_1}{s_1}\varphi_S\left(\frac{u_1}{t_1}\right) + \frac{a_2}{s_2}\varphi_S\left(\frac{u_2}{t_2}\right).
\end{aligned}$$

Thus φ_S is an R_S-linear map.

Now to see that $-_S$ is a functor, we need to check that it preserves identities and compositions. First we show it preserves identities. Let M be an R-module. Then

$$\begin{aligned}
(1_M)_S\left(\frac{u}{s}\right) &= \frac{1_M(u)}{s} \\
&= \frac{u}{s} \\
&= 1_{M_S}\left(\frac{u}{s}\right)
\end{aligned}$$

for all $u/s \in M_S$. Thus $(1_M)_S = 1_{M_S}$, and hence $-_S$ preserves identities. Next we show it preserves compositions. Let $\varphi\colon M \to M'$ and $\varphi'\colon M' \to M''$ be two R-linear maps. Then

$$\begin{aligned}
(\varphi'\varphi)_S\left(\frac{u}{s}\right) &= \frac{(\varphi'\varphi)(u)}{s} \\
&= \frac{\varphi'(\varphi(u))}{s} \\
&= \varphi'_S\left(\frac{\varphi(u)}{s}\right) \\
&= \varphi'_S\left(\varphi_S\left(\frac{u}{s}\right)\right) \\
&= (\varphi'_S\varphi_S)\left(\frac{u}{s}\right)
\end{aligned}$$

for all $u/s \in M_S$. Thus $(\varphi'\varphi)_S = \varphi'_S\varphi_S$, and hence $-_S$ preserves compositions. □

45.4.1 Natural isomorphism between functors $R_S \otimes_R -$ and $-_S$

Lemma 45.2. *Let N be an R-module. Every element in $R_S \otimes_R N$ can be expressed as an elementary tensor of the form $(1/s) \otimes v$ with $s \in S$ and $v \in N$.*

Proof. Let $\sum_{i=1}^n (a_i/s_i) \otimes v_i$ be a general tensor in $R_S \otimes_R N$. Then

$$\begin{aligned}
\frac{a_1}{s_1} \otimes v_1 + \cdots + \frac{a_n}{s_n} \otimes v_n &= \frac{a_1s_2\cdots s_n}{s_1s_2\cdots s_n} \otimes v_1 + \cdots + \frac{s_1s_2\cdots a_n}{s_1s_2\cdots s_n} \otimes v_n \\
&= \frac{1}{s_1s_2\cdots s_n} \otimes a_1s_2\cdots s_nv_1 + \cdots + \frac{1}{s_1s_2\cdots s_n} \otimes s_1s_2\cdots a_nv_n \\
&= \frac{1}{s_1s_2\cdots s_n} \otimes (a_1s_2\cdots s_nv_1 + \cdots + s_1s_2\cdots a_nv_n) \\
&= \frac{1}{s} \otimes v,
\end{aligned}$$

where $s = s_1s_2\cdots s_n$ and $v = a_1s_2\cdots s_nv_1 + \cdots + s_1s_2\cdots a_nv_n$. □

Proposition 45.8. *Let S be a multiplicatively closed subset of R. Then we have a natural isomorphism between functors*

$$R_S \otimes_R -\colon \mathbf{Mod}_R \to \mathbf{Mod}_{R_S} \quad \textit{and} \quad -_S\colon \mathbf{Mod}_R \to \mathbf{Mod}_{R_S}$$

Proof. For each R-module M, we define $\eta_M\colon R_S \otimes_R M \to M_S$ by

$$\eta_M\left(\frac{1}{s} \otimes u\right) = \frac{u}{s}$$

for all $(1/s) \otimes u \in R_S \otimes_R M$. By Lemma (45.2), every tensor in $R_S \otimes_R M$ can be expressed as an elementary tensor of the form $(1/s) \otimes u$, and so η_M really is defined on all of $R_S \otimes_R M$. Also η_M is a well-defined R-linear map since the map $R_S \times M \to M_S$ given by

$$\left(\frac{1}{s}, u\right) \mapsto \frac{u}{s}$$

is readily seen to be R-bilinear. The map η_M is surjective since every element in M_S can be expressed in the form u/s. Let us show that η_M is injective. Suppose $(1/s) \otimes u \in \ker \eta_M$. Then $u/s = 0/1$. Then exists a $t \in S$ such that

$$\begin{aligned} tu &= t \cdot 1 \cdot u \\ &= t \cdot s \cdot 0 \\ &= 0. \end{aligned}$$

This implies

$$\begin{aligned} \frac{1}{s} \otimes u &= \frac{t}{st} \otimes u \\ &= \frac{1}{st} \otimes tu \\ &= \frac{1}{st} \otimes 0 \\ &= 0. \end{aligned}$$

Thus η_M is injective, and hence an isomorphism.

Now we will show that η is a natural transformation. Let $\varphi\colon M \to N$ be an R-linear map. We need to show that the diagram below commutes

$$\begin{tikzcd} R_S \otimes_R M \arrow[r, "\eta_M"] \arrow[d, "1\otimes\varphi"'] & M_S \arrow[d, "\varphi_S"] \\ R_S \otimes_R N \arrow[r, "\eta_N"'] & N_S \end{tikzcd} \tag{149}$$

Let $(1/s) \otimes u \in R_S \otimes_R M$. Then

$$\begin{aligned} (\varphi_S \eta_M)\left(\frac{1}{s} \otimes u\right) &= \varphi_S\left(\eta_M\left(\frac{1}{s} \otimes u\right)\right) \\ &= \varphi_S\left(\frac{u}{s}\right) \\ &= \frac{\varphi(u)}{s} \\ &= \eta_N\left(\frac{1}{s} \otimes \varphi(u)\right) \\ &= \eta_N\left((1 \otimes \varphi)\left(\frac{1}{s} \otimes u\right)\right) \\ &= (\eta_N(1 \otimes \varphi))\left(\frac{1}{s} \otimes u\right). \end{aligned}$$

Therefore the diagram (327) commutes. □

45.4.2 Localization is Essentially Surjective

Proposition 45.9. *Let S be a multiplicatively closed subset of R. Then the localization functor $-_S$ is essentially surjective.*

Proof. Let M be an R_S-module. Then M is also an R-module via the action

$$a \cdot u = \frac{a}{1} \cdot u$$

for all $a \in R$ and $u \in M$. Then $R_S \otimes_R M$ is an R_S-module via the action

$$\frac{a}{s} \cdot \left(\frac{b}{t} \otimes u\right) = \frac{ab}{st} \otimes u$$

for all a/s and b/t in R_S and for all $u \in M$. We claim that M is isomorphic to $R_S \otimes_R M$ as R_S-modules. Indeed, let $\varphi\colon R_S \otimes_R M \to M$ be given by

$$\varphi\left(\frac{1}{s} \otimes u\right) = \frac{1}{s} \cdot u$$

for all $(1/s) \otimes u \in R_S \otimes M$. This map is well-defined and R-linear since the corresponding map $R_S \times M \to M$, given by

$$\left(\frac{a}{s}, u\right) \mapsto \frac{a}{s} \cdot u$$

is R-bilinear. This map is injective since if $(1/s) \cdot u = 0$, then $u = 0$, which implies $(1/s) \otimes u = 0$. Finally, the map is surjective since if $u \in M$, then $\varphi((1/1) \otimes u) = u$. Therefore localization is essentially surjective since $M_S \cong R_S \otimes_R M$. □

45.5 Properties of Localization

The following proposition is used quite often:

Proposition 45.10. *Let N be an R-mdoule and let L and M be R-submodules of N. The following are equivalent:*

1. *$L = M$;*
2. *$L_{\mathfrak{p}} = M_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \subseteq R$;*
3. *$L_{\mathfrak{m}} = M_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m} \subseteq R$.*

Proof. That 1 implies 2 and that 2 implies 3 are obvious. So it suffices to show 3 implies 1. First we show $M \subseteq L$. Let $u \in M$. If $L :_R u = R$, then $u \in L$ (since $1 \cdot u \in L$). Otherwise $L :_R u$ is contained in some maximal ideal $\mathfrak{m}$. Then observe that $u/1 \notin L_{\mathfrak{m}}$. Indeed, we have $u/1 \in L_{\mathfrak{m}}$ if and only if there exists an $s \in R \backslash \mathfrak{m}$ such that $su \in L$, but since $\mathfrak{m}$ is the set of all such s, we see that $u/1 \notin L_{\mathfrak{m}}$. This contradicts the fact that $M_{\mathfrak{m}} = L_{\mathfrak{m}}$. Thus we must have $L :_R u = R$, which implies $u \in L$. Thus $M \subseteq L$. The reverse inclusion is proved similarly. □

45.5.1 Localization Commutes with Arbitrary Sums, Finite Intersections, and Radicals

Proposition 45.11. *Let $S \subseteq R$ be a multiplicative set, let M be an R-modules, and let $\{M_\lambda\}$ be a collection of R-submodules of M indexed over a set Λ. Then*

1. *Localization commutes with arbitrary sums: $(\sum_{\lambda \in \Lambda} M_\lambda)_S = \sum_{\lambda \in \Lambda} (M_\lambda)_S$.*
2. *Localization commutes with finite intersections: if $\Lambda = \{1, \dots, n\}$ is finite, then $(\bigcap_{i=1}^n M_i)_S = \bigcap_{i=1}^n (M_i)_S$.*
3. *Localization commutes with radicals: let $I \subseteq R$ be an ideal. Then $(\sqrt{I})_S = \sqrt{I_S}$.*

Proof.
1. Let $u/s \in (\sum_{\lambda \in \Lambda} M_\lambda)_S$. So $s \in S$ and $u \in \sum_{\lambda \in \Lambda} M_\lambda$, which means we can express it in the form

$$u = u_{\lambda_1} + \cdots + u_{\lambda_n}$$

where $u_{\lambda_i} \in M_{\lambda_i}$ for all $1 \leq i \leq n$. Then

$$\begin{aligned} \frac{u}{s} &= \frac{u_{\lambda_1} + \cdots + u_{\lambda_n}}{s} \\ &= \frac{u_{\lambda_1}}{s} + \cdots + \frac{u_{\lambda_n}}{s} \\ &\in \sum_{\lambda \in \Lambda} (M_\lambda)_S. \end{aligned}$$

Therefore $(\sum_{\lambda \in \Lambda} M_\lambda)_S \subseteq \sum_{\lambda \in \Lambda} (M_\lambda)_S$.

Conversely, suppose $\sum_{i=1}^n u_{\lambda_i}/s_{\lambda_i} \in \sum_{\lambda \in \Lambda} (M_\lambda)_S$ where $u_{\lambda_i} \in M_{\lambda_i}$ and $s_{\lambda_i} \in S$ for all $1 \leq i \leq n$. Then

$$\begin{aligned} \sum_{i=1}^n \frac{u_{\lambda_i}}{s_{\lambda_i}} &= \sum_{i=1}^n \frac{s_{\lambda_1} \cdots s_{\lambda_{i-1}} u_{\lambda_i} s_{\lambda_{i+1}} \cdots s_{\lambda_{jn}}}{s_{\lambda_1} \cdots s_{\lambda_n}} \\ &= \frac{1}{s_{\lambda_1} \cdots s_{\lambda_n}} \sum_{i=1}^n s_{\lambda_1} \cdots s_{\lambda_{i-1}} u_{\lambda_i} s_{\lambda_{i+1}} \cdots s_{\lambda_{jn}} \\ &\in \left(\sum_{\lambda \in \Lambda} M_\lambda\right)_S. \end{aligned}$$

Therefore $(\sum_{\lambda\in\Lambda} M_\lambda)_S \supseteq \sum_{\lambda\in\Lambda}(M_\lambda)_S$.

2. Let $u/s \in (\bigcap_{i=1}^n M_i)_S$. So $u \in \bigcap_{i=1}^n M_i$ and $s \in S$. This means $u \in M_i$ for all $1 \le i \le n$. Thus $u/s \in \bigcap_{i=1}^n (M_i)_S$. This implies $(\bigcap_{i=1}^n M_i)_S \subseteq \bigcap_{i=1}^n (M_i)_S$.

Conversely, let $u/s \in \bigcap_{i=1}^n (M_i)_S$. Then $u/s = u_i/s_i$ where $u_i \in M_i$ and $s_i \in S$ for all $1 \le i \le n$. For each $1 \le i \le n$, choose $s_i' \in S$ such that $s_i' s_i u = s_i' s u_i$. Then

$$\begin{aligned} \frac{u}{s} &= \frac{s_1' s_1 \cdots s_n' s_n u}{s_1' s_1 \cdots s_n' s_n s} \\ &\in \left(\bigcap_{i=1}^n M_i\right)_S. \end{aligned}$$

This implies $(\bigcap_{i=1}^n M_i)_S \supseteq \bigcap_{i=1}^n (M_i)_S$.

3. Let $x/s \in (\sqrt{I})_S$. Then $s \in S$ and $x \in \sqrt{I}$, which means $x^n \in I$ for some $n \in \mathbb{N}$. Then

$$\begin{aligned} \left(\frac{x}{s}\right)^n &= \frac{x^n}{s^n} \\ &\in I_S \end{aligned}$$

which implies $x/s \in \sqrt{I_S}$. Therefore $(\sqrt{I})_S \subseteq \sqrt{I_S}$.

Conversely, let $x/s \in \sqrt{I_S}$. Then $(x/s)^n \in I_S$ for some $n \in \mathbb{N}$. So $x^n \in I$, which implies $x \in \sqrt{I}$. Therefore $(\sqrt{I})_S \supseteq \sqrt{I_S}$. □

45.6 Total Ring of Fractions

Definition 45.4. Let A be a ring and let S be the set of all nonzerodivisors in A. We define the **total ring of fractions** of A to be $Q(A) := S^{-1}A$.

Proposition 45.12. *Let A be a ring and $B = A/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r)$ with $\mathfrak{p}_i \subset A$ prime ideals. Then*

$$Q(B) \cong \bigoplus_{i=1}^r Q(A/\mathfrak{p}_i).$$

In particular, $Q(B)$ is a direct sum of fields.

Proof. Let $S = A \backslash (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r)$. Then

$$\begin{aligned} S^{-1}B &= S^{-1}\left(A/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r)\right) \\ &\cong S^{-1}A/S^{-1}(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r) \\ &= S^{-1}A/(S^{-1}\mathfrak{p}_1 \cap \cdots \cap S^{-1}\mathfrak{p}_r) \\ &\cong \bigoplus_{i=1}^r \left(S^{-1}A/S^{-1}\mathfrak{p}_i\right) \\ &\cong \bigoplus_{i=1}^r \left(S^{-1}(A/\mathfrak{p}_i)\right) \end{aligned}$$

Finally, we have $S^{-1}B = \overline{S}^{-1}B = Q(B)$ and $S^{-1}(A/\mathfrak{p}_i) = \overline{S}^{-1}(A/\mathfrak{p}_i) = Q(A/\mathfrak{p}_i)$.

□

Let $S = A \backslash (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r)$. Then

$$\begin{aligned} S^{-1}B &= S^{-1}\left(A/(Q_1 \cap \cdots \cap Q_r)\right) \\ &\cong S^{-1}A/S^{-1}(Q_1 \cap \cdots \cap Q_r) \\ &= S^{-1}A/(S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_r) \\ &\cong \bigoplus_{i=1}^r \left(S^{-1}A/S^{-1}Q_i\right) \\ &\cong \bigoplus_{i=1}^r \left(S^{-1}(A/Q_i)\right) \end{aligned}$$

Finally, we have $S^{-1}B = \overline{S}^{-1}B = Q(B)$ and $S^{-1}(A/\mathfrak{p}_i) = \overline{S}^{-1}(A/\mathfrak{p}_i) = Q(A/\mathfrak{p}_i)$. The maximal ideals in $S^{-1}A$ are $S^{-1}\mathfrak{p}_i$. Assume $S^{-1}Q_i$ and $S^{-1}Q_j$ are not relatively prime. Then $S^{-1}Q_i + S^{-1}Q_j \subset S^{-1}\mathfrak{p}_k$ for some k. This implies $Q_i + Q_j \subset \mathfrak{p}_k$, which implies $\mathfrak{p}_i \subset \mathfrak{p}_k$ and $\mathfrak{p}_j \subset \mathfrak{p}_k$, which is a contradiction.

Proposition 45.13. *Let S and T be two multiplicatively closed sets in the ring A. Define $ST = \{st \mid s \in S \text{ and } t \in T\}$. Then*

1. *ST is multiplicatively closed.*
2. *There is exists an isomorphism $\varphi : i(T)^{-1}(S^{-1}A) \to (ST)^{-1}A$, where $i(T)$ is the multiplicative set given by*
$$i(T) = \left\{ \frac{t}{s} \mid t \in T, s \in S \right\}.$$
In particular, if $S \subset T$, then $i(T)^{-1}(S^{-1}A) \cong T^{-1}A$.

Proof.

1. Suppose s_1t_1 and s_2t_2 are two elements in ST. Then
$$(s_1t_1)(s_2t_2) = (s_1s_2)(t_1t_2) \in ST.$$
Also, $1 = 1 \cdot 1 \in ST$. Therefore ST is multiplicatively closed.
2. Let $\varphi : i(T)^{-1}(S^{-1}A) \to (ST)^{-1}A$ be given by mapping $(a/s_1)/(t/s_2)$ to as_2/s_1t. We first need to check that this is well-defined. Suppose $(a'/s_1')/(t'/s_2') \sim (a/s_1)/(t/s_2)$. This means there exists a $t''/s'' \in i(T)$ such that
$$\frac{t''}{s''}\left(\frac{a't}{s_1's_2} - \frac{at'}{s_1s_2'}\right) = 0,$$
which means that there exists an $s \in S$ such that
$$st''(a'ts_1s_2' - at's_1's_2) = 0.$$
But this implies that $as_2/s_1t \sim a's_2'/s_1't'$ since $st'' \in ST$. Therefore φ is well-defined. The map φ is clearly surjective. We will show that φ is also injective. Suppose $as_2/s_1t = 0$. This implies that there exists $st' \in ST$ such that $st'as_2 = 0$. But this implies $(a/s_1)/(t/s_2) = 0$ since $(t'/1) \in i(T)$ with
$$\frac{t'}{1}\frac{a}{s_1} = \frac{at'}{s_1} = 0,$$
since $ss_2 \in S$ with $ss_2(at') = 0$. Finally, that φ is in fact an A-module morphism is easy to verify, and we leave as an exercise for the reader.

□

Lemma 45.3. *Let A be a Noetherian ring and let S be the set of all zerodivisors. Then*
$$S = \bigcup_{\mathfrak{p} \in Ass(\langle 0 \rangle)} \mathfrak{p}.$$

Proof. Let $a \in A$ be a zerodivisor. Then there exists a nonzero $b \in A$ such that $ab = 0$. Let I denote the ideal $0 : b$. Then I has a primary decomposition, since A is Noetherian, as
$$I = Q_1 \cap \cdots \cap Q_k,$$
where $\mathfrak{p}_i = \sqrt{Q_i}$ are the associated prime ideals. Moreover, there exists $b_i \in A$ such that $\mathfrak{p}_i = I : b_i = 0 : bb_i$. Then $\mathfrak{p}_i$ are associated prime ideals of A and $a \in I \subset \mathfrak{p}_i$ implies $a \in \bigcup_{\mathfrak{p} \in \mathrm{Ass}(\langle 0 \rangle)} \mathfrak{p}$. Therefore $S \subset \bigcup_{\mathfrak{p} \in \mathrm{Ass}(\langle 0 \rangle)} \mathfrak{p}$. The reverse inclusion is trivial. □

Proposition 45.14. *Let A be a Noetherian ring and let $\mathfrak{p} \in Ass(\langle 0 \rangle)$. Then*
$$A_{\mathfrak{p}} = Q(A)_{\mathfrak{p}Q(A)}.$$

Proof. Let S be the set of all nonzerodivisors and let $T = A \backslash \mathfrak{p}$. Then $S \subset T$ by Lemma (45.3). Therefore
$$Q(A)_{\mathfrak{p}Q(A)} = i(T)^{-1}(S^{-1}A) \cong T^{-1}A = A_{\mathfrak{p}}$$
by Proposition (45.13). □

Lemma 45.4. *Let A be a ring, $S \subset A$ be a multiplicatively closed subset and M, N be A-modules with $N \subset M$. Then*

$$(M/N)_S \cong M_S/N_S.$$

Proof. Let $\varphi : (M/N)_S \to M_S/N_S$ be the map given by $\varphi(\overline{m}/s) \mapsto \overline{m/s}$. The map is easily seen to be well-defined:

$$\varphi(\overline{m+n}/s) = \overline{(m+n)/s} = \overline{m/s}.$$

It is also clearly surjective. To show that it is injective, suppose $\varphi(\overline{m}/s) = \overline{m/s} = \overline{0}$. Then $m/s = n/s'$ for some $n/t \in N_S$. This implies there exists $s'' \in A \backslash \mathfrak{p}$ such that $s''s'm = s''sn$. But then $\overline{m}/s = 0$, since $\overline{s''s'm} = \overline{s''sn} = 0$, with $s''s' \in A \backslash \mathfrak{p}$. □

Proposition 45.15. *Let A be a ring, $S \subset A$ a multiplicatively closed subset, N, M be A-modules, and $\varphi : M \to N$ be an A-module homomorphism. Then*

1. *$Ker(\varphi_S) = Ker(\varphi)_S$.*
2. *$Im(\varphi_S) = Im(\varphi)_S$.*
3. *$Coker(\varphi_S) = Coker(\varphi)_S$.*

Remark 62. In particular, localization with respect to S is an **exact functor**. That is, if $0 \to M' \to M \to M'' \to 0$ is an exact sequence of A-modules, then $0 \to M'_S \to M_S \to M''_S \to 0$ is an exact sequence of A_S-modules.

Proof.

1. Suppose $m/s \in \mathrm{Ker}(\varphi_S)$. This implies there exists $s' \in A \backslash \mathfrak{m}$ such that $s'\varphi(m) = \varphi(s'm) = 0$. But then $s'm \in \mathrm{Ker}(\varphi)$, and $m/s = s'm/s's \in \mathrm{Ker}(\varphi)_S$. Conversely, suppose $m/s \in \mathrm{Ker}(\varphi)_S$. Then $\varphi_S(m/s) = \varphi(m)/s = 0$, and therefore $m/s \in \mathrm{Ker}(\varphi_S)$.
2. Suppose $\varphi_S(m/s) \in \mathrm{Im}(\varphi_S)$. Then $\varphi_S(m/s) = \varphi(m)/s \in \mathrm{Im}(\varphi)_S$. Conversely, suppose $\varphi(m)/s \in \mathrm{Im}(\varphi)_S$. Then $\varphi(m)/s = \varphi_S(m/s) \in \mathrm{Im}(\varphi_S)$.
3. Finally, using Lemma (45.4), we have

$$\begin{aligned} \mathrm{Coker}(\varphi_S) &= N_S/\mathrm{Im}(\varphi_S) \\ &= N_S/\mathrm{Im}(\varphi)_S \\ &= (N/\mathrm{Im}(\varphi)_S \\ &= \mathrm{Coker}(\varphi)_S. \end{aligned}$$

□

Proposition 45.16. *Let A be a ring and let M be an A-module. The following conditions are equivalent:*

1. *$M = \langle 0 \rangle$.*
2. *$M_{\mathfrak{p}} = \langle 0 \rangle$ for all prime ideals $\mathfrak{p}$.*
3. *$M_{\mathfrak{m}} = \langle 0 \rangle$ for all maximal ideals $\mathfrak{m}$.*

Proof. (1) implies (2) and (2) implies (3) is obvious. To prove (3) implies (1), assume m is a nonzero element in M. Then $\mathrm{Ann}(m)$ is an ideal in A, hence it must be contained in a maximal ideal in A, say $\mathfrak{m}$. However, this would imply that $M_{\mathfrak{m}} \neq 0$ since $m/1$ would be a nonzero element: Everything which kills m, is contained in $\mathfrak{m}$. We have reached a contradiction, and therefore there are no nonzero elements in M, in other words $M = \langle 0 \rangle$. □

Proposition 45.17. *Let A be a ring, M an A-module and N, L submodules of M. Then $N = L$ if and only if $N_{\mathfrak{m}} = L_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ in A.*

Proof. If $N = L$, then we certainly have $N_{\mathfrak{m}} = L_{\mathfrak{m}}$ for all prime ideals $\mathfrak{m}$. Conversely, suppose $N_{\mathfrak{m}} = L_{\mathfrak{m}}$ for all prime ideals $\mathfrak{m}$. To obtain a contradiction, assume there exists an $n \in N$ such that $n \notin L$. Then $L :_A n = \{a \in A \mid an \in L\}$ is a proper ideal in A since $1 \notin L :_A n$. Therefore it is contained in a maximal ideal, say $\mathfrak{m}$. But this implies $N_{\mathfrak{m}} \neq L_{\mathfrak{m}}$, since $n/1 \in N_{\mathfrak{m}}$ but $n/1 \notin L_{\mathfrak{m}}$: If $n/1 = \ell/s$ for some $\ell \in L$, then there exists some $s' \in A \backslash \mathfrak{m}$ such that $s'sn = s'\ell \in L$, but $s's \notin \mathfrak{m} \supset n :_A L$, which is a contradiction. Therefore we must have $N \subset L$. By the same reasoning, we can show $L \subset N$. Therefore $L = N$. □

Corollary 37. *Let A be a ring, N, M be A-modules, and $\varphi : M \to N$ be an A-module homomorphism. Then*

1. *φ is injective if and only if $\varphi_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$.*
2. *φ is surjective if and only if $\varphi_{\mathfrak{m}}$ is injective for all maximal ideals $\mathfrak{m}$.*

Proof.

1. Suppose $\varphi_{\mathfrak{m}}$ is injective for all maximal ideals $\mathfrak{m}$ in A. Then $0 \cong \mathrm{Ker}(\varphi_{\mathfrak{m}}) \cong \mathrm{Ker}(\varphi)_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ in A. Therefore by Proposition (45.16), we must have $\mathrm{Ker}(\varphi) \cong 0$. Conversely, suppose φ is injective. Then $\mathrm{Ker}(\varphi) \cong 0$ implies $0 \cong \mathrm{Ker}(\varphi)_{\mathfrak{m}} \cong \mathrm{Ker}(\varphi_{\mathfrak{m}})$ for all maximal ideals $\mathfrak{m}$ in A.

2. Suppose $\varphi_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$ in A. Then $N_{\mathfrak{m}} = \mathrm{Im}(\varphi_{\mathfrak{m}}) = \mathrm{Im}(\varphi)_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ in A. Therefore $N = \mathrm{Im}(\varphi)$, by Proposition (45.17). Conversely, suppose φ is injective. Then $N = \mathrm{Im}(\varphi)$ implies $N_{\mathfrak{m}} = \mathrm{Im}(\varphi)_{\mathfrak{m}}$, which implies $\varphi_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$ in A.

□

Proposition 45.18. *Let A be a ring, $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be prime ideals in A, and $\langle 0 \rangle \neq M$ a finitely generated A-module such that $M_{\mathfrak{p}_i} \neq \langle 0 \rangle$ for all i. Then there exists $m \in M$ such that $m/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$ for all i.*

Proof. Nakayama's lemma implies that $M_{\mathfrak{p}_i}/\mathfrak{p}_i M_{\mathfrak{p}_i} \neq 0$. Therefore we may choose $m_i/1 \in M_{\mathfrak{p}_i}$ such that if $am_i \in \mathfrak{p}_i M$, then $a \in \mathfrak{p}_i$. In particular, this means $m_i/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$ for all i. We now want to glue these local solutions together. Start with $m_i/1 \in M_{\mathfrak{p}_i}$ and $m_j/1 \in M_{\mathfrak{p}_j}$. If $m_i/1 \notin \mathfrak{p}_j M_{\mathfrak{p}_j}$, then ignore the $m_j/1$ term and keep the $m_i/1$ term. Similarly, if $m_j/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$, then drop $m_i/1$ and keep the $m_j/1$ term. If both $m_i/1 \in \mathfrak{p}_j M_{\mathfrak{p}_j}$ and $m_j/1 \in \mathfrak{p}_i M_{\mathfrak{p}_i}$, then add the terms $m_i/1$ and $m_j/1$ to get $(m_i + m_j)/1$. Now assume, we have constructed an element $m/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$ for $i = 1, 2, \dots k-1$, and assume $m/1 \in \mathfrak{p}_k M_{\mathfrak{p}_k}$. Choose $x_i \in \mathfrak{p}_i$ such that $x_i \notin \mathfrak{p}_k$ for all $i = 1, 2, \dots, k-1$. Then $x_1 x_2 \cdots x_{k-1} m_k/1 \in \mathfrak{p}_i M_{\mathfrak{p}_i}$ for $i = 1, 2, \dots, k-1$ and $x_1 x_2 \cdots x_{k-1} m_k/1 \notin \mathfrak{p}_k M_{\mathfrak{p}_k}$. This implies $m/1 + x_1 x_2 \cdots x_{k-1} m_k/1 = (m + x_1 x_2 \cdots x_{k-1} m_k)/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$ for $i = 1, 2, \dots, k$. □

A key fact about localization is that every linear map $\varphi : M \to N$ of $A_{\mathfrak{p}}$-modules comes from the localization of a linear map of A-modules. That is, we have have a commutative diagram

$$\begin{tikzcd} M \arrow[r, "\varphi"] & N \\ M \otimes_A A_{\mathfrak{p}} \arrow[u] \arrow[r, "\varphi_{\mathfrak{p}}"'] & N \otimes_A A_{\mathfrak{p}} \arrow[u] \end{tikzcd}$$

where the vertical arrows are isomorphisms, given by mapping $m \otimes 1/s$ to m/s and $n \otimes 1/s$ to n/s respectively. Thus, when we talk about a linear map of $A_{\mathfrak{p}}$-modules, we may assume it has the form $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$.

45.7 Localization commutes with Hom and Tensor Products

Lemma 45.5. *Let A be a ring, $\mathfrak{p}$ an ideal in A, and M, N A-modules. Then there exists an injective linear Ψ : $Hom_A(N, M)_{\mathfrak{p}} \to Hom_{A_{\mathfrak{p}}}(N_{\mathfrak{p}}, M_{\mathfrak{p}})$. Moreover, if N is finitely presented, then this map is also surjective, and hence an isomorphism.*

Proof. Define $\Psi_N : \mathrm{Hom}_A(N, M)_{\mathfrak{p}} \to \mathrm{Hom}_{A_{\mathfrak{p}}}(N_{\mathfrak{p}}, M_{\mathfrak{p}})$ by sending the element $\varphi/s \in \mathrm{Hom}_A(N, M)_{\mathfrak{p}}$ to map $\Psi_N(\varphi/s)$ given by:

$$\Psi_N \left(\frac{\varphi}{s} \right) \left(\frac{n}{t} \right) = \frac{\varphi(n)}{st}.$$

We need to be sure this is well-defined. Let φ'/s' be another representation, so that there exists an $s'' \notin \mathfrak{p}$ such that $s''s'\varphi = s''s\varphi'$. Then

$$\begin{aligned} \Psi_N \left(\frac{\varphi'}{s'} \right) \left(\frac{n}{t} \right) &= \frac{\varphi'(n)}{s't} \\ &= \frac{\varphi(n)}{st}, \end{aligned}$$

since $s''st\varphi'(n) = s''s't\varphi(n)$ for all $n/t \in N_{\mathfrak{p}}$. Next, we check that $\Psi_N(\varphi/s)$ is $A_{\mathfrak{p}}$- linear:

$$\begin{aligned} \Psi_N \left(\frac{\varphi}{s} \right) \left(\frac{t'n + tn'}{tt'} \right) &= \frac{\varphi(t'n + tn')}{stt'} \\ &= \frac{t'\varphi(n) + t\varphi(n')}{stt'} \\ &= \frac{\varphi(n)}{st'} + \frac{\varphi(n')}{st'} \\ &= \Psi_N \left(\frac{\varphi}{s} \right) \left(\frac{n}{t} \right) + \Psi_N \left(\frac{\varphi}{s} \right) \left(\frac{n'}{t'} \right), \end{aligned}$$

for all n/t and n'/t' in $N_\mathfrak{p}$, and

$$\begin{aligned}\Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{a}{u}\cdot\frac{n}{t}\right) &= \frac{\varphi(an)}{sut} \\ &= \frac{a}{u}\cdot\frac{\varphi(n)}{st} \\ &= \frac{a}{u}\cdot\Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{n}{t}\right).\end{aligned}$$

for all a/u in $A_\mathfrak{p}$ and n/t in $N_\mathfrak{p}$. So $\Psi_N(\varphi/s) \in \mathrm{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p})$. Next, suppose

$$\Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{n}{t}\right) = 0,$$

for all $n/t \in N_\mathfrak{p}$. Then there exists an $u_n \in A\backslash\mathfrak{p}$ such that $u_n\varphi(n) = 0$ for all $n \in N$. But this implies $\varphi/s = 0$, so Ψ_N is injective.

Now we want to show the second part of the lemma. First assume that N is a free A-module with basis $e_1, \dots, e_k$. Then $N_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module with basis $e_1/1, \dots, e_k/1$. Suppose $\varphi \in \mathrm{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p})$. Then φ is completely determined by where it maps the basis elements, say, $\varphi(e_i/1) = m_i/s_i$ for all $i = 1, \dots, k$. Define $\varphi_i \in \mathrm{Hom}_A(N, M)$ by

$$\varphi_i(e_j) = \begin{cases} s_i & \text{if } i = j, \\ 0 & \text{otherwise.}\end{cases}$$

Then $\varphi_1/s_1 + \cdots + \varphi_k/s_k \in \mathrm{Hom}_A(N, M)_\mathfrak{p}$, and $\Psi_N(\varphi_1/s_1 + \cdots + \varphi_k/s_k) = \varphi$ since they act the same on the basis vectors $e_1/1, \dots, e_k/1$. If, now, N is a finitely presented A-module, then there is an exact sequence

$$A^t \longrightarrow A^s \longrightarrow N \longrightarrow 0$$

Since $\mathrm{Hom}_A(-, M)$ is a left exact contravariant functor, and localization preserves homology, we obtain a commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_A(N,M)_\mathfrak{p} \arrow[r] \arrow[d, dashed, "\Psi_N"] & \mathrm{Hom}_A(A^s,M)_\mathfrak{p} \arrow[r] \arrow[d, "\Psi_{A^s}"] & \mathrm{Hom}_A(A^t,M)_\mathfrak{p} \arrow[d, "\Psi_{A^t}"] \\ 0 \arrow[r] & \mathrm{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p},M_\mathfrak{p}) \arrow[r] & \mathrm{Hom}_{A_\mathfrak{p}}(A^s_\mathfrak{p},M_\mathfrak{p}) \arrow[r] & \mathrm{Hom}_{A_\mathfrak{p}}(A^t_\mathfrak{p},M_\mathfrak{p}) \end{tikzcd}$$

Since Ψ_{A^s} and Ψ_{A^t} are isomorphisms, and easy diagram chase tells us that there must exist a unique isomorphism $\Psi_N : \mathrm{Hom}_A(N, M)_\mathfrak{p} \to \mathrm{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p})$ which makes this diagram commute. □

Lemma 45.6. *Let A be a ring, $\mathfrak{p}$ an ideal in A, and M, N A-modules. Then $N_\mathfrak{p} \otimes_A M_\mathfrak{p} = N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p} = (N \otimes_A M)_\mathfrak{p}$.*

Remark 63. Notice that we are saying $N_\mathfrak{p} \otimes_A M_\mathfrak{p}$ is literally the same set as $N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}$ and $(N \otimes_A M)_\mathfrak{p}$.

Proof. For the first identity, we just need to show that $\frac{n}{s} \otimes m = n \otimes \frac{m}{s}$ for every $m \in M$, $n \in N$ and $s \in A\backslash\mathfrak{p}$. We have

$$\begin{aligned}\frac{n}{s}\otimes m &= \frac{n}{s}\otimes\frac{sm}{s} \\ &= \frac{sn}{s}\otimes\frac{m}{s} \\ &= n\otimes\frac{m}{s}.\end{aligned}$$

For second identity, we show that every element in $N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}$ has the form $\frac{(n_1\otimes m_1+\cdots+n_k\otimes m_k)}{s}$, where $s \in A\backslash\mathfrak{p}$. Start with an arbitrary element $\frac{n_1}{s_1}\otimes m_1 + \cdots + \frac{n_k}{s_k}\otimes m_k$ in $N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}$, where $s_i \in A\backslash\mathfrak{p}$. We have

$$\frac{n_1}{s_1}\otimes m_1 + \cdots + \frac{n_k}{s_k}\otimes m_k = \frac{1}{s_1 s_2\cdots s_k}\left(s_2\cdots s_k n_1\otimes m_1 + \cdots + s_1\cdots s_{k-1}n_k\otimes m_k\right),$$

which proves the claim. □

45.8 Local Rings

Definition 45.5. A ring A is called **local** if it has exactly one maximal ideal $\mathfrak{m}$. If A is local, then we call $A/\mathfrak{m}$ the **residue field** of A. Rings with finitely many maximal ideals are called **semi-local**.

Lemma 45.7. *Let A be a ring.*

1. *A is a local ring if and only if the set of non-units is an ideal (which is then the maximal ideal).*

2. *Let $\mathfrak{m} \subset A$ be a maximal ideal such that every element of the form $1 + a$, where $a \in \mathfrak{m}$, is a unit. Then A is local.*

Proof.

1. Let A be a local ring with maximal ideal $\mathfrak{m}$ and let $x \in A$ be a non-unit. Then $\langle x \rangle \neq 1$, and so $\langle x \rangle$ is contained in a maximal ideal. Since there is only one maximal ideal, we must have $\langle x \rangle \subset \mathfrak{m}$, i.e. $x \in \mathfrak{m}$. Therefore $\mathfrak{m}$ contains the set of all non-units. Since the set of all non-units already contains $\mathfrak{m}$, we see that $\mathfrak{m}$ is the set of all non-units. To prove the converse, let A be a ring and let $\mathfrak{m}$ be the set of all non-units in A. Suppose $\mathfrak{m}$ is an ideal and let $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be two maximal ideals in A. Then $\mathfrak{m} \supset \mathfrak{m}_1$ and $\mathfrak{m} \supset \mathfrak{m}_2$. Since $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are maximal ideals, we must have equality, thus $\mathfrak{m}_1 = \mathfrak{m} = \mathfrak{m}_2$.

2. Let $u \in A \backslash \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $\langle \mathfrak{m}, u \rangle = A$ and, hence, $1 = uv + a$ for some $v \in A$ and $a \in \mathfrak{m}$. By assumption, $uv = 1 - a$ is a unit. Hence, u is a unit and $\mathfrak{m}$ is the set of non-units. The claim follows from (1).

□

45.9 The Covariant Functor $-_S$

Proposition 45.19. *Let S be a multiplicatively closed subset of R. We obtain a functor*

$$-_S \colon \mathbf{Mod}_R \to \mathbf{Mod}_{R_S}$$

from the category of R-modules to the category of R_S-modules, where the R-module M is assigned to the R_S-module M_S and where the R-linear map $\varphi \colon M \to M'$ is assigned to the R_S-linear map $\varphi_S \colon M_S \to M'_S$, where φ_S is defined by

$$\varphi_S\left(\frac{u}{s}\right) = \frac{\varphi(u)}{s}$$

for all $u/s \in M_S$.

Proof. We need to check that $-_S$ preserves compositions and identities. We first check that it preserves compositions. Let $\varphi \colon M \to M'$ and $\varphi' \colon M' \to M''$ be two R-linear maps and let $u/s \in M_S$. Then

$$\begin{aligned}
(\varphi'_S\varphi_S)\left(\frac{u}{s}\right) &= \varphi'_S\left(\varphi_S\left(\frac{u}{s}\right)\right) \\
&= \varphi'_S\left(\frac{\varphi(u)}{s}\right) \\
&= \frac{\varphi'(\varphi(u))}{s} \\
&= \frac{(\varphi'\varphi)(u)}{s} \\
&= (\varphi'\varphi)_S\left(\frac{u}{s}\right).
\end{aligned}$$

It follows that $\varphi'_S\varphi_S = (\varphi'\varphi)_S$. Hence $-_S$ preserves compositions. Next we check that $-_S$ preserves identities. Let M be an R-module and $u/s \in M_S$. Then we have

$$\begin{aligned}
(1_M)_S\left(\frac{u}{s}\right) &= \frac{1_M(u)}{s} \\
&= \frac{u}{s} \\
&= 1_{M_S}\left(\frac{u}{s}\right).
\end{aligned}$$

It follows that $(1_M)_S = 1_{M_S}$. Hence $-_S$ preserves identities. □

45.9.1 Natural Isomorphism from $-_S$ to $- \otimes_R R_S$

Proposition 45.20. *Let S be a multiplicatively closed subset of R. Then there exists a natural isomorphism*

$$\tau\colon\ - \otimes_R R_S \to -_S$$

of functors.

Proof. Let M be an R-module. We first observe that every tensor in $M \otimes_R R_S$ can be expressed as an elementary tensor of the form $u \otimes (1/s)$ where $u \in M$ and $s \in S$. Indeed, let $\sum_{i=1}^k u_i \otimes (a_i/s_i)$ be any tensor. Then we have

$$\begin{aligned} u_1 \otimes \frac{a_1}{s_1} + \cdots + u_k \otimes \frac{a_k}{s_k} &= u_1 \otimes \frac{a_1 s_2 \cdots s_k}{s_1 s_2 \cdots s_k} + \cdots + u_k \otimes \frac{s_1 \cdots s_{k-1} a_k}{s_1 s_2 \cdots s_k} \\ &= (a_1 s_2 \cdots s_k u_1 + \cdots + s_1 \cdots s_{k-1} a_k u_k) \otimes \frac{1}{s_1 s_2 \cdots s_k} \\ &= \widetilde{u} \otimes \frac{1}{\widetilde{s}}, \end{aligned}$$

where

$$\widetilde{u} = a_1 s_2 \cdots s_k u_1 + \cdots + s_1 \cdots s_{k-1} a_k u_k \in M \quad \text{and} \quad s = s_1 s_2 \cdots s_k \in S.$$

Define $\tau_M\colon M \otimes_R R_S \to M_S$ by

$$\tau_M\left(u \otimes \frac{1}{s}\right) = \frac{u}{s}$$

for all $u \otimes (1/s) \in M \otimes_R R_S$. The map τ_M is easily checked to be well-defined, surjective, and an R-linear map (in fact an R_S-linear map). To show it is injective, let $u \otimes (1/s) \in \ker \varphi$. Then since $\varphi(u)/s = 0$, we may choose a $t \in S$ such that $t\varphi(u) = 0$. Then

$$\begin{aligned} u \otimes \frac{1}{s} &= u \otimes \frac{t}{st} \\ &= tu \otimes \frac{1}{st} \\ &= 0 \otimes \frac{1}{st} \\ &= 0. \end{aligned}$$

Thus $\ker \tau_M = 0$, which implies τ_M is injective.

Thus for each R-module M, we obtain an isomorphism $\tau_M\colon M \otimes_R R_S \to M_S$. We claim that τ_- is natural in M, so that it is a natural isomorphism. Indeed, let $\varphi\colon M \to M'$ be an R-linear map. We need to check that the following diagram commutes

$$\begin{tikzcd} M \otimes_R R_S \arrow[r, "\tau_M"] \arrow[d, "\varphi\otimes 1"'] & M_S \arrow[d, "\varphi_S"] \\ M' \otimes_R R_S \arrow[r, "\tau_{M'}"'] & M'_S \end{tikzcd} \tag{150}$$

Let $u \otimes \frac{1}{s} \in M \otimes_R R_S$. Then we have

$$\begin{aligned} (\varphi_S \tau_M)\left(u \otimes \frac{1}{s}\right) &= \varphi_S\left(\tau_M\left(u \otimes \frac{1}{s}\right)\right) \\ &= \varphi_S\left(\frac{u}{s}\right) \\ &= \frac{\varphi(u)}{s} \\ &= \tau_{M'}\left(\varphi(u) \otimes \frac{1}{s}\right) \\ &= \tau_{M'}\left((\varphi \otimes 1)\left(u \otimes \frac{1}{s}\right)\right) \\ &= (\tau_{M'}(\varphi \otimes 1))\left(u \otimes \frac{1}{s}\right). \end{aligned}$$

□

Corollary 38. *Let S be a multiplicatively closed subset of R. Then $-_S$ is exact.*

Proof. The functor $- \otimes_R R_S$ is exact since R_S is a flat R-module. Thus $-_S$ must be exact too since $-_S$ is naturally isomorphic to $- \otimes_R R_S$. □

45.9.2 Localization is Essentially Surjective

Throughout the rest of this section, let S be a multiplicatively closed subset of R.

Proposition 45.21. *Localization is essentially surjective.*

Proof. Let us first show that localization is essentially surjective. Let M be an R_S-module. Then M is also an R-module via the action

$$a \cdot u = \frac{a}{1} \cdot u$$

for all $a \in R$ and $u \in M$. Then $R_S \otimes_R M$ is an R_S-module via the action

$$\frac{a}{s} \cdot \left(\frac{b}{t} \otimes u \right) = \frac{ab}{st} \otimes u$$

for all a/s and b/t in R_S and for all $u \in M$. We claim that M is isomorphic to $R_S \otimes_R M$ as R_S-modules. Indeed, let $\varphi \colon R_S \otimes_R M \to M$ be given by

$$\varphi \left(\frac{1}{s} \otimes u \right) = \frac{1}{s} \cdot u$$

for all $(1/s) \otimes u \in R_S \otimes M$ [5]. This map is well-defined and linear since the corresponding map $R_S \times M \to M$, given by $(a/s, u) \mapsto (a/s) \cdot u$, is bilinear. This map is injective since if $(1/s) \cdot u = 0$, then $u = 0$, which implies $(1/s) \otimes u = 0$. Finally, the map is surjective since if $u \in M$, then $\varphi((1/1) \otimes u) = u$. Therefore localization is essentially surjective since $M_S \cong R_S \otimes_R M$. $\square$

46 Hom

Let M and N be R-modules. We denote by $\mathrm{Hom}_R(M, N)$ to be the set of all R-linear maps from M to N. In fact, $\mathrm{Hom}_R(M, N)$ is more than just a set, it is an abelian group, where addition is defined pointwise: if $\varphi, \psi \in \mathrm{Hom}_R(M, N)$, then we define $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ to be the R-linear map given by

$$(\varphi + \psi)(u) = \varphi(u) + \psi(u)$$

for all $u \in M$. If R is commutative, then $\mathrm{Hom}_R(M, N)$ is more than just an abelian group; it has the structure of an R-module, where scalar multiplication is defined pointwise: if $\varphi \in \mathrm{Hom}_R(M, N)$ and $a \in R$, then we define $a\varphi \in \mathrm{Hom}_R(M, N)$ to be the R-linear map given by

$$(a\varphi)(u) = \varphi(au)$$

for all $u \in M$. Note that if R is not commutative, then $a\varphi$ is R-linear if and only if $a \in Z(R)$. Indeed, given $a, b \in R$, we have

$$\begin{aligned} (a\varphi)(bu) &= \varphi(abu) \\ &= \varphi(bau) \\ &= b\varphi(au) \\ &= b(a\varphi)(u), \end{aligned}$$

where we were allowed to commute a and b since $a \in Z(R)$.

46.1 Properties of Hom

46.1.1 Universal Mapping Property for Products

Proposition 46.1. *Let M be an R-module, let I be an index set, and let N_i be an R-module for each $i \in I$. Then*

1. *$Hom_R\left(\bigoplus_{i\in I} N_i, M\right) \cong \prod_{i\in I} Hom_R\left(N_i, M\right)$.*
2. *$Hom_R\left(M, \prod_{i\in I} N_i\right) \cong \prod_{i\in I} Hom_R\left(M, N_i\right)$*
3. *If, moreover, M is finitely generated, then $Hom_R\left(M, \bigoplus_{i\in I} N_i\right) \cong \bigoplus_{i\in I} Hom_R\left(M, N_i\right)$.*

Remark 64. In other words, the contravariant functor $\mathrm{Hom}_R(-, M)$ takes direct sums to direct products, the covariant functor $\mathrm{Hom}_R(M, -)$ takes direct products to direct products, and if M is finitely-generated, then the covariant functor $\mathrm{Hom}_R(M, -)$ also takes direct sums to direct sums.

[5] Note that every element in $R_S \otimes_R M$ can be put into an elementary tensor form $(1/s) \otimes u$.

Proof. 1. For each $i \in I$, let $\iota_i \colon N_i \to \bigoplus_{i \in I} N_i$ denote the ith inclusion map. Define a map $\Psi \colon \operatorname{Hom}_R\left(\bigoplus_{i\in I} N_i, M\right) \to \prod_{i \in I} \operatorname{Hom}_R\left(N_i, M\right)$ by

$$\Psi(\varphi) = (\varphi|_{N_i}) = (\varphi \circ \iota_i)$$

for all $\varphi \in \operatorname{Hom}_R\left(\bigoplus_{i\in I} N_i, M\right)$. The map Ψ is R-linear as it is a composition of R-linear maps in each component. To see that it is an isomorphism, we construct an inverse map. Define a map $\Phi \colon \prod_{i\in I} \operatorname{Hom}_R\left(N_i, M\right) \to \operatorname{Hom}_R\left(\bigoplus_{i\in I} N_i, M\right)$ by

$$\Phi((\varphi_i))(y_{i_1} + \cdots + y_{i_n}) = \varphi_{i_1}(y_{i_1}) + \cdots + \varphi_{i_n}(y_{i_n})$$

for all $(\varphi_i) \in \prod_{i\in I} \operatorname{Hom}_R\left(N_i, M\right)$ and $y_{i_1} + \cdots + y_{i_n} \in \bigoplus_{i\in I} N_i$.

Let us check that Ψ is indeed the inverse to Φ. Let $\varphi \in \operatorname{Hom}_R\left(\bigoplus_{i\in I} N_i, M\right)$ and let $y_{i_1} + \cdots + y_{i_n} \in \bigoplus_{i\in I} N_i$. Then

$$\begin{aligned}
(\Phi\Psi)(\varphi)(y_{i_1} + \cdots + y_{i_n}) &= \Phi(\varphi|_{N_i})(y_{i_1} + \cdots + y_{i_n}) \\
&= \varphi|_{N_{i_1}}(y_{i_1}) + \cdots + \varphi|_{N_{i_n}}(y_{i_n}) \\
&= \varphi(y_{i_1}) + \cdots + \varphi(y_{i_n}) \\
&= \varphi(y_{i_1} + \cdots + y_{i_n}).
\end{aligned}$$

It follows that $\Phi\Psi = 1$.

Conversely, let $(\varphi_i) \in \prod_{i\in I} \operatorname{Hom}_R\left(N_i, M\right)$. Observe that for each $i \in I$, we have

$$(\Phi(\varphi_i) \circ \iota_i)(y) = \varphi_i(y)$$

for all $y \in N_i$. It follows that $\Phi(\varphi_i) \circ \iota_i = \varphi_i$. Therefore

$$\begin{aligned}
(\Psi\Phi)((\varphi_i)) &= \Psi(\Phi(\varphi_i)) \\
&= (\Phi(\varphi_i) \circ \iota_i) \\
&= (\varphi_i).
\end{aligned}$$

This implies $\Psi\Phi = 1$.

2. Define a map $\Psi \colon \operatorname{Hom}_R\left(M, \prod_{i\in I} N_i\right) \to \prod_{i\in I} \operatorname{Hom}_R\left(M, N_i\right)$ by

$$\Psi(\varphi) = (\pi_i \circ \varphi)_{i \in I}$$

for all $\varphi \in \operatorname{Hom}_R\left(M, \prod_{i\in I} N_i\right)$, where $\pi_i \colon \prod_{i\in I} N_i \to N_i$ is the projection to the ith coordinate. We claim that Ψ is an isomorphism.

We first check that it is R-linear. Let $a, b \in R$ and $\varphi, \psi \in \operatorname{Hom}_R\left(M, \prod_{i\in I} N_i\right)$. Then

$$\begin{aligned}
\Psi(a\varphi + b\psi) &= (\pi_i \circ (a\varphi + b\psi)) \\
&= (a(\pi_i \circ \varphi) + b(\pi_i \circ \psi)) \\
&= a(\pi_i \circ \varphi) + b(\pi_i \circ \psi) \\
&= a\Psi(\varphi) + b\Psi(\psi).
\end{aligned}$$

Thus Ψ is R-linear. To show that Ψ is an isomorphism, we construct its inverse. Let $(\varphi_i) \in \prod_{i\in I} \operatorname{Hom}_R\left(M, N_i\right)$. Define $\Phi((\varphi_i)) \colon M \to \prod_{i\in I} N_i$ by

$$\Phi((\varphi_i))(x) := (\varphi_i(x))$$

for all $x \in M$. Then clearly Φ and Ψ are inverse to each other. Indeed, let $\varphi \in \operatorname{Hom}_R\left(M, \prod_{i\in I} N_i\right)$. Then

$$\begin{aligned}
\Phi(\Psi(\varphi))(x) &= \Phi((\pi_i \circ \varphi))(x) \\
&= ((\pi_i \circ \varphi)(x)) \\
&= \varphi(x)
\end{aligned}$$

for all $x \in M$. Thus $\Phi(\Psi(\varphi)) = \varphi$. Conversely, let $(\varphi_i) \in \prod_{i\in I} \operatorname{Hom}_R\left(M, N_i\right)$. Then

$$\begin{aligned}
\Psi(\Phi(\varphi_i)) &= (\pi_i \circ \Phi(\varphi_i)) \\
&= (\pi_i \circ \varphi)) \\
&= \varphi(x)
\end{aligned}$$

3. Let $\varphi \in \bigoplus_{i \in I} \mathrm{Hom}_R(M, N_i)$ and let

$$\varphi = \sum_{k=1}^{n} \varphi_{i_k}$$

be the unique decomposition of φ, where $\varphi_{i_k} \in \mathrm{Hom}_R(M, N_{i_k})$ for each $1 \leq k \leq n$. We can view φ as an element in $\mathrm{Hom}_R(M, \bigoplus_{i \in I} N_i)$. Indeed, for each $x \in M$, we have

$$\varphi(x) = \sum_{k=1}^{n} \varphi_{i_k}(x) \in \bigoplus_{i \in I} N_i.$$

Thus we have

$$\bigoplus_{i \in I} \mathrm{Hom}_R(M, N_i) \subset \mathrm{Hom}_R\left(M, \bigoplus_{i \in I} N_i\right).$$

For the other direction, suppose that $\{x_1, \dots, x_n\}$ is a generating set for M and let $\varphi \in \mathrm{Hom}_R(M, \bigoplus_{i \in I} N_i)$. For each $1 \leq k \leq n$, let

$$\varphi(x_k) = y_{i_{1,k}} + \cdots + y_{i_{n_k,k}}$$

be the unique decomposition of $\varphi(x_k)$. It follows that

$$\varphi(M) \subset \bigoplus_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n_k}} N_{i_{j,k}}.$$

In particular, we may view φ as an element in

$$\begin{aligned} \mathrm{Hom}_R\left(M, \bigoplus_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n_k}} N_{i_{j,k}}\right) &\cong \bigoplus_{\substack{1 \leq k \leq n \\ 1 \leq j \leq n_k}} \mathrm{Hom}_R(M, N_{i_{j,k}}) \\ &\subset \bigoplus_{i \in I} \mathrm{Hom}_R(M, N_i). \end{aligned}$$

□

46.1.2 Hom Commutes with Localization Under Certain Conditions

Recall that the localization functor $-_S$ is essentially surjective. This means that every R_S-module is isomorphic to an R_S-module of the form M_S where M is an R-module. We now want to show that the localization functor is faithful, but not necessarily full.

Lemma 46.1. *Let S be a multiplicatively closed subset of R and let M and N be R-modules. Then there exists an injective R_S-linear map*

$$\Psi\colon \mathrm{Hom}_R(M, N)_S \to \mathrm{Hom}_{R_S}(M_S, N_S).$$

Moreover, if M is finitely presented, then this map is also surjective, and hence an isomorphism.

Proof. We define $\Psi\colon \mathrm{Hom}_R(M, N)_S \to \mathrm{Hom}_{R_S}(M_S, N_S)$ by

$$\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u}{t}\right) = \frac{\varphi(u)}{st}. \tag{151}$$

for all $\varphi/s \in \mathrm{Hom}_R(M, N)_S$ and $u/t \in M_S$. We need to check that (151) is well-defined. Let φ'/s' and u'/t' be two different representations of φ/s and u/t respectively. Choose $s'', t'' \in S$ such that $s''s'\varphi = s''s\varphi'$ and $t''t'u = t''tu'$. Then

$$\begin{aligned} \Psi_M\left(\frac{\varphi'}{s'}\right)\left(\frac{u'}{t'}\right) &= \frac{\varphi'(u')}{s't'} \\ &= \frac{s''s\varphi'(t''tu')}{s''st''ts't'} \\ &= \frac{s''s'\varphi(t''t'u)}{s''st''ts't'} \\ &= \frac{\varphi(u)}{st}. \end{aligned}$$

Thus (151) is well-defined.

Next, we check that $\Psi_M(\varphi/s)$ is R_S-linear: we have

$$\begin{aligned}
\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{t'u+tu'}{tt'}\right) &= \frac{\varphi(t'u+tu')}{stt'} \\
&= \frac{t'\varphi(u)+t\varphi(u')}{stt'} \\
&= \frac{\varphi(u)}{st'}+\frac{\varphi(u')}{st'} \\
&= \Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u}{t}\right)+\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u'}{t'}\right),
\end{aligned}$$

for all u/t and u'/t' in M_S, and

$$\begin{aligned}
\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{a}{t'}\cdot\frac{u}{t}\right) &= \frac{\varphi(au)}{st't} \\
&= \frac{a}{t'}\cdot\frac{\varphi(u)}{st} \\
&= \frac{a}{t'}\cdot\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u}{t}\right).
\end{aligned}$$

for all a/t' in R_S and u/t in M_S. Thus $\Psi_M(\varphi/s)$ is R_S-linear.

Finally, we check that Ψ is injective. Suppose

$$\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u}{t}\right)=0,$$

for all $u/t \in N_{\mathfrak{p}}$. Then there exists an $s_u \in S$ such that $s_u\varphi(u)=0$ for all $u \in M$. But this implies $\varphi/s=0$, so Ψ_M is injective.

Now we want to show the second part of the lemma. First assume that M is a finite free R-module with basis $e_1,\dots,e_m$. Then M_S is a free R_S-module with basis $e_1/1,\dots,e_m/1$. Suppose $\varphi \in \mathrm{Hom}_{R_S}(M_S,N_S)$. Then φ is completely determined by where it maps the basis elements, say,

$$\varphi\left(\frac{e_i}{1}\right)=\frac{v_i}{t_i}$$

for all $i=1,\dots,m$. For each $1 \le i \le m$, let $\varphi_i\colon M \to N$ be the unique R-linear map such that

$$\varphi_i(e_j)=\begin{cases} v_i & \text{if } i=j, \\ 0 & \text{otherwise.}\end{cases}$$

Then

$$\frac{\varphi_1}{t_1}+\cdots+\frac{\varphi_m}{t_m} \in \mathrm{Hom}_R(M,N)_S \quad \text{and} \quad \Psi_M\left(\frac{\varphi_1}{t_1}+\cdots+\frac{\varphi_m}{t_m}\right)=\varphi$$

since they act the same on the basis vectors $e_1/1,\dots,e_m/1$. Thus, in the case where M is a finite free R-module, the map Ψ_M is surjective.

Now we assume that M is a finitely presented R-module, then there is an exact sequence

$$G \longrightarrow F \longrightarrow M \longrightarrow 0$$

where F and G are finite free R-modules. The since $\mathrm{Hom}_R(-,N)$ is left exact contravariant and $-_S$ is exact covariant, we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_R(M,N)_S \arrow[r] \arrow[d, dashed, "\Psi_M"] & \mathrm{Hom}(F,N)_S \arrow[r] \arrow[d, "\Psi_F"] & \mathrm{Hom}(G,N)_S \arrow[d, "\Psi_G"] \\
0 \arrow[r] & \mathrm{Hom}_{R_S}(M_S,N_S) \arrow[r] & \mathrm{Hom}_{R_S}(F_S,N_S) \arrow[r] & \mathrm{Hom}_{R_S}(G_S,N_S)
\end{tikzcd}$$

where the columns are isomorphisms. An easy diagram chase tells us that

$$\Psi_M\colon \mathrm{Hom}_R(M,N)_S \to \mathrm{Hom}_{R_S}(M_S,N_S)$$

is the unique isomorphism which makes this diagram commute. $\square$

46.2 Functorial Properties of Hom

46.2.1 The Covariant Functor $\mathrm{Hom}_R(M,-)$

Proposition 46.2. *Let M be an R-module. We obtain a covariant functor*

$$\mathrm{Hom}_R(M,-)\colon \mathbf{Mod}_R \to \mathbf{Mod}_R$$

from the category of R-modules to itself, where the R-module N is assigned to the R-module $\mathrm{Hom}_R(M,N)$ and where the R-linear map $\varphi\colon N \to N'$ is assigned to the R-linear map $\varphi_*\colon \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M,N')$, where φ_* is defined by

$$\varphi_*(\psi) = \varphi\psi$$

for all $\psi \in \mathrm{Hom}_R(M,N)$.

Proof. We need to check that $\mathrm{Hom}_R(M,-)$ preserves compositions and identities. We first check that it preserves compositions. Let $\varphi\colon N \to N'$ and $\varphi'\colon M' \to N''$ be two R-linear maps and let $\psi \in \mathrm{Hom}_R(M,N)$. Then we have

$$\begin{aligned}(\varphi'\varphi)_*(\psi) &= \varphi'\varphi\psi \\ &= \varphi'_*(\varphi\psi) \\ &= \varphi'_*(\varphi_*(\psi)) \\ &= (\varphi'_*\varphi_*)(\psi)\end{aligned}$$

It follows that $(\varphi'\varphi)_* = \varphi'_*\varphi_*$. Hence $\mathrm{Hom}_R(M,-)$ preserves compositions. Next we check that $\mathrm{Hom}_R(M,-)$ preserves identities. Let N be an R-module and let $\psi \in \mathrm{Hom}_R(M,N)$. Then we have

$$\begin{aligned}(1_N)_*(\psi) &= 1_N\psi \\ &= \psi \\ &= 1_{\mathrm{Hom}_R(M,N)}(\psi).\end{aligned}$$

It follows that $(1_N)_* = 1_{\mathrm{Hom}_R(M,N)}$. Hence $\mathrm{Hom}_R(M,-)$ preserves identities. □

46.2.2 The Contravariant Functor $\mathrm{Hom}_R(-,N)$

Proposition 46.3. *Let N be an R-module. We obtain a contravariant functor*

$$\mathrm{Hom}_R(-,N)\colon \mathbf{Mod}_R \to \mathbf{Mod}_R$$

from the category of R-modules to itself, where the R-module M is assigned to the R-module $\mathrm{Hom}_R(M,N)$ and where the R-linear map $\varphi\colon M \to M'$ is assigned to the R-linear map $\varphi^*\colon \mathrm{Hom}_R(M',N) \to \mathrm{Hom}_R(M,N)$, where φ^* is defined by

$$\varphi^*(\psi') = \psi'\varphi$$

for all $\psi' \in \mathrm{Hom}_R(M',N)$.

Proof. We need to check that $\mathrm{Hom}_R(-,N)$ preserves compositions and identities. We first check that it preserves compositions. Let $\varphi\colon M \to M'$ and $\varphi'\colon M' \to M''$ be two R-linear maps and let $\psi'' \in \mathrm{Hom}_R(M'',N)$. Then we have

$$\begin{aligned}(\varphi'\varphi)^*(\psi'') &= \psi''\varphi'\varphi \\ &= (\varphi'^*(\psi''))\varphi \\ &= \varphi^*(\varphi'^*(\psi'')) \\ &= (\varphi^*\varphi'^*)(\psi'')\end{aligned}$$

It follows that $(\varphi'\varphi)^* = (\varphi^*\varphi'^*)$. Hence $\mathrm{Hom}_R(-,N)$ preserves compositions. Next we check that $\mathrm{Hom}_R(-,N)$ preserves identities. Let M be an R-module and let $\psi \in \mathrm{Hom}_R(M,N)$. Then we have

$$\begin{aligned}(1_M)^*(\psi) &= \psi 1_M \\ &= \psi \\ &= 1_{\mathrm{Hom}_R(M,N)}(\psi).\end{aligned}$$

It follows that $(1_M)^* = 1_{\mathrm{Hom}_R(M,N)}$. Hence $\mathrm{Hom}_R(-,N)$ preserves identities. □

46.2.3 Left Exactness of $\mathrm{Hom}_R(-,N)$

Proposition 46.4. *The sequence of R-modules*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0 \tag{152}$$

is exact if and only if for all R-modules N the induced sequence

$$0 \longrightarrow \mathrm{Hom}_R(M_3,N) \xrightarrow{\varphi_2^*} \mathrm{Hom}_R(M_2,N) \xrightarrow{\varphi_1^*} \mathrm{Hom}_R(M_1,N) \tag{153}$$

is exact.

Proof. Suppose that (320) is exact and let N be any R-module. We first show exactness at $\mathrm{Hom}_R(M_3,N)$. Let $\psi_3 \in \ker\varphi_2^*$. Then

$$\begin{aligned} 0 &= \varphi_2^*(\psi_3) \\ &= \psi_3\varphi_2 \\ &= \psi_3, \end{aligned}$$

where we used the fact that φ_2 is surjective to obtain the third line from the second line. Therefore φ_2^* is injective, which implies exactness at $\mathrm{Hom}_R(M_3,N)$.

Next we show exactness at $\mathrm{Hom}_R(M_2,N)$. Let $\psi_2 \in \ker\varphi_1^*$. Then

$$\begin{aligned} 0 &= \varphi_1^*(\psi_2) \\ &= \psi_2\varphi_1 \end{aligned}$$

implies ψ_2 kills the image of φ_1. We define $\psi_3\colon M_3 \to N$ as follows: let $u_3 \in M_3$. Choose $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ (such a choice is possible since φ_2 is surjective). We define

$$\psi_3(u_3) = \psi_2(u_2).$$

The map ψ_3 is well-defined since ψ_2 kills the image of φ_1. Indeed, if $v_2 \in M_2$ was another lift of u_3 under φ_2, then

$$\begin{aligned} v_2 - u_2 &\in \ker\varphi_2 \\ &= \mathrm{im}\,\varphi_1. \end{aligned}$$

Thus

$$\begin{aligned} \psi_2(v_2) &= \psi_2(v_2 - u_2 + u_2) \\ &= \psi_2(v_2-u_2) + \psi_2(u_2) \\ &= \psi_2(u_2). \end{aligned}$$

Thus the map ψ_3 is well-defined. The map ψ_3 is also R-linear. Indeed, let $a,b \in R$ and let $u_3, v_3 \in M_3$. Choose lifts of u_3, v_3 under φ_2, say $u_2, v_2 \in M_2$ (so $\varphi_2(u_2) = u_3$ and $\varphi(v_2) = v_3$). Then $au_2 + bv_2$ is easily seen to be a lift of $au_3 + bv_3$ under φ and so we have

$$\begin{aligned} \psi_3(au_3 + bv_3) &= \psi_2(au_2 + bv_2) \\ &= a\psi_2(u_2) + b\psi_2(v_2) \\ &= a\psi_3(u_3) + b\psi_3(v_3). \end{aligned}$$

Thus ψ_3 is R-linear. Finally, observe that

$$\begin{aligned} \varphi_2^*(\psi_3)(u_2) &= (\psi_3\varphi_2)(u_2) \\ &= \psi_3(\varphi_2(u_2)) \\ &= \psi_3(u_3) \\ &= \psi_2(u_2) \end{aligned}$$

for all $u_2 \in M_2$. It follows that $\psi_2 = \varphi_2^*(\psi_3)$, and hence $\psi_2 \in \mathrm{im}\,\varphi_2^*$. Therefore we have exactness at $\mathrm{Hom}_R(M_2,N)$.

Conversely, suppose that (320) is exact for all R-modules N. We first show φ_2 is surjective. Set $N = M_3/\operatorname{im}\varphi_2$ and let $\pi\colon M_3 \to M_3/\operatorname{im}\varphi_2$ be the quotient map. Observe that

$$\begin{aligned}\varphi_2^*(\pi) &= \pi\varphi_2 \\ &= 0 \\ &= \varphi_2^*(0).\end{aligned}$$

It follows from injectivity of φ_2^* that $\pi = 0$. In other words, $M_3 = \operatorname{im}\varphi_2$, hence φ_2 is surjective.

Next we show exactness at M_2. First set $N = M_3$. Then exactness of (320) implies

$$\begin{aligned}0 &= (\varphi_1^*\varphi_2^*)(1_{M_3}) \\ &= (\varphi_1^*(\varphi_2^*(1_{M_3})) \\ &= \varphi_1^*(1_{M_3}\varphi_2) \\ &= 1_{M_3}\varphi_2\varphi_1 \\ &= \varphi_2\varphi_1.\end{aligned}$$

Thus $\ker\varphi_2 \supseteq \operatorname{im}\varphi_1$. For the reverse inclusion, set $N = M_2/\operatorname{im}\varphi_1$ and let $\pi\colon M_2 \to M_2/\operatorname{im}\varphi_1$ be the quotient map. Then

$$\begin{aligned}\varphi_1^*(\pi) &= \pi\varphi_1 \\ &= 0\end{aligned}$$

implies there exists $\psi_3\colon M_3 \to M_2/\operatorname{im}\varphi_1$ such that $\pi = \varphi_2^*(\psi_3)$ by exactness of (320). Thus, if $u_2 \in \ker\varphi_2$, then

$$\begin{aligned}0 &= \psi_3(0) \\ &= \psi_3(\varphi_2(u_2)) \\ &= (\psi_3\varphi_2)(u_2) \\ &= (\varphi_2^*(\psi_3))(u_2) \\ &= \pi(u_2)\end{aligned}$$

implies $u_2 \in \operatorname{im}\varphi_1$. Thus $\ker\varphi_2 \subseteq \operatorname{im}\varphi_1$. □

46.2.4 Naturality

Proposition 46.5. *Let $\varphi\colon M \to M'$ be an R-linear map. Then we obtain an induced natural transformation*

$$\operatorname{Hom}_R(\varphi, -)\colon \operatorname{Hom}_R(M, -) \to \operatorname{Hom}_R(M', -)$$

between functors.

Proof. Let $\psi\colon N \to N'$ be an R-linear map. We need to check that the following diagram commutes

$$\begin{tikzcd} \operatorname{Hom}_R(M,N) \arrow[r, "\varphi^*"] \arrow[d, "\psi_*"'] & \operatorname{Hom}_R(M',N) \arrow[d, "\psi_*"] \\ \operatorname{Hom}_R(M,N') \arrow[r, "\varphi^*"'] & \operatorname{Hom}_R(M',N') \end{tikzcd} \tag{154}$$

Let $\phi \in \operatorname{Hom}_R(M,N)$. Then we have

$$\begin{aligned}(\psi_*\varphi^*)(\phi) &= \psi_*(\varphi^*(\phi)) \\ &= \psi_*(\phi\varphi) \\ &= \psi\phi\varphi \\ &= \varphi^*(\psi\phi) \\ &= \varphi^*(\psi_*(\phi)) \\ &= (\varphi^*\psi_*)(\phi).\end{aligned}$$

It follows that $\psi_*\varphi^* = \varphi^*\psi_*$, and so the diagram (154) commutes. □

Remark 65. By a similar argument, every R-linear map $\psi\colon N \to N'$ induces a natural transformation

$$\operatorname{Hom}_R(-,\psi)\colon \operatorname{Hom}_R(-,N) \to \operatorname{Hom}_R(-,N').$$

47 Limits and Colimits

47.1 Inverse Systems and Inverse Limits

Let $(\Lambda, \leq)$ be a preordered set. An **inverse system** of R-modules and R-linear maps over Λ is a pair $(M_\lambda, \varphi_{\lambda\mu})$ consisting of a family of R-modules $\{M_\lambda\}$ indexed by Λ and a family of R-linear maps $\{\varphi_{\lambda\mu} \colon M_\mu \to M_\lambda\}_{\lambda \leq \mu}$ such that for all $\kappa \leq \lambda \leq \mu$, we have

$$\varphi_{\lambda\lambda} = 1_{M_\lambda} \quad \text{and} \quad \varphi_{\kappa\mu} = \varphi_{\kappa\lambda}\varphi_{\lambda\mu}.$$

We say the pair (M, ψ_λ) consisting of an R-module M and a family of R-linear maps $\psi_\lambda \colon M \to M_\lambda$ is **compatible** with the inverse system $(M_\lambda, \varphi_{\lambda\mu})$ if

$$\varphi_{\lambda\mu}\psi_\mu = \psi_\lambda.$$

for all $\lambda \leq \mu$. A pair (M, ψ_λ) is called the **inverse limit** (or simply just limit) of the inverse system $(M_\lambda, \varphi_{\lambda\mu})$ if it is final with respect to the property of being compatible with the inverse system: if $(\widetilde{M}, \widetilde{\psi}_\lambda)$ is another pair compatible with the inverse system $(M_\lambda, \varphi_{\lambda\mu})$, then there exists a unique R-linear map $\phi \colon \widetilde{M} \to M$ such that

$$\psi_\lambda \phi = \widetilde{\psi}_\lambda$$

for all λ. The universality part of this definition implies that if an inverse limit exists, then it is unique up to unique isomorphism (hence why we are justified in calling it *the* inverse limit and not *an* inverse limit). With this in mind, if the inverse limit exists then we usually denote it by $(\varprojlim M_\lambda, \pi_\lambda)$. We often abuse notation slightly by just denoting the inverse limit via the underlying module $\varprojlim M_\lambda$ where it is understood that the inverse limit comes equipped with canonical "projection" maps $\pi_\lambda \colon \varprojlim M_\lambda \to M_\lambda$ for all $\lambda \in \Lambda$. Let us now show that the inverse limit in fact always exists.

Proposition 47.1. *Let $(M_\lambda, \varphi_{\lambda\mu})$ be an inverse system of R-modules and R-linear maps over a preordered set $(\Lambda, \leq)$. Then inverse limit of this system has the following description: it is given by*

$$\varprojlim M_\lambda = \left\{ (u_\lambda) \in \prod_{\lambda \in \Lambda} M_\lambda \mid \varphi_{\lambda\mu}(u_\mu) = u_\lambda \text{ for all } \lambda \leq \mu \right\},$$

together with the projection maps $\pi_\lambda \colon M \to M_\lambda$ obtained by restricting the canonical projection maps $\prod_\lambda M_\lambda \to M_\lambda$ to M.

Proof. We need to show that the pair $(\varprojlim M_\lambda, \pi_\lambda)$ is universally compatible with the inverse system $(M_\lambda, \varphi_{\lambda\mu})$. Let (M, ψ_λ) be compatible with respect to the invserse system $(M_\lambda, \varphi_{\lambda\mu})$, so $\varphi_{\lambda\mu}\psi_\mu = \psi_\lambda$ for all $\lambda \leq \mu$. By the universal mapping property of the product, there exists a unique R-linear map $\psi \colon M \to \prod_\lambda M_\lambda$ such that $\pi_\lambda \psi = \psi_\lambda$ for all $\lambda \in \Lambda$. In fact, this map lands in $\varprojlim M_\lambda$ since

$$\begin{aligned} \varphi_{\lambda\mu}\pi_\mu\psi(u) &= \varphi_{\lambda\mu}\psi_\mu(u) \\ &= \psi_\lambda(u) \\ &= \pi_\lambda\psi(u) \end{aligned}$$

for all $u \in M$. This establishes existence and uniqueness, and thus $\varprojlim M_\lambda$ satisfies the universal mapping property. $\square$

47.1.1 Pullbacks

Consider the inverse system depicted below:

$$\begin{tikzcd} & M_2 \arrow[d, "\varphi_{12}"] \\ M_3 \arrow[r, "\varphi_{13}"'] & M_1 \end{tikzcd}$$

The inverse limit of this inverse system is called the **pullback** with respect to φ_{13} and φ_{12} and is often denoted $M_3 \times_{M_1} M_2$. To simplify notation in what follows, we will write $M_{32} = M_3 \times_{M_1} M_2$. As in the general case, this module has the following description:

$$M_{32} = \{(u_3, u_2) \in M_3 \times M_2 \mid \varphi_{13}u_3 = \varphi_{12}u_2\}.$$

The canonical projection maps $\pi_1 \colon M_{32} \to M_3$ and $\pi_2 \colon M_{32} \to M_2$ are the usual ones. Let us show that pullbacks preserve surjective/injective maps and also reflect injective maps in the following sense:

Proposition 47.2. *Let $\varphi_{13} \colon M_3 \to M_1$ and $\varphi_{12} \colon M_2 \to M_1$ be R-linear maps and set $M_{32} = M_3 \times_{M_1} M_2$ to be their pullback. We have the following commutative diagram*

$$\begin{tikzcd}
0 \arrow[r] & \ker \pi_2 \arrow[r] \arrow[d, "\widetilde{\pi}_1"] & M_{32} \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & M_2 \arrow[r] \arrow[d, "\varphi_{12}"] & \operatorname{coker} \pi_2 \arrow[r] \arrow[d, "\overline{\varphi}_{12}"] & 0 \\
0 \arrow[r] & \ker \varphi_{13} \arrow[r] & M_3 \arrow[r, "\varphi_{13}"'] & M_1 \arrow[r] & \operatorname{coker} \varphi_{13} \arrow[r] & 0
\end{tikzcd}$$

where $\widetilde{\pi}_1$ is the restriction of π_1 to $\ker \pi_2$ and where $\overline{\varphi}_{12}$ is the map induced by φ_{12}. The map $\widetilde{\pi}_1$ is an isomorphism and the map $\overline{\varphi}_{12}$ is injective. In particular, φ_{12} is injective if and only if π_1 is injective. Similarly, φ_{12} is surjective if and only if π_1 is surjective and $\overline{\varphi}_{12}$ is an isomorphism.

Proof. To see that $\widetilde{\pi}_1$ is surjective, note that if $u_3 \in \ker \varphi_{13}$, then $(u_3, 0) \in \ker \pi_2$ and $\pi_1(u_3, 0) = u_3$. To see that $\widetilde{\pi}_1$ is injective, note that $(u_3, u_2) \in \ker \pi_2$ implies $u_2 = 0$ and $(u_3, 0) \in \ker \widetilde{\pi}_1$ implies $u_3 = 0$. By a symmetrical argument, one can show that we have the following commutative diagram

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & & \\
 & 0 \arrow[r] \arrow[d] & \ker \pi_1 \arrow[r, "\widetilde{\pi}_2"] \arrow[d] & \ker \varphi_{12} \arrow[r] \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker \pi_2 \arrow[r] \arrow[d, "\widetilde{\pi}_1"] & M_{32} \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & M_2 \arrow[r] \arrow[d, "\varphi_{12}"] & \operatorname{coker} \pi_2 \arrow[r] \arrow[d, "\overline{\varphi}_{12}"] & 0 \\
0 \arrow[r] & \ker \varphi_{13} \arrow[r] \arrow[d] & M_3 \arrow[r, "\varphi_{13}"'] \arrow[d] & M_1 \arrow[r] \arrow[d] & \operatorname{coker} \varphi_{13} \arrow[r] & 0 \\
 & 0 \arrow[r] & \operatorname{coker} \pi_1 \arrow[r, "\overline{\varphi}_{13}"] \arrow[d] & \operatorname{coker} \varphi_{12} \arrow[d] & & \\
 & & 0 & 0 & &
\end{tikzcd}$$

which is exact everywhere. □

Let us now apply the proposition above to prove Schanuel's Lemma:

Lemma 47.1. *(Schanuel's Lemma) Let*

$$0 \longrightarrow K \xrightarrow{\iota} P \xrightarrow{\varphi} M \longrightarrow 0$$

and

$$0 \longrightarrow K' \xrightarrow{\iota'} P' \xrightarrow{\varphi'} M \longrightarrow 0$$

be two short exact sequences of R-modules where P and P' are projective R-modules. Then there is an isomorphism

$$P' \oplus K \cong P \oplus K.$$

Proof. Let $P \times_M P'$ be the pullback of $\varphi \colon P \to M$ and $\varphi' \colon P' \to M$. This comes equipped with maps $\pi_1 \colon P \times_M P' \to P$ and $\pi_2 \colon P \times_M P' \to P'$ which are both necessarily surjective since both φ and φ' are surjective. Since P and P' are projective and since $\ker \pi_1 \cong K'$ and $\ker \pi_2 \cong K$ by the proposition above, we have

$$\begin{aligned}
P' \oplus K &\cong P' \oplus \ker \pi_2 \\
&\cong P \times_M P' \\
&\cong P \oplus \ker \pi_1 \\
&\cong P \oplus K'.
\end{aligned}$$

□

We have

$$a_{00} + a_{10}x + a_{01}y +$$

47.2 Direct/Directed Systems and Direct Limits

Let $(\Lambda, \leq)$ be a preordered set. A **direct system** $(M_\lambda, \varphi_{\lambda\mu})$ of R-modules and R-linear maps over Λ consists of a family of R-modules $\{M_\lambda\}$ indexed by Λ and a family of R-linear maps $\{\varphi_{\lambda\mu} \colon M_\lambda \to M_\mu\}_{\lambda \leq \mu}$ such that for all $\kappa \leq \lambda \leq \mu$, we have

$$\varphi_{\lambda\lambda} = 1_{M_\lambda} \quad \text{and} \quad \varphi_{\kappa\mu} = \varphi_{\lambda\mu}\varphi_{\kappa\lambda}.$$

If Λ is a directed set, then we say $(M_\lambda, \varphi_{\lambda\mu})$ is a **directed system**. If M is an R-module and $\{\psi_\lambda \colon M_\lambda \to M\}$ is a collection of R-linear maps, then we say the pair (M, ψ_λ) is **compatible** with the direct system $(M_\lambda, \varphi_{\lambda\mu})$ if

$$\psi_\mu \varphi_{\lambda\mu} = \psi_\lambda.$$

for all $\lambda \leq \mu$. We say (M, ψ_λ) is the **direct limit** (or colimit) of the direct system $(M_\lambda, \varphi_{\lambda\mu})$ if it is universally compatible in the following sense: if $(\widetilde{M}, \widetilde{\psi}_\lambda)$ is compatible with the direct system $(M_\lambda, \varphi_{\lambda\mu})$, then there exists a unique R-linear map $\phi \colon M \to \widetilde{M}$ such that

$$\phi\psi_\lambda = \widetilde{\psi}_\lambda$$

for all λ.

Assuming the direct limit exists, then it is a standard exercise to show that the direct limit is unique up to unique isomorphism, hence why we refer to it as *the* direct limit and not *a* direct limit. With this in mind, we denote the direct limit by $\varinjlim M_\lambda$. Let us now show that the direct limit does in fact exist.

Proposition 47.3. *Let $(M_\lambda, \varphi_{\lambda\mu})$ be a direct system of R-modules and R-linear maps over a preordered set $(\Lambda, \leq)$. Then direct limit of this system exists and is given by*

$$\varinjlim M_\lambda := \bigoplus_{\lambda \in \Lambda} M_\lambda / \langle \{ (\iota_\lambda - \iota_\mu \varphi_{\lambda\mu})(u_\lambda) \mid u_\lambda \in M_\lambda \text{ and } \lambda \leq \mu \} \rangle$$

together with the inclusion maps

$$\bar{\iota}_\lambda \colon M_\lambda \to \varinjlim M_\lambda$$

for all $\lambda \in \Lambda$, where $\bar{\iota}_\lambda$ is the composite of the inclusion map $\iota_\lambda \colon M_\lambda \to \bigoplus_{\lambda \in \Lambda} M_\lambda$ together with the quotient map $\bigoplus_{\lambda \in \Lambda} M_\lambda \to \varinjlim M_\lambda$

Proof. We need to show that $\varinjlim M_\lambda$ (as described in the proposition above) is universally compatible. Let (M, ψ_λ) be compatible with respect to the direct system $(M_\lambda, \varphi_{\lambda\mu})$. By the universal mapping property of the coproduct, there exists a unique R-linear map $\psi \colon \bigoplus_\lambda M_\lambda \to M$ such that $\psi\iota_\lambda = \psi_\lambda$ for all λ. In fact, since

$$\begin{aligned}
\psi(\iota_\lambda - \iota_\mu \varphi_{\lambda\mu})(u_\lambda) &= \psi\iota_\lambda(u_\lambda) - \psi\iota_\mu\varphi_{\lambda\mu}(u_\lambda) \\
&= \psi_\lambda(u_\lambda) - \psi_\mu\varphi_{\lambda\mu}(u_\lambda) \\
&= \psi_\lambda(u_\lambda) - \psi_\lambda(u_\lambda) \\
&= 0
\end{aligned}$$

for all $u_\lambda \in M_\lambda$ and $\lambda \in \Lambda$, the universal mapping property of quotients implies there exists a unique R-linear map $\overline{\psi} \colon \varinjlim M_\lambda \to M$ such that

$$\overline{\psi}\bar{\iota}_\lambda = \psi\iota_\lambda = \psi_\lambda.$$

This shows that $\varinjlim M_\lambda$ satisfies the universal mapping property. □

It turns out that direct limits are much easier to describe when they are direct limits over *directed* systems. The next proposition gives us an idea of why this is true.

Proposition 47.4. *Let $(M_\lambda, \varphi_{\lambda\mu})$ be a directed system of R-modules and R-linear maps over a directed set $(\Lambda, \leq)$ and set $M = \varinjlim M_\lambda$.*

1. *Each element of M has the form $\overline{u}_\lambda$ for some $\lambda \in \Lambda$ and $u_\lambda \in M_\lambda$.*
2. *We have $\overline{u}_\lambda = 0$ if and only if $\varphi_{\lambda\mu}(u_\lambda) = 0$ for some $\lambda \leq \mu$.*

Proof. 1. An element in M has the form $\sum_{i=1}^n \overline{u}_{\lambda_i}$ where $\lambda_1, \dots, \lambda_n \in \Lambda$ and $u_{\lambda_i} \in M_{\lambda_i}$ for all $1 \leq i \leq n$. Since Λ

is directed, there exists a $\lambda \in \Lambda$ such that $\lambda_i \leq \lambda$ for all $1 \leq i \leq n$. Then we have

$$\begin{aligned}\sum_{i=1}^{n} \overline{u}_{\lambda_i} &= \sum_{i=1}^{n} \overline{\varphi_{\lambda_i,\lambda}(u_{\lambda_i})} \\ &= \overline{\sum_{i=1}^{n} \varphi_{\lambda_i,\lambda}(u_{\lambda_i})} \\ &= \overline{u}_\lambda,\end{aligned}$$

[6]where $\overline{u}_\lambda = \sum_{i=1}^{n} \varphi_{\lambda_i,\lambda}(u_{\lambda_i})$. Each $\varphi_{\lambda_i,\lambda}(u_{\lambda_i})$ lands in M_λ, so $u_\lambda \in M_\lambda$.

2. If $\varphi_{\lambda\mu}(u_\lambda) = 0$ for some $\lambda \leq \mu$, then $\overline{u}_\lambda = \overline{\varphi_{\lambda\mu}(u_\lambda)} = 0$. Conversely, suppose $\overline{u}_\lambda = 0$. Then we have

$$\iota_\lambda(u_\lambda) = \sum_{i=1}^{n} \iota_{\lambda_i}(u_{\lambda_i}) - \sum_{i=1}^{n} \iota_{\mu_i}\varphi_{\lambda_i,\mu_i}(u_{\lambda_i}) \tag{155}$$

for some $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in \Lambda$ and $u_{\lambda_i} \in M_{\lambda_i}$ for all $1 \leq i \leq n$, where we may assume that $\lambda_i \neq \mu_i$ since otherwise we have $\iota_{\lambda_i} - \iota_{\mu_i}\varphi_{\lambda_i,\mu_i} = 0$. Since $u_\lambda \in M_\lambda$, we may assume that $u_{\lambda_i} \in M_\lambda$ for each $1 \leq i \leq n$. In particular, this implies

$$u_\lambda = \sum_{i=1}^{n} u_{\lambda_i} \quad \text{and} \quad \sum_{i=1}^{n} \varphi_{\lambda,\mu_i}(u_{\lambda_i}) = 0.$$

Now if $\mu_i = \mu = \mu_j$ for each $1 \leq i, j \leq n$, then clearly we have

$$\begin{aligned}\varphi_{\lambda,\mu}(u_\lambda) &= \varphi_{\lambda,\mu}\left(\sum_{i=1}^{n} u_{\lambda_i}\right) \\ &= \sum_{i=1}^{n} \varphi_{\lambda,\mu}(u_{\lambda_i}) \\ &= 0.\end{aligned}$$

Otherwise, choose $\mu \in \Lambda$ such that $\mu_i \leq \mu$ for all $1 \leq i \leq n$. Then it's easy to see that we still have $\varphi_{\lambda,\mu}(u_\lambda) = 0$. □

47.2.1 Taking Directed Limits is an Exact Functor

Definition 47.1. Suppose $(M_\lambda, \varphi_{\lambda\mu})$ and $(M'_\lambda, \varphi'_{\lambda\mu})$ are two direct systems over a partially ordered set $(\Lambda, \leq)$. A **morphism** $\psi\colon (M_\lambda, \varphi_{\lambda\mu}) \to (M'_\lambda, \varphi'_{\lambda\mu})$ of direct systems consists of a collection of graded R-linear maps $\psi_\lambda\colon M_\lambda \to M'_\lambda$ indexed by Λ such that for all $\lambda \leq \mu$ we have

$$\varphi'_{\lambda\mu}\psi_\lambda = \psi_\mu\varphi_{\lambda\mu}.$$

The morphism ψ induces a graded R-linear map $\varinjlim \psi_\lambda\colon \varinjlim M_\lambda \to \varinjlim M'_\lambda$ uniquely determined by

$$\varinjlim \psi_\lambda(\overline{u}_\lambda) = \overline{\psi_\lambda(u_\lambda)}$$

for all $u_\lambda \in M_\lambda$ for all $\lambda \in \Lambda$.

Proposition 47.5. *Let*

$$0 \longrightarrow (M_\lambda, \varphi_\lambda) \xrightarrow{\psi} (M'_\lambda, \varphi'_\lambda) \xrightarrow{\psi'} (M''_\lambda, \varphi''_\lambda) \longrightarrow 0$$

be a short exact sequence of directed systems of graded R-modules and graded R-linear maps. Then

$$0 \longrightarrow \varinjlim M_\lambda \xrightarrow{\varinjlim \psi_\lambda} \varinjlim M'_\lambda \xrightarrow{\varinjlim \psi'_\lambda} \varinjlim M_\lambda \longrightarrow 0$$

is a short exact sequence of graded R-modules and graded R-linear maps.

6

Proof. We first show $\varinjlim \psi_\lambda$ is injective. Let $\overline{u}_\lambda \in \varinjlim M_\lambda$ and suppose $\overline{\psi_\lambda u_\lambda} = 0$. Then there exists $\mu \geq \lambda$ such that

$$\begin{aligned} 0 &= \varphi'_{\lambda\mu}\psi_\lambda u_\lambda \\ &= \psi_\mu \varphi_{\lambda\mu} u_\lambda. \end{aligned}$$

Since ψ_λ is injective, we have $\varphi_{\lambda\mu}u_\lambda = 0$, which implies $\overline{u}_\lambda = 0$. So $\varinjlim \psi_\lambda$ is injective.

Next we show exactness at $\varinjlim M'_\lambda$. Let $\overline{u'}_\lambda \in \varinjlim M'_\lambda$ and suppose $\overline{\psi'_\lambda u'_\lambda} = 0$. Then there exists $\mu \geq \lambda$ such that

$$\begin{aligned} 0 &= \varphi''_{\lambda\mu}\psi'_\lambda u'_\lambda \\ &= \psi'_\mu \varphi'_{\lambda\mu} u'_\lambda. \end{aligned}$$

This implies $\varphi'_{\lambda\mu}u'_\lambda = \psi_\mu u_\mu$ for some $u_\mu \in M_\mu$, by exactness at $(M'_\lambda, \varphi'_\lambda)$. Thus

$$\begin{aligned} \overline{u'_\lambda} &= \overline{\varphi'_{\lambda\mu}u'_\lambda} \\ &= \overline{\psi_\mu u_\mu}. \end{aligned}$$

This implies exactness at $\varinjlim M'_\lambda$. Exactness at $\varinjlim M''_\lambda$ is easy and is left as an exercise. □

48 Nakayama's Lemma and its Consequences

Nakayama's Lemma is a powerful tool we use in Commutative Algebra. In order to know Commutative Algebra, one must be familiar with Nakayama's Lemma. Before we state and prove Nakayama's Lemma, we need to discuss the Jacobson radical of a ring.

Definition 48.1. The **Jacobson radical** of R, denoted $\mathrm{rad}(R)$, is defined by the formula

$$\mathrm{rad}(R) := \bigcap_{\substack{\mathfrak{m}\subset R \\ \mathfrak{m}\text{ maximal}}} \mathfrak{m}.$$

Example 48.1. Suppose $(R, \mathfrak{m})$ is a local ring. Then $\mathrm{rad}(R) = \mathfrak{m}$.

Proposition 48.1. *Let $x \in \mathrm{rad}(R)$. Then $1 - x \in R^\times$.*

Proof. Suppose that $1 - x \notin R^\times$. Then there exists a maximal ideal which contains $1 - x$, choose $\mathfrak{m}$ to be this maximal ideal. But then this implies $x \notin \mathfrak{m}$, contradicting the fact that $x \in \mathrm{rad}(R)$. □

48.1 Nakayama's Lemma

We now state and prove Nakayama's Lemma:

Lemma 48.1. *(Nakayama). Let R be a ring, let I be an ideal contained in $\mathrm{rad}(R)$, let M a finitely generated R-module, and let $N \subset M$ a submodule such that $M = IM + N$. Then $M = N$. In particular, if $M = IM$, then $M = 0$.*

Proof. Assume $M \neq N$, and let $u_1, \dots, u_s \in M$ such that their classes form a system of generators of M/N and where s is minimal. Since $u_s \in M = IM + N$, there exists $x_1, \dots, x_s \in I$ and $v \in N$ such that

$$u_s = \sum_{r=1}^{s} x_r u_r + v.$$

This implies

$$(1 - x_s)u_s = \sum_{r=1}^{s-1} x_r u_r + v.$$

Since x_s is contained in every maximal ideal, $1 - x_s$ is a unit in R, and so

$$u_s = \sum_{r=1}^{s-1} x_r (1 - x_s)^{-1} u_r + (1 - x_s)^{-1} v,$$

which contradicts the minimality of the chosen system of generators. □

Corollary 39. *Let $(R, \mathfrak{m})$ be a local ring, let M a finitely-generated R-module, and let $u_1, \dots, u_s$ be elements in M such that their classes form a system of generators for the $(R/\mathfrak{m})$-vector space $M/\mathfrak{m}M$. Then $u_1, \dots, u_s$ generates M as an R-module.*

Proof. Since $\overline{u}_1, \dots, \overline{u}_s$ generates $M/\mathfrak{m}M$ as an $(R/\mathfrak{m})$-vector space, we have

$$M = \mathfrak{m}M + \sum_{r=1}^{s} Ru_r. \tag{156}$$

Indeed, let $u \in M$. Choose $a_1, \dots, a_s \in R$ such that

$$\overline{u} = \sum_{r=1}^{s} \overline{a}_r \overline{u}_r = \sum_{r=1}^{s} a_r \overline{u}_r.$$

This implies $u - \sum_{r=1}^{s} a_r u_r \in \mathfrak{m}M$. Thus

$$u = \left(u - \sum_{r=1}^{s} a_r u_r \right) + \sum_{r=1}^{s} a_r u_r,$$

shows us that $u \in \mathfrak{m}M + \sum_{r=1}^{s} Ru_r$. Combining (156) with Nakayama's Lemma, we see that

$$M = \sum_{r=1}^{s} Ru_r.$$

□

Remark 66. The finite generation hypothesis is crucial. For a counterexample, consider the local ring $R = \mathbb{Z}_{(p)}$ and the quotient R-module $\mathbb{Q}/\mathbb{Z}_{(p)}$. In this case $\mathfrak{m} = pR$, so

$$\begin{aligned} M/\mathfrak{m}M &= M/pM \\ &= 0, \end{aligned}$$

since every element of $\mathbb{Q}$ has the form px for some $x \in \mathbb{Q}$. However, obviously $M \neq 0$ (and also M is not finitely generated as an R-module in this case).

Example 48.2. Let $R = K[x, y, z]_{\langle x,y,z \rangle}$, let $\mathfrak{m} = \langle x, y, z \rangle$, and let M be the R-module with presentation

$$R^2 \xrightarrow{\begin{pmatrix} 0 & y \\ xy-1 & xz \\ xy+1 & xz \end{pmatrix}} R^3 \longrightarrow M \longrightarrow 0.$$

Let $u_i \in M$ be the image the standard basis element $e_i \in R^3$ for $i = 1, 2, 3$. The set $\{u_1, u_2, u_3\}$ is *not* a minimal generating set of M. Indeed, since the functor $- \otimes_R (R/\mathfrak{m})$ is right-exact, we obtain a presentation of the $(R/\mathfrak{m})$-vector space $M/\mathfrak{m}M$:

$$(R/\mathfrak{m})^2 \xrightarrow{\begin{pmatrix} 0 & 0 \\ -1 & 0 \\ 1 & 0 \end{pmatrix}} (R/\mathfrak{m})^3 \longrightarrow M/\mathfrak{m}M \longrightarrow 0$$

This presentation matrix has rank 1, and so $M/\mathfrak{m}M$ is a 2-dimensional K-vector space. In fact, it's not hard to see that

$$M/\mathfrak{m}M = K\overline{u}_1 + K\overline{u}_3,$$

since the equation $-\overline{u}_2 + \overline{u}_3 = 0$ tells us that $\overline{u}_2$ is superfluous. According to Nakayama's Lemma, we should be able to lift $\overline{u}_1, \overline{u}_3 \in M/\mathfrak{m}M$ to a minimal generating set of M. In particular, $\{u_1, u_3\}$ should be a minimal generating set of M. To see that it is, we use the fact that $xy - 1$ is a unit in R to perform the following sequence of elementary row and column operations:

$$\begin{pmatrix} 0 & y \\ xy-1 & xz \\ xy+1 & xz \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & y \\ xy-1 & xz \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & y \\ xy-1 & 0 \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & y \\ 1 & 0 \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix}.$$

Letting $\{e_1', e_2'\}$ denote the standard basis for R^2, then this sequence of elementary row operations corresponds base changes:

$$\{e_1, e_2, e_3\} \to \{e_1, (xy-1)e_2 + (xy+1)e_3, e_3\} \qquad \text{and} \qquad \{e_1', e_2'\} \to \left\{e_1', \frac{-xz}{xy-1}e_1' + e_2'\right\}.$$

So we see that $\begin{pmatrix} 0 & y \\ 1 & 0 \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix}$ can be used as a presentation matrix for M. Again, the trivial condition $u_2 = 0$ implies that we can toss u_2 out, so that

$$M = Ru_1 + Ru_3.$$

Lemma 48.2. *Let M be a finitely generated R-module and let S be a multiplicatively closed subset of R. Suppose $u_1, \dots, u_m \in M$ generate M_S as an R_S-module. Then there exists an $s \in S$ such that $u_1, \dots, u_m$ generate M_s as an R_s-module.*

Remark 67. In particular, the lemma says that if $M_S = 0$ then there exists an $s \in S$ such that $M_s = 0$.

Proof. Suppose $v_1, \dots, v_n \in M$ generate M as an R-module. Since $u_1, \dots, u_m$ generate M_S as an R_S-module, for each $1 \leq j \leq n$, we have

$$v_j = \sum_{i=1}^{m} (r_{ij}/s_{ij})u_i$$

where $r_{ij} \in R$ and $s_{ij} \in S$. In particular, v_j is contained in the R_s-submodule of M_s generated by $u_1, \dots, u_m$ where s is the product of all of the s_{ij}. Since $v_1, \dots, v_n$ already generate M as an R-module, it follows that $u_1, \dots, u_m$ generates M_s as an R_s-module. □

48.2 Krull's Intersection Theorem

We now prove the following important corollary of Nakayama's Lemma:

Corollary 40. *(Krull's interesection theorem) Let R be a Noetherian ring, let I be an ideal contained in the Jacobson radical of R, and let M a finitely generated R-module. Then*

$$\bigcap_{k \in \mathbb{N}} I^k M = 0.$$

Proof. Let $N := \bigcap_k I^k M$. Then N is a finitely generated R-module since it is a submodule of the finitely generated module M over the Noetherian ring R. By Nakayama's Lemma, it is sufficient to show that $IN = N$. Let

$$\mathcal{L} := \{L \subset M \text{ submodule } \mid L \cap N = IN\}.$$

The set $\mathcal{L}$ is nonempty since $IN \in \mathcal{L}$. Since R is Noetherian, the set $\mathcal{L}$ has a maximal element, choose $L \in \mathcal{L}$ to be such a maximal element. It remains to prove that $I^k M \subset L$ for some k, because this implies

$$\begin{aligned} N &= I^k M \cap N \\ &\subset L \cap N \\ &= IN, \end{aligned}$$

and from Nakayama's Lemma, we would conclude that $N = 0$. Since I is finitely generated, it suffices to prove that for any $x \in I$ there is some positive integer $n \in \mathbb{N}$ such that $x^n M \subset L$ (If $I = \langle x_1, \dots, x_s \rangle$ with $x_r^{n_r} M \subset L$ for each $1 \leq r \leq s$, then $I^{n_1 + \cdots + n_s} M \subset L$).

Let $x \in I$ and consider the chain of ideals

$$L :_M x \subset L :_M x^2 \subset \cdots.$$

This chain stabilizes because R is Noetherian. Choose $n \in \mathbb{N}$ with $L :_M x^n = L :_M x^{n+1}$. We claim that $x^n M \subset L$. Indeed, by the maximality of L it is enough to prove that $(L + x^n M) \cap N \subset IN$ since obviously,

$$\begin{aligned} IN &= L \cap N \\ &\subset (L + x^n M) \cap N. \end{aligned}$$

Let $u \in (L + x^n M) \cap N$, so $u = v + x^n w$, with $v \in L$ and $w \in M$. Now

$$\begin{aligned} x^{n+1} w &= xu - xv \\ &\in IN + L \\ &= L \cap N + L \\ &= L, \end{aligned}$$

which implies $w \in L :_M x^{n+1} = L :_M x^n$. Therefore, $x^n w \in L$, and, consequently, $u \in L$. This implies $u \in L \cap N = IN$. □

49 Filtered Rings and Modules

49.1 Filtered Rings

Definition 49.1. A **filtered ring** is a ring R together with a descending sequence $(R_n)_{n\in\mathbb{Z}_{\geq 0}}$ of ideals R_n of R which satisfies $R_0 = R$ and $R_m R_n \subseteq R_{m+n}$ for all m,n. The sequence (R_n) is called a **filtration** of R. If Q is an ideal of R, then (Q^n) is a filtration of R. We call this the Q**-filtration** of R. In this case, we call $R = (Q^n)$ the Q**-filtered ring**.

49.1.1 The associated graded ring

Let $R = (R_n)$ be a filtered ring. Let $\mathrm{gr}(R)$ be the graded module given by

$$\mathrm{gr}(R) = \bigoplus_{n=0}^{\infty} \mathrm{gr}_n(R) = \bigoplus_{n=0}^{\infty} R_n/R_{n+1},$$

The canonical maps $R_m \times R_n \to R_{m+n}$ define, by passing to quotients, bilinear maps from $\mathrm{gr}_m(R) \times \mathrm{gr}_n(R) \to \mathrm{gr}_{m+n}(R)$, whence a bilinear map from $\mathrm{gr}(R) \times \mathrm{gr}(R)$ to $\mathrm{gr}(R)$. We obtain a graded ring structure on $\mathrm{gr}(R)$; this is called the **graded ring associated to the filtered ring** R.

Example 49.1. Let $R = \Bbbk[x,y,z]$ and let $A = R_{\mathfrak{m}}/I$ where $I = \langle x^2+y^3+z^4, xy+xz+z^3\rangle$ and $\mathfrak{m} = \langle x,y,z\rangle$. Equip A with the $\mathfrak{m}$-adic filtration. A standard basis for I with respect to the ds order is given by

$$\begin{aligned} g_1 &= x^2+y^3+z^4 \\ g_2 &= xy+xz+z^3 \\ g_3 &= y^4+y^3z-xz^3+yz^4+z^5. \end{aligned}$$

Therefore $\mathrm{gr}\, A = R/J$ where $J = \langle x^2, xy+xz, y^4+y^3z-xz^3\rangle$. A free resolution $\mathrm{gr}\, A$ over R is given by

$$R(-3)\oplus R(-5) \xrightarrow{\begin{pmatrix} x & y^3 \\ -y-z & -z^3 \\ 0 & -x \end{pmatrix}} R(-2)\oplus R(-2)\oplus R(-4) \xrightarrow{\begin{pmatrix} xy+xz & x^2 & y^4+y^3z-xz^3 \end{pmatrix}} R \longrightarrow R/J$$

Therefore we conclude that the Hilbert-Poincare series of $\mathrm{gr} A$ is given by

$$\begin{aligned} \mathcal{H}_{\mathrm{gr}\, A}(t) &= \frac{1-\left(t^2+t^2+t^4\right)+\left(t^3+t^5\right)}{(1-t)^3} \\ &= \frac{1+2t+t^2+t^3}{1-t} \\ &= 1+3t+4t^2+5t^3+5t^4+5t^5+\cdots. \end{aligned}$$

In particular, $\deg(\mathrm{gr}\, A) = 5$ and $P(n) = 5$ where P is the hilbert polynomial of $\mathrm{gr}\, A$. Therefore $\mathrm{mult}(A,\mathfrak{m}) = 5$ and $\deg(\mathrm{HSP}_{M,Q}) = 1$. Finally, we list the first few graded pieces of $\mathrm{gr}\, A$:

$$\begin{aligned} A/\mathfrak{n} &= \Bbbk \\ \mathfrak{n}/\mathfrak{n}^2 &= \Bbbk\overline{x}+\Bbbk\overline{y}+\Bbbk\overline{z} \\ \mathfrak{n}^2/\mathfrak{n}^3 &= \Bbbk\overline{xz}+\Bbbk\overline{y}^2+\Bbbk\overline{yz}+\Bbbk\overline{z}^2 \\ \mathfrak{n}^3/\mathfrak{n}^4 &= \Bbbk\overline{xz}^2+\Bbbk\overline{y}^3+\Bbbk\overline{y}^2\overline{z}+\Bbbk\overline{yz}^2+\Bbbk\overline{z}^3 \\ \mathfrak{n}^4/\mathfrak{n}^5 &= \Bbbk\overline{xz}^3+\Bbbk\overline{y}^3\overline{z}+\Bbbk\overline{y}^2\overline{z}^2+\Bbbk\overline{yz}^3+\Bbbk\overline{z}^4 \\ &\vdots \end{aligned}$$

49.1.2 The associated blowup ring

Definition 49.2. Let $R = (R_n)$ be a filtered ring. Let $\mathrm{bl}(R)$ be the graded module given by

$$\mathrm{bl}(R) = \bigoplus_{n=0}^{\infty} R_n = R + R_1 t + R_2 t^2 + R_3 t^3 + \cdots$$

where we view t as an indeterminate variable which keeps track of the grading: the homogeneous component in degree n is $\mathrm{bl}_n(R) = R_n t^n$ and where multiplication is uniquely determined by

$$(xt^m)(yt^n) = xyt^{m+n}$$

for all $x \in R_m$ and $y \in R_n$. In particular, $\mathrm{bl}(R)$ inherits the structure of a graded R-algebra with $\mathrm{bl}_0(R) = R$; this is called the **blowup algebra associated to the filtered ring** R. The blowup algebra comes equipped with a maximal ideal

$$\mathrm{bl}(R_1) = \bigoplus_{n=0}^{\infty} R_{n+1} = R_1 + R_2 t + R_2 t^2 + R_3 t^3 + \cdots$$

We obtain an isomorphism $\mathrm{bl}(R)/\mathrm{bl}(R_1) \simeq \mathrm{gr}(R)$.

Proposition 49.1. *Let $R = (Q^n)$ be the Q-filtered ring where Q is an ideal of R. Then $\mathrm{bl}(R)$ is a noetherian.*

Proof. Since R is Noetherian, R_1 is a finitely-generated R-ideal, say

$$R_1 = \langle x_1, \dots, x_s \rangle_R = Rx_1 + \cdots + Rx_s.$$

This implies $\mathrm{bl}(R_1)$ is a finitely generated $\mathrm{bl}(R)$-ideal with

$$\mathrm{bl}(R_1) = \langle x_1 t, \dots, x_s t \rangle_{\mathrm{bl}(R)} = \mathrm{bl}(R)x_1 t + \cdots \mathrm{bl}(R)x_s t,$$

here we are using the fact that $R_m R_n = R_{m+n}$ for all $m, n \in \mathbb{N}$. There is a unique R-algebra homomorphism

$$\varphi \colon R[X_1, \dots, X_s] \to \mathrm{bl}(R)$$

such that $\varphi(X_r) = x_r t$ for all $1 \le r \le s$. This homomorphism is a surjective ring homomorphism from a Noetherian ring, and hence $\mathrm{bl}(R)$ is a noetherian ring. □

Example 49.2. Let $R = \Bbbk[x,y]/\langle y^2 - x^3 - x^2 \rangle$, let $Q = \langle \overline{x}, \overline{y} \rangle$ (we drop the overlines from $\overline{x}$ and $\overline{y}$ in just write x and y in order to simplify notation in what follows), and equip R with the Q-filtration making $R = (Q^n)$ into a filtered ring. Let $\varphi \colon R[u,v] \to \mathrm{bl}(R)$ be the unique surjective R-algebra homomorphism such that $\varphi(u) = xt$ and $\varphi(v) = yt$. The kernel of φ is an ideal of $R[u,v]$ which is homogeneous in the variables u, v:

$$\ker \varphi = \langle (x^2 + x)u - yv, v^2 - (x+1)u^2, yv - (x+1)xu, xv - yu \rangle.$$

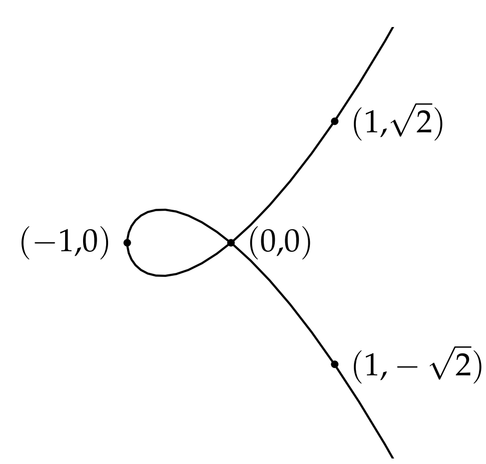
Thus we see that $\mathrm{bl}(R) \cong \Bbbk[x,y,u,v]/\mathfrak{a}$ where

$$\mathfrak{a} = \langle v^2 - (x+1)u^2, yv - (x+1)xu, xv - yu, y^2 - x^3 - x^2 \rangle.$$

In particular, $\mathrm{bl}(R)$ corresponds to an algebraic subset $Y \subseteq \mathbb{A}^2_{x,y} \times \mathbb{P}^1_{u,v}$. Let $A = R[v]/\langle v^2 - (x+1), yv - x(x+1), xv - y \rangle$, so A corresponds to the affine open $U = Y \cap (\mathbb{A}^2_{x,y} \times \mathrm{D}(u))$. We have a canonical ring homomorphism $\iota \colon R \to A$ where ι is the inclusion map. Let us try to understand this homomorphism from a geometric point of view. Let $V = \mathrm{V}_K(y^2 - x^3 - x^2)$ be affine algebraic subset of $\mathbb{A}^2(\Bbbk)$ defined by the equation $y^2 = x^3 + x^2$. The points of $\operatorname{Spec} R$ are in one-to-one correspondence with the points of V: they are all of the form

$$\mathfrak{p}_{(a,b)} = \langle x - a, y - b \rangle$$

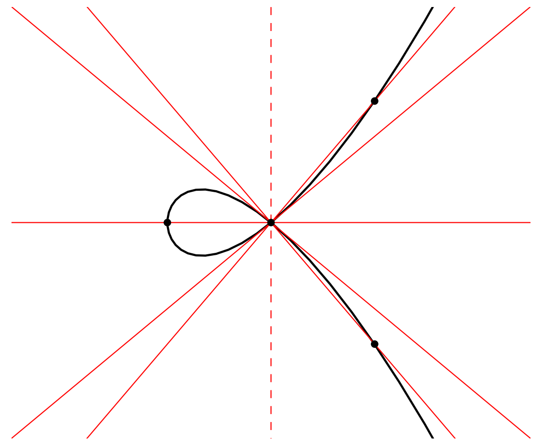
where $(a,b) \in V$, that is, where $a, b \in K$ such that $b^2 = a^3 + a^2$. If $K = \mathbb{R}$, we can visualize the points of $\operatorname{Spec} R$ as below:



The points of Spec A correspond to the affine open set X: they have the form

$$\mathfrak{p}_{(a,b),[1:t]} = \langle x-a, y-b, v-\mu \rangle$$

where $a, b, \mu \in K$ such that $b^2 = a^3 + a^2$, $\mu = b/a$, and $\mu^2 = a+1$. If $K = \mathbb{R}$. we can visualize the points of Spec A as below:/



In particular, $\mathfrak{p}_{(a,b),[1:\mu]}$ corresponds to the point $(a,b) \in V$ together with a line $y = \mu x$ that passes through that point, where μ represents the slope of that line. The map $\iota \colon R \to A$ induces a continuous map ${}^{\mathrm{a}}\iota \colon \operatorname{Spec} A \to \operatorname{Spec} R$ given by

$${}^{\mathrm{a}}\iota(\mathfrak{p}_{(a,b),[1:\mu]}) = \mathfrak{p}_{(a,b)}.$$

This corresponds to the projection map $\pi \colon U \to V$ given by

$$\pi(a,b,\mu) = (a,b).$$

For instance, there are two points in U which map onto the origin $(0,0)$, namely $(0,0,1)$ and $(0,0,-1)$, corresponding to the lines $y = x$ and $y = -x$ respectively. Notice that in the image above there are "missing" points. For instance, we drew a vertical dashed line in the image above; it should correspond to the line $x = 0$, but it has nowhere to go under this projection. In fact, this missing line corresponds to the extra point in $\operatorname{Proj}(\operatorname{bl}(R))$ which doesn't belong to A.

49.2 Seminorms

Definition 49.3. Let R be a ring and let $\|\cdot\| \colon R \to [0,\infty]$ be a map.

1. We say $\|\cdot\|$ is **normalized** if $\|0\| = 0$ and $\|1\| = 1 = \|-1\|$.
2. We say $\|\cdot\|$ is **positive-definite** if $\|r\| = 0$ if and only if $r = 0$.
3. We say $\|\cdot\|$ is **submultiplicative** if
$$\|r_1 r_2\| \leq \|r_1\|\|r_2\| \tag{157}$$
for all $r_1, r_2 \in R$. If (157) is an equality, then we say $\|\cdot\|$ is **multiplicative**. Finally we say $\|\cdot\|$ is **power-multiplicative** if
$$\|r^n\| = \|r\|^n$$
for all $r \in R$ and $n \in \mathbb{N}$.
4. We say $\|\cdot\|$ is **subadditive** if
$$\|r_1 + r_2\| \leq \|r_1\| + \|r_2\|$$
for all $r_1, r_2 \in R$. If $\|\cdot\|$ satisfies the stronger property that
$$\|r_1 + r_2\| \leq \max\{\|r_1||, \|r_2\|\}$$
for all $r_1, r_2 \in R$, then we say $\|\cdot\|$ is **ultraadditive** or **non-Archimedean**.

Definition 49.4. Let R be a ring and equip it with a map $\|\cdot\|\colon R \to [0,\infty]$.

1. If $\|\cdot\|$ is normalized, submultiplicative, and subadditive, then we call $\|\cdot\|$ an R**-seminorm** (or more simply **seminorm** if R is understood from context) and we call the pair $R = (R, \|\cdot\|)$ a **seminormed ring**. In this case, note that $\|\cdot\|$ being normalized and submultiplicative implies $\|-r\| = \|r\|$ for all $r \in R$. If $||\cdot||$ is a seminorm which is also positive-definite, then we call $\|\cdot\|$ a **norm** and we call the pair $R = (R, \|\cdot\|)$ a **normed ring**.

2. If $\|\cdot\|$ is normalized, submultiplicative, and ultraadditive, then we call $\|\cdot\|$ an **ultraseminorm** or **non-Archimedean seminorm** and we call the pair $R = (R, \|\cdot\|)$ an **ultraseminormed ring** or a **non-Archimedean seminormed ring**. In this case, note that $\|\cdot\|$ being normalized and submultiplicative implies $\|-r\| = \|r\|$ for all $r \in R$. If $||\cdot||$ is a seminorm which is also positive-definite, then we call $\|\cdot\|$ an **ultranorm** or **non-Archimedean norm** and we call the pair $R = (R, \|\cdot\|)$ an **ultranormed ring** or a **non-Archimedian normed ring**.

3. We call $\|\cdot\|$ a **semivaluation** and R is **semivalued ring** if $\|\cdot\|$ is a multiplicative seminorm and we call $\|\cdot\|$ a **valuation** and R a **valued ring** if $\|\cdot\|$ is a multiplicative norm.

Proposition 49.2. *Let R be a non-Archimedean seminormed ring and let $r_1, r_2 \in R$ such that $\|r_1\| > \|r_2\|$. Then $\|r_1 + r_2\| = \|r_1\|$.*

Proof. The non-Archimedian property of $\|\cdot\|$ already tells us that $\|r_1 + r_2\| \leq \|r_1\|$. To prove the reverse inequality, note that $\|r_1 - r_2\| \leq \|r_1\|$, thus if we set $r_1 = r_1 + r_2$, then we obtain $\|r_1\| \leq \|r_1 + r_2\|$. It follows that $\|r_1 + r_2\| = \|r_1\|$. □

Proposition 49.3. *A power-multiplicative seminorm $\|\cdot\|$ on R is non-Archimedian if and only of $\|n\| \leq 1$ for all $n \in \mathbb{Z}$.*

Remark 68. Let R be a seminormed ring such that $\|R\| \leq 1$ (meaning $\|r\| \leq 1$ for all $r \in R$). Then we have $\|R^\times\| = 1$. Indeed, let $u, v \in R^\times$ such that $uv = 1$. Then we have

$$\begin{aligned} 1 &= \|1\| \\ &= \|uv\| \\ &\leq \|u\|\|v\| \\ &\leq 1. \end{aligned}$$

It follows that $\|u\| = 1 = \|v\|$.

49.2.1 Pseudometric induced by seminorm

An R-seminorm $\|\cdot\|$ induces an R**-pseudometric** d in the usual way, namely d is defined by

$$\mathrm{d}(r_1, r_2) = \|r_1 - r_2\|$$

for all $r_1, r_2 \in R$. Being a psuedometric means that it satisfies the following three properties:

1. $\mathrm{d}(r, r) = 0$ for all $r \in R$.

2. $\mathrm{d}(r_1, r_2) = \mathrm{d}(r_2, r_1)$ for all $r_1, r_2 \in R$.

3. $\mathrm{d}(r_1, r_3) \leq \mathrm{d}(r_1, r_2) + \mathrm{d}(r_2, r_3)$ for all $r_1, r_2, r_3 \in R$.

Indeed, the first two properties are trivial. For the third property, observe that

$$\begin{aligned} \mathrm{d}(a, c) &= N(a - c) \\ &= N(a - c + c - b) \\ &\leq \max\{N(a - c), N(c - b)\} \\ &= \max\{N(a - c), N(b - c)\} \\ &= \max\{\mathrm{d}(a, c), \mathrm{d}(b, c)\} \end{aligned}$$

for all $a, b, c \in R$.

Finally, the R-pseudoultranorm N gives R the structure of a **psuedoultranormed space**. For each $a \in R$ and m we define

$$\mathrm{B}_m^R(a) = \mathrm{B}_m(a) := \{x \in R \mid N(x - a) < 1/m\} = \{x \mid \mathrm{d}(x, a) < 1/m\}. \tag{158}$$

Next we define

$$\mathcal{B}^R = \mathcal{B} = \{\mathrm{B}_m(a) \mid a \in R \text{ and } m \in \mathbb{N}\},$$

and we let $\tau(\mathcal{B})$ be the smallest topology which contains $\mathcal{B}$. The topology $\tau(\mathcal{B})$ is called the **topology induced by pseudoultranorm** N. It is straightforward to theck that $\mathcal{B}$ serves as a basis for this topology.

Proposition 49.4. *$\mathcal{B}$ is a basis.*

Proof. First note that $\mathcal{B}$ covers R. Indeed, for any $m \geq 0$ we have

$$R \subseteq \bigcup_{a \in R} \mathrm{B}_m(a).$$

In fact, we already have $R = \mathrm{B}_0(0)$! Next let $a, b \in R$ and let $n \geq m \geq 0$. Then observe that

$$\mathrm{B}_m(a) \cap \mathrm{B}_n(b) = \begin{cases} \mathrm{B}_n(b) & \text{if } \mathrm{d}(a,b) \leq 1/m \\ \emptyset & \text{else} \end{cases}$$

In particular we see that $\mathcal{B}$ is a basis for M. □

49.2.2 From non-Archimedean R-seminorms to R-filtrations

Unless otherwise specified, we fix $\varepsilon \in (0,1)$ (for instance take $\varepsilon = 1/2$).

Proposition 49.5. *Let R be a ring and let $\|\cdot\|$ be a non-Archimedean R-seminorm such that $\|R\| \leq 1$. For each $n \in \mathbb{N}$, we set*

$$R_n = \{r \in R \mid \|r\| \leq \varepsilon^n\}.$$

*Then (R_n) is an R-filtration, called the **filtration induced by** $\|\cdot\|$.*

Proof. First note that we obviously have $R_0 = R$. Also, (R_n) is obviously a descending sequence of sets. Suppose that $x \in R_m$ and $y \in R_n$. Then

$$\|xy\| \leq \|x\|\|y\| \leq \varepsilon^{m+n}$$

implies $xy \in R_{m+n}$. Thus we have $R_m R_n \subseteq R_{m+n}$. Finally, we need to check that R_n is an ideal. It is clearly closed under scalar multiplication since $R_0 R_n \subseteq R_n$. To see that it is closed under addition, let $x, y \in R_n$. Then we have

$$\|x+y\| \leq \max\{\|x\|, \|y\|\} \leq \varepsilon^n.$$

It follows that R_n is closed under addition as well, so it is an ideal. □

49.2.3 From R-filtrations to non-Archimedean R-seminorms

Proposition 49.6. *Let (R_n) be an R-filtration. Define $\|\cdot\|: R \to [0,1]$ by*

$$\|r\| = \begin{cases} \varepsilon^n & \text{if } r \in R_n \backslash R_{n+1} \\ 0 & \text{if } r \in \bigcap_{n \in \mathbb{N}} R_n \end{cases}$$

*for all $r \in R$. Then $\|\cdot\|$ is a non-Archmedean R-seminorm, called the **non-Archimedean R-seminorm induced by** (R_n).*

Proof. Left as an easy exercise. □

49.3 Filtered R-modules

Definition 49.5. Let $R = (R_n)$ be a filtered ring. A **filtered R-module** is an R-module M together with descending sequence $(M_n)_{n \in \mathbb{Z}}$ of submodules of M which satisfies $M_0 = M$ and $R_m M_n \subseteq M_{m+n}$ for all m, n. If we write "let M be a filtered R-module", then it is understood that R is a filtered ring and that M is a filtered R-module. Given two filtered R-modules M and N, and morphism between them is an R-linear map $\varphi: M \to N$ such that $\varphi(M_n) \subseteq N_n$. The collection of all filtered R-modules and their morphisms forms an additive category which we denoted by $\mathbf{FMod}_R$. If L is an R-submodule of M, then we obtain the **induced filtration** (L_n) on L defined by the formula $L_n = L \cap M_n$. Similarly the **quotient filtration** on M/L is the filtration $((M/L)_n)$ where $(M/L)_n = (M_n + L)/L$. $N_n = (M_n + L)/L$.

Remark 69. If $M = (M_n)$ is a filtered R-module, then we obtain an induced pseduoultranorm $\mathrm{N}_{M,\gamma}$ on M which is defined in the same way as the induced pseudoultranorm $\mathrm{N}_{R,\gamma}$ on R.

In $\mathbf{FMod}_R$, the notion of injective and surjective morphisms are the usual notions. Every morphism $\varphi: M \to N$ admits a kernel $\ker\varphi$ and a cokernel $\operatorname{coker}\varphi$: the underlying modules of $\ker\varphi$ and $\operatorname{coker}\varphi$ are the usual kernel and cokernel, together with the induced filtration and quotient filtration. We similarly define $\operatorname{im}\varphi = \ker(N \to \operatorname{coker}\varphi)$ and $\operatorname{coim}\varphi = \operatorname{coker}(\ker\varphi \to M)$. We have the canonical factorization:

$$\ker\varphi \to M \to \operatorname{coim}\varphi \xrightarrow{\theta} \operatorname{im}\varphi \to N \to \operatorname{coker}\varphi$$

where θ is bijective. One says that φ is a **strict morphism** if θ is an isomorphism of filtered modules, it amounts to the same as saying $\varphi(M_n) = \varphi(M) \cap N_n$ for each $n \in \mathbb{Z}$ (in general we only have $\varphi(M_n) \subseteq \varphi(M) \cap N_n$). There exist bijective morphisms that are not isomorphisms ($\mathbf{FMod}_R$ is *not* an abelian category).

49.3.1 The associated graded module

Definition 49.6. Let $R = (R_n)$ be a filtered ring and let $M = (M_n)$ be a filtered R-module. Let $\operatorname{gr}(M)$ be the graded module given by

$$\operatorname{gr}(M) = \bigoplus_{n=0}^{\infty} \operatorname{gr}_n(M) = \bigoplus_{n\in\mathbb{Z}} M_n/M_{n+1},$$

The canonical maps $R_m \times M_n \to M_{m+n}$ define, by passing to quotients, bilinear maps from $\operatorname{gr}_m(R) \times \operatorname{gr}_n(M) \to \operatorname{gr}_{m+n}(M)$, whence a bilinear map from $\operatorname{gr}(R) \times \operatorname{gr}(M)$ to $\operatorname{gr}(M)$. Thus, $\operatorname{gr}(M)$ obtains the structure of a graded $\operatorname{gr}(R)$-module; this is called the **graded module associated to the filtered ring** R. If $\varphi\colon M \to N$ is a morphism of filtered R-modules, then φ defines, by passing to quotients, homomorphisms

$$\operatorname{gr}_n(\varphi) : M_n/M_{n+1} \to N_n/N_{n+1}$$

whence a homomorphism $\operatorname{gr}(\varphi)\colon \operatorname{gr}(M) \to \operatorname{gr}(N)$. We obtain a functor

$$\operatorname{gr}\colon \mathbf{FMod}_R \to \mathbf{GMod}_{\operatorname{gr}(R)}$$

from the category of filtered R-modules to the category of graded $\operatorname{gr}(R)$-modules.

49.3.2 The associated blowup module

Definition 49.7. Let $M = (M_n)$ be a filtered R-module. Let $\operatorname{bl}(M)$ be the graded module given by

$$\operatorname{bl}(M) = \bigoplus_{n=0}^{\infty} M_n = M + M_1 t + M_2 t^2 + M_3 t^3 + \cdots$$

where we view t as an indeterminate variable which keeps track of the grading: the homogeneous component in degree n is $\operatorname{bl}_n(M) = M_n t^n$ and where R-scalar multiplication is defined by

$$(at^m)(ut^n) = aut^{m+n}$$

where $a \in R_m$ and $u \in M_n$. In particular, $\operatorname{bl}(M)$ inherits the structure of a graded $\operatorname{bl}(R)$-module; this is called the **blowup module associated to the filtered module** M.

49.3.3 Pseudometric Induced by Q-Filtration

We now want to show that M is actually a pseudo-ultrametric space where the $\mathrm{B}_m(u)$ defined in (**??**) are actually the open balls for this pseudo-ultrametric. We define $\mathrm{d}_{(M_n)}\colon M \times M \to \mathbb{R}$ by

$$\mathrm{d}_{(M_n)}(u,v) = \begin{cases} c^n & \text{if } u - v \in M_n \backslash M_{n+1} \\ 0 & \text{if } u - v \in \bigcap_{n\in\mathbb{N}} M_n \end{cases}$$

where $c \in (0,1)$ (it doesn't matter which c we choose, but typically we choose $c = 1/e$ in the characteristic 0 case and we choose $c = 1/p$ in the characteristic p case). As usual we supress (M_n) from the subscript and simply write d whenever context is clear. In particular, if $u - v \in M_n$, then $\mathrm{d}(u,v) \leq c^n$. We claim that d is a pseudo-ultrametric. Indeed, it is obviously symmetric. It also satisfies the strong triangle inequality: given $u, v, w \in M$, we have

$$\mathrm{d}(u,w) \leq \max(\mathrm{d}(u,v), \mathrm{d}(v,w)).$$

Indeed, suppose $u, v, w \in M$ such that $u - v \in M_m \backslash M_{m+1}$ and $v - w \in M_n \backslash M_{n+1}$, where without loss of generality, we may assume $n \geq m$. Then $u - w = (u - v) + (v - w) \in M_m$. Thus we certainly have

$$\begin{aligned} \mathrm{d}(u,w) &\leq c^m \\ &= \max(c^m, c^n) \\ &= \max(\mathrm{d}(u,v), \mathrm{d}(v,w)). \end{aligned}$$

Note that if $n > m$, then this is actually an equality: since $u - v \notin M_{m+1}$, we cannot have $u - w = (u - v) + (v - w) \in M_{m+1}$ since $v - w \in M_{m+1}$. Finally note that $\mathrm{d}(u, u) = 0$ for all $u \in M$, however there may exist two distinct $u, v \in M$ such that $\mathrm{d}(u, v) = 0$. This is why d is just a pseudo-ultrametric and not a genuine ultrametric: it need not satisfy positive-definiteness. It's easy to see however that it will be a genuine ultrametric if and only if $\bigcap M_n = 0$ if and only if M is Hausdorff. Finally, observe that for each $u \in M$ and $m \geq 0$, we have

$$\begin{aligned} \mathrm{B}_m(u) &= u + M_m \\ &= \{u + v \mid v \in M_m\} \\ &= \{w \mid u - w \in M_m\} && \text{setting } w = u + v \\ &= \{w \mid \mathrm{d}(u, w) \leq c^m\}. \end{aligned}$$

Thus the $\mathrm{B}_m(u)$'s are precisely the open balls in the pseudo-ultrametric space induced by the pseudo-ultrametric d.

49.3.4 Convergence, Cauchy sequences, and completion

Since we are working in a pseudoultrametric space, it makes sense to talk about Cauchy sequences and completeness.

Definition 49.8. Let $M = (M_n)$ be a filtered R-module and let (u_n) be a sequence of elements in M.

1. We say the sequence (u_n) converges to an element $u \in M$ if for all $k \in \mathbb{N}$ there exists $\pi(k) \in \mathbb{N}$ such that

$$n \geq \pi(k) \text{ implies } u_n - u \in M_k. \tag{159}$$

   In this case, we say (u_n) is a **convergent sequence** and that it **converges** to u. We denote this by $u_n \to u$ as $n \to \infty$, or $\lim_{n\to\infty} u_n = u$, or even just $u_n \to u$. Note that if M is Hausdorff, then u must be unique: (u_n) can only converge to one element in this case. The function $\pi\colon \mathbb{N} \to \mathbb{N}$ is called a **stabilizing function** of (u_n) (with respect to u). Suppose that $k_1 < k_2$ and $\pi(k_1) > \pi(k_2)$. Then $n \geq \pi(k_2)$ implies $u_n - u \in M_{k_2} \subseteq M_{k_1}$. Thus if we defined $\widetilde{\pi}\colon \mathbb{N} \to \mathbb{N}$ by $\widetilde{\pi}(k_1) := \pi(k_2)$ and $\widetilde{\pi}(k) := \pi(k)$ for all $k \neq k_1$, then we obtain a new stabilizing function of (u_n). In particular, we can always choose a strictly increasing stabilizing function of (u_n) (that is $\pi(k) > k$). The **standard stabilizing function** of (u_n) is the function $\mathrm{s}\colon \mathbb{N} \to \mathbb{N}$ defined by

$$\mathrm{s}(k) = \inf\{m \mid n \geq m \text{ implies } u_n - u \in M_k\}.$$

   In other words, $n \geq \mathrm{s}(k)$ implies $u_n - u \in M_k$ and if $\mathrm{s}(k) \neq 1$ then $n = \mathrm{s}(k) - 1$ implies $u_n - u \notin M_k$. It is straightforward to check that s is an increasing function which satisfies $\mathbf{1} \leq \mathrm{s} \leq \pi$ where $\mathbf{1}\colon \mathbb{N} \to \mathbb{N}$ is the constant function defined by $\mathbf{1}(k) = k$ and where π is a stabilizing function of (u_n). Note we can also describe (159) as saying $n \geq \pi(k)$ implies $\overline{u}_n = \overline{u} = \overline{u}_{\mathrm{s}(k)}$ in M/M_k.

2. We say the sequence (u_n) is M**-Cauchy** (or simply **Cauchy** if M is understood from context) if for all $k \in \mathbb{N}$ there exists $\rho(k) \in \mathbb{N}$ such that

$$n, m \geq \rho(k) \text{ implies } u_m - u_n \in M_k,$$

   or equivalently, $n \geq m \geq \rho(k)$ implies $\overline{u}_m = \overline{u}_n = \overline{u}_{\rho(k)}$ in M/M_k. The set of all Cauchy sequences in M will be denoted $\mathfrak{C}(M)$. The set of all Cauchy sequences which converge to 0 is denoted $\mathfrak{C}_0(M)$. The function $\rho\colon \mathbb{N} \to \mathbb{N}$ is called a **Cauchy-stabilizing function** of (u_n). Note that if $u_n \to u$, then (u_n) is Cauchy, and a Cauchy-stabilizing function of (u_n) is the same as a stabilizing function of (u_n). Indeed, suppose π is a stabilizing function of (u_n). Then $n, m \geq \pi(k)$ implies

$$u_n - u_m = (u_n - u) + (u - u_m) \in M_k.$$

   since $u_n - u \in M_k$ and $u - u_m \in M_k$. It follows that (u_n) is Cauchy and π is a Cauchy-stabilizing function of (u_n). Next suppose that ρ is a Cauchy-stabilizing function of (u_n). If there exists some $m \geq \rho(k)$ such that $u_m - u \in M_k$, then it would follows that $n \geq \rho(k)$ implies

$$u_n - u = (u_n - u_m) + (u_m - u) \in M_k,$$

   so to show ρ is a stabilizing function of (u_n), it suffices to show that for some $m \geq \rho(k)$, we have $u_m - u \in M_k$. But this is clear since $u_n \to u$. Thus we drop "Cauchy" in "Cauchy-stabilizing" and just write "stabilizing" since these give the same concepts when (u_n) is convergent. Note that even though every convergent sequence is Cauchy, we do not necessarily have the converse. We say M is **complete** if every M-Cauchy sequence is convergent.

Example 49.3. Suppose for a convergent sequence (u_n) converging to u, we have

$$\begin{aligned}
&u_1 - u \in M_4 \backslash M_5 && \text{i.e. } \mathrm{d}(u_1, u) = c^4 \\
&u_2 - u \in M_2 \backslash M_3 && \text{i.e. } \mathrm{d}(u_2, u) = c^2 \\
&u_3 - u \in \bigcap M_n && \text{i.e. } \mathrm{d}(u_3, u) = 0 \\
&u_4 - u \in M \backslash M_1 && \text{i.e. } \mathrm{d}(u_4, u) = 1 \\
&u_5 - u \in M_1 \backslash M_2 && \text{i.e. } \mathrm{d}(u_5, u) = c^1 \\
&u_6 - u \in M_4 \backslash M_5 && \text{i.e. } \mathrm{d}(u_6, u) = c^4 \\
&u_7 - u \in M_2 \backslash M_3 && \text{i.e. } \mathrm{d}(u_7, u) = c^2 \\
&u_8 - u \in M_4 \backslash M_5 && \text{i.e. } \mathrm{d}(u_8, u) = c^4 \\
&u_n - u \in \bigcap M_n && \text{for } n \geq 9
\end{aligned}$$

Then $\mathrm{s}(1) = 5$ since $u_n - u \in M_1$ for all $n \geq 5$ and $u_4 - u \notin M$. More generally we have

$$\mathrm{s}(k) = \begin{cases} 5 & \text{if } k = 1 \\ 6 & \text{if } k = 2 \\ 8 & \text{if } k = 3, 4 \\ 9 & \text{if } k \geq 5 \end{cases}$$

49.3.5 Analytic Description of Completion

In analysis, one learns about how to construct a completion of a given metric space (X, d). Let us briefly recall how this works. We define $\mathfrak{C}(X)$ to be the set of all Cauchy sequences in X. The metric d on X induces a pseudometric $\widetilde{\mathrm{d}}$ on $\mathfrak{C}(X)$, defined by

$$\widetilde{\mathrm{d}}((x_n), (y_n)) = \lim_{n \to \infty} \mathrm{d}(x_n, y_n). \tag{160}$$

One shows that (160) is a well-defined pseudometric on $\mathfrak{C}(X)$ and that $\mathfrak{C}(X)$ is a complete pseudometric space. To get a genuine metric space, we put an equivalence relation on $\mathfrak{C}(X)$, namely we say $(x_n) \sim (y_n)$ if and only if $\widetilde{\mathrm{d}}((x_n), (y_n)) = 0$. One then shows that the pseudometric $\widetilde{\mathrm{d}}$ on $\mathfrak{C}_X$ induces a genuine metric $[\widetilde{\mathrm{d}}]$ on $[\mathfrak{C}(X)] = \mathfrak{C}(X)/\sim$. Finally one shows that $([\mathfrak{C}(X)], [\widetilde{\mathrm{d}}])$ is a **completion** of (X, d). This means that $[\mathfrak{C}(X)]$ is complete and that the natural map $\iota \colon X \to [\mathfrak{C}(X)]$ given by $x \mapsto (\overline{x})$ is an isometric embedding with dense image. It can be shown that completions are unique up to a unique isometry which respects inclusion maps. Thus we typically refer to $[\mathfrak{C}(X)]$ as *the* completion of X.

49.3.6 Algebraic Description of Completion

Returning to our setting, note that $\mathfrak{C}^0(M)$ plays the role of the equivalence relation $\sim$ above, namely $(u_n) \sim (v_n)$ if and only if $(u_n - v_n) \in \mathfrak{C}^0(M)$. It is easy to then see that $[\mathfrak{C}(M)] = \mathfrak{C}(M)/\mathfrak{C}^0(M)$ is the completion of M. In fact, we have more structure on $[\mathfrak{C}(M)]$. Indeed, $\mathfrak{C}(M)$ is a R-module and $\mathfrak{C}^0(M)$ is an R-submodule of $\mathfrak{C}(M)$, where addition and multiplication are defined pointwise. Thus we have an R-module structure on $[\mathfrak{C}(M)]$. Here's is a really nice description of $[\mathfrak{C}(M)]$ as an R-module:

Theorem 49.1. *We have an R-module isomorphism*

$$[\mathfrak{C}(M)] \cong \varprojlim M/M_k.$$

Proof. We define $\Phi \colon [\mathfrak{C}(M)] \to \varprojlim M/M_k$ as follows: let $[(u_n)] \in [\mathfrak{C}(M)]$, so (u_n) is a Cauchy sequence which represents the coset $[(u_n)]$. For each $k \in \mathbb{N}$, choose $\pi(k) \in \mathbb{N}$ such that $m, n \geq \pi(k)$ implies $u_n - u_m \in M_k$. In particular, this means $m, n \geq \pi(k)$ implies $\overline{u}_n = \overline{u}_m = \overline{u}_{\pi(k)}$ in M/M_k. Here we think of $\pi \colon \mathbb{N} \to \mathbb{N}$ as a strictly increasing function and we refer to it as a **stabilizing function** for the Cauchy sequence (u_n). We are now ready to define Φ. We set

$$\Phi([(u_n)_{n \in \mathbb{N}}]) = (\overline{u}_{\pi(k)})_{k \in \mathbb{N}}. \tag{161}$$

Note that (161) really does land in $\varprojlim M/M_k$ since π is a stabilizing function for the Cauchy sequence (u_n). We need to check that (161) is well-defined since it clearly depends on many choices.

First, suppose $\rho \colon \mathbb{N} \to \mathbb{N}$ is another stabilizing function for the Cauchy sequence (u_n). So for each $k \in \mathbb{N}$ we have $m, n \geq \rho(k)$ implies $\overline{u}_n = \overline{u}_m$ in M/M_k. Then choosing $n \geq \max(\rho(k), \pi(k))$ would give us $\overline{u}_{\pi(k)} = \overline{u}_n = \overline{u}_{\rho_{(k)}}$ in M/M_k. Thus our construction of Φ does not depend on the choice of a stabilizing function. Next, suppose $(u_n+\varepsilon_n)$ is another representative of the coset $[(u_n)]$ where $\varepsilon_n \to 0$. For each $k \in \mathbb{N}$, choose $\rho(k) \in \mathbb{N}$ such that $n \geq \rho(k)$ implies $\varepsilon_n \in M_k$, and set $\varrho = \max(\pi,\rho)$. Then for each $k \in \mathbb{N}$, we have $\overline{\varepsilon}_{\varrho(k)} = \overline{\varepsilon}_{\rho(k)} = 0$ and $\overline{u}_{\varrho(k)} = \overline{u}_{\pi(k)}$ in M/M_k. Thus

$$(\overline{u}_{\varrho(k)} + \overline{\varepsilon}_{\varrho(k)}) = (\overline{u}_{\pi(k)}).$$

This shows us that Φ does not depend on the choice of a representative of the coset $[(u_n)]$. All choice have been accounted for, and hence Φ is well-defined.

Let us now check that Φ is R-linear. Let $a,b \in R$ and suppose $[(u_n)],[(v_n)] \in [\mathfrak{C}(M)]$. We can choose a common stabilizing function $\pi\colon \mathbb{N} \to \mathbb{N}$ for the Cauchy sequences (u_n) and (v_n), meaning for each $k \in \mathbb{N}$ we have $m,n \geq \pi(k)$ implies $\overline{u}_n = \overline{u}_{\pi(k)}$ and $\overline{v}_n = \overline{v}_{\pi(k)}$ in M/M_k. Then observe that π is a stabilizing function for the Cauchy sequence (au_n+bv_n), hence

$$\begin{aligned}\Phi([(au_n+bv_n)]) &= (a\overline{u}_{\pi(k)} + b\overline{v}_{\pi(k)}) \\ &= a(\overline{u}_{\pi(k)}) + b(\overline{v}_{\pi(k)}) \\ &= a\Phi([u_n]) + b\Phi([v_n]).\end{aligned}$$

Let us now check that Φ is surjective. Let $(\overline{u}_k) \in \varprojlim M/M_k$. So for each $k \in \mathbb{N}$ we have $n,m \geq k$ implies $\overline{u}_n = \overline{u}_m$ in M/M_k. However this is precisely the same thing as saying (u_n) is a Cauchy sequence in M with the identity function $1\colon \mathbb{N} \to \mathbb{N}$ being a stabilizing function for (u_n). Thus $\Phi([(u_n)]) = (u_k)$, and so we see that Φ is surjective.

Finally, let us check that Φ is injective. Suppose $[(u_n)] \in \ker \Phi$. Thus $u_{\pi(k)} \in M_k$ for all $k \in \mathbb{N}$. In particular, we see that $u_{\pi(n)} \to 0$ as $n \to \infty$. However $(u_{\pi(n)})$ being a subsequence of the Cauchy sequence (u_n) forces $u_n \to 0$ as $n \to \infty$ as well. Thus $[(u_n)] = 0$ in $[\mathfrak{C}(M)]$. It follows that Φ is injective. □

Suppose (M'_n) is another Q-filtration of M such that $(M_n) \geq (M'_n)$. Thus there exists some $d \in \mathbb{N}$ such that $M'_n \supseteq M_{n+d}$ for all $n \in \mathbb{Z}$. An (M'_n)-Cauchy sequence is automatically an (M_n)-Cauchy sequence nce the topology induced by (M_n) is *stronger* than the topology induced by (M'_n). Thus we have an inclusion

$$\mathfrak{C}_{(M_n)}(M) \subseteq \mathfrak{C}_{(M'_n)}(M).$$

Furthermore, if a sequence converges to 0 in the (M_n)-topology, then it also converges to 0 in the weaker (M'_n)-topology. Thus we have an inclusion

$$\mathfrak{C}^0_{(M_n)}(M) \subseteq \mathfrak{C}^0_{(M'_n)}(M).$$

Thus we have a natural map

$$\Psi_{(M'_n),(M_n)}\colon [\mathfrak{C}_{(M_n)}(M)] \to [\mathfrak{C}_{(M'_n)}(M)].$$

Let us denote $\Phi_{(M_n)}$ to be the isomorphism constructed in the proof of (49.1). The analagous isomorphism with respect to the Q-filtration (M'_n) is then denoted $\Phi_{(M'_n)}$.

On the other hand, since $M_{n+d} \subseteq M'_n$ for all $n \in \mathbb{N}$, we have natural maps $M/M_{n+d} \to M/M'_n$

Proposition 49.7. *With the notation above, we have a commutative diagram*

$$\begin{array}{ccc} [\mathfrak{C}_{(M'_n)}(M)] & \longrightarrow & \lim M/M'_k \\ \uparrow & & \uparrow \\ [\mathfrak{C}_{(M_n)}(M)] & \longrightarrow & \lim M/M_k \end{array}$$

Proof. Let $[(u_n)] \in [\mathfrak{C}_{(M_n)}(M)]$. Choose a stabilizing function $\pi\colon \mathbb{N} \to \mathbb{N}$ for the (u_n) as an (M_n)-Cauchy sequence. Then observe that for each $k \in \mathbb{N}$, we have $n \geq \pi(k+d)$ implies $u_n \in M_{k+d} \subseteq M'_k$. In particular, the function $\pi_d\colon \mathbb{N} \to \mathbb{N}$, defined by $\pi_d(m) = \pi(d+m)$, is a stabilizing function for (u_n) as an (M'_n)-Cauchy sequence. Thus

$$\Phi_{(M'_n)}[(u_n)] = (\overline{u}_{\pi_d(k)}).$$

□

It is natural to wonder if in fact we have $\Phi_{(M_n)} = \Phi_{(M'_n)}$. Then answer is yes! Indeed, let $[(u_n)] \in [\mathfrak{C}(M)]$ and choose a stabilizing function $\pi\colon \mathbb{N} \to \mathbb{N}$ for (u_n) with respect to $\mathrm{d}_{(M_n)}$. Then for each $k \in \mathbb{N}$ we have $m,n \geq \pi(k+d)$ implies $\overline{u}_n = \overline{u}_m$ in M/M_{k+d}, hence $\overline{u}_n = \overline{u}_m$ in M/M'_k since $M_{k+d} \subseteq M'_k$. In particular, we see that

$$\Phi_{(M_n)}([u_n]) = (\overline{u}_{\pi(k)})$$

49.3.7 Topological equivalence vs strong equivalence

Let $M = (M_n)$ and $M = (M'_n)$ be two filtrations of M (so $M_0 = M = M'_0$) and let d and d' be their corresponding induced pseudoultrametrics. We want to understand under what conditions do these pseudoultrametrics induce the same topology on M. To see what conditions we need, first note that $\tau' \supseteq \tau$ if and only if for each $\mathrm{B}_k(u) \in \mathcal{B}$ there exists $\mathrm{B}'_{\pi(k)}(u) \in \mathcal{B}'$ such that $\mathrm{B}'_{\pi(k)}(u) \subseteq \mathrm{B}_k(u)$. Equivalently, $\tau' \supseteq \tau$ if and only if for each $k \in \mathbb{N}$ there exists $\Pi(k) \in \mathbb{N}$ such that $M'_{\pi(k)} \subseteq M_k$. Note that since (M'_n) is descending, this is equivalent to saying

$$n \geq \Pi(k) \text{ implies } M'_n \subseteq M_k$$

The function $\Pi\colon \mathbb{N} \to \mathbb{N}$ is called a **stabilizing function** of M' with respect to M. Just like in the convergent sequence case, we can choose such a stabilizing function to be strictly increasing, and we can define the **standard stabilizing funcion** of M' with respect to M to be the function $\mathrm{S}_{M',M}\colon \mathbb{N} \to \mathbb{N} \cup \{\infty\}$ defined by

$$\mathrm{S}_{M',M}(k) = \inf\{m \mid M'_m \subseteq M_k\}.$$

In other words, $n \geq \mathrm{S}(k)$ implies $M'_n \subseteq M'_{\mathrm{S}(k)} \subseteq M_k$ and if $\mathrm{S}(k) \neq 1$ then $M'_{\mathrm{S}(k)-1} \not\subseteq M_k$. We say M' it **topologically stronger** than M if

$$\mathrm{S}_{M',M}(k) < \infty$$

for all $k \in \mathbb{N}$. In other words, for each basic open M_k in the M-topology, we can find a basic open M'_m in the M'-topology such that $M'_m \subseteq M_k$. Note that M' being topologically stronger than M is equivalent to saying $\tau' \supseteq \tau$.

Now suppose M is topologically stronger than M' and let (u_n) be an M-Cauchy sequence. Let S denote the standard stabilizing function of M with respect to M' and let s denote the standard stabilizing function of (u_n). Then observe that (u_n) is an M'-Cauchy sequence since

$$\begin{aligned} m, n \geq (\mathrm{s} \circ \mathrm{S})(k) &\implies m, n \geq \mathrm{s}(\mathrm{S}(k)) \\ &\implies u_m - u_n \in M_{\mathrm{S}(k)} \\ &\implies u_m - u_n \in M'_k. \end{aligned}$$

shows that $s \circ S$ is a stabilizing function of (u_n) in the M'-topology. It follows that $\mathfrak{C}(M) \subseteq \mathfrak{C}(M')$. Similarly, if $u_n \to u$ in M, then $u_n \to u$ in M' since

$$\begin{aligned} n \geq (\mathrm{s} \circ \mathrm{S})(k) &\implies n \geq \mathrm{s}(\mathrm{S}(k)) \\ &\implies u_n - u \in M_{\mathrm{S}(k)} \\ &\implies u_n - u \in M_k. \end{aligned}$$

It follows that $\mathfrak{C}_0(M) \subseteq \mathfrak{C}_0(M')$. We get a homomorphism

$$\widehat{M} := \varprojlim M/M_n \simeq \mathfrak{C}(M)/\mathfrak{C}_0(M) \to \mathfrak{C}(M')/\mathfrak{C}_0(M') \simeq \varprojlim M'/M'_k := \widehat{M}'$$

49.4 Contractibility

Let $\varphi\colon (A, \mathfrak{m}) \to (B, \mathfrak{n})$ be a local ring homomorphism and assume that $\mathfrak{m} \neq 0$ (so A is not a field hence B is not a field hence $\mathfrak{n} \neq 0$). Being a local ring homomorphism means $\varphi(\mathfrak{m}) \subseteq \mathfrak{n}$. Since $\varphi^{-1}(\mathfrak{n})$ is necessarily a prime ideal of A, the condition $\varphi(\mathfrak{m}) \subseteq \mathfrak{n}$ is equivalent to the condition $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$. Now equip A with the $\mathfrak{m}$-adic filtration, so $A = (A_n)$ where $A_n = \mathfrak{m}^n$ and let $A' = (A'_n)$ be the filtered A-module where $A'_n = \varphi^{-1}(\mathfrak{n}^n)$ (so in particular we have $A_0 = A = A'_0$ and $A_1 = \mathfrak{m} = A'_1$). Note that (A'_n) really is an $\mathfrak{m}$-filtration since if $x \in A_m = \mathfrak{m}^m$ and $y \in A'_n = \varphi^{-1}(\mathfrak{n}^n)$, then

$$\varphi(xy) = \varphi(x)\varphi(y) \in \varphi(\mathfrak{m}^m)\mathfrak{n}^n \subseteq \mathfrak{n}^{m+n},$$

implies $xy \in A'_{m+n}$. Let S denote the standard stabilizing function of (A'_n) with respect to to (A_n), that is, $S\colon \mathbb{N} \to \mathbb{N} \cup \{\infty\}$ is given by

$$S(k) = \inf\{m \mid A'_m \subseteq A_k\} = \inf\{m \mid \varphi^{-1}(\mathfrak{n}^m) \subseteq \mathfrak{m}^k\}.$$

In other words, if $n \geq S(k)$ then $A_n \subseteq A'_{S(k)} \subseteq A_k$ and if $S(k) > m \geq 1$, then $A'_m \not\subseteq A_k$. Note that if $k_2 \geq k_1$, then $A'_{S(k_2)} \subseteq A_{k_2} \subseteq A_{k_1}$ implies implies $S(k_2) \geq S(k_1)$. Thus the sequence $(S(k)/k)_{k \in \mathbb{N}}$ is monotone increasing, so it makes sense to define the limit

$$c = \mathrm{c}_{B,A} = \lim_{k \to \infty} \frac{S(k)}{k} \in [0, \infty].$$

We call c the **contractibility** of B with respect to A. Note that since φ is a local ring homomorphism, we have $A'_k \supseteq A_k$ for all k. In particular, if A is not Artinian (so (A_n) is strictly descending), then we must have $S \geq \mathbf{1}_k$ (we write $\mathbf{1}_k$ for the function $\mathbb{N} \to \mathbb{N}$ defined by $\mathbf{1}_k(k) = k$). In this case we have $\mathrm{c}_{B,A} \in [1, \infty]$.

Example 49.4. Consider the case where $A = K[y]_{\langle y \rangle}$, $B = K[x,y]_{\langle x,y \rangle}/\langle y^2 - x^3 \rangle$, and $\varphi\colon A \to B$ is the inclusion map. We calculate $A'_n := \varphi^{-1}(\mathfrak{n}^n)$ for various $n \in \mathbb{N}$. We have

$$\begin{aligned}
A'_1 &= \varphi^{-1}(\mathfrak{n}) = \mathfrak{m} \\
A'_2 &= \varphi^{-1}(\mathfrak{n}^2) = \mathfrak{m}^2 \\
A'_3 &= \varphi^{-1}(\mathfrak{n}^3) = \mathfrak{m}^2 && \text{since } y^2 = x^3 \text{ in } B \\
A'_4 &= \varphi^{-1}(\mathfrak{n}^4) = \mathfrak{m}^3 && \text{since } y^3 = x^3 y \text{ in } B \\
A'_5 &= \varphi^{-1}(\mathfrak{n}^5) = \mathfrak{m}^4 && \text{since } y^4 = x^6 \text{ in } B \\
A'_6 &= \varphi^{-1}(\mathfrak{n}^6) = \mathfrak{m}^4 && \text{since } y^4 = x^6 \text{ in } B \\
&\vdots
\end{aligned} \tag{162}$$

If S denotes the standard stabilizing function of (A'_n) with respect to $(\mathfrak{m}^n)$, then the calculations (162) tells us that the sequence $(S(k))_{k \geq 1}$ starts out as

$$(S(k))_{k \geq 1} = (1, 2, 4, 5, 7, 8, \dots)$$

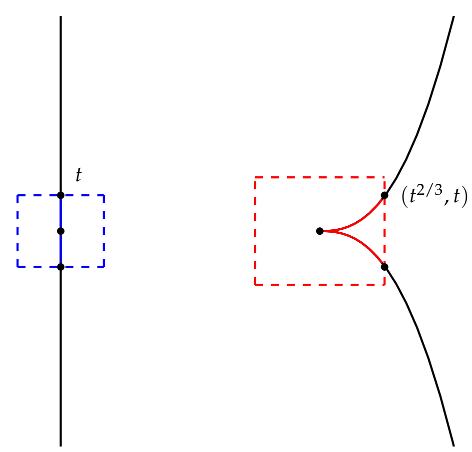
More generally, we have

$$S(n) = \begin{cases} 3m - 2 & \text{if } n = 2m - 1 \text{ where } m \geq 1 \\ 3m - 1 & \text{if } n = 2m \text{ where } m \geq 1 \end{cases}$$

It follows that the contractibility of B with respect to A is given by

$$c = \mathrm{c}_{B,A} = \lim_{k \to \infty} \frac{S(k)}{k} = \frac{3}{2}.$$

To see what's going on geometrically, consider the image below:



The red square represents the open box neighborhood of $\mathfrak{n}$ given by $\{\boldsymbol{x} \in \mathbb{R}^2 \mid \|\boldsymbol{x}\|_\infty < t^{2/3}\}$ (where $t < 1$) and the blue square represents the open box neighborhood of $\mathfrak{m}$ given by $\{\boldsymbol{x} \in \mathbb{R}^2 \mid \|\boldsymbol{x}\|_\infty < t\}$. Intuitively, we think of the ring homomorphism $\varphi\colon A \to B$ as inducing a map $f\colon Y \to X$ given by $f(\mathfrak{n}) = \mathfrak{m}$ where we set $Y = \operatorname{Spec} B = \{0, \mathfrak{n}\}$ and $X = \operatorname{Spec} A = \{0, \mathfrak{m}\}$. The map $f\colon Y \to X$ is thought of as a contraction map with contractibility factor being $3/2$ (the red box whose side length is $2t^{2/3}$ is contracted to the blue box whose side length is $2t$).

Example 49.5. Consider the case where $A = K[y]_{\langle y \rangle}$ and $B = K[y, \boldsymbol{x}]_{\langle y, \boldsymbol{x} \rangle}$ where $\boldsymbol{x} = (x_1, x_2, \dots, x_n, \dots)$. Since

$$A'_k = \varphi^{-1}(\mathfrak{n}^k) = \mathfrak{m}^k = A_k$$

for all $k \in \mathbb{N}$, it follows that $\mathrm{S}_{B,A} = \mathbf{1}_k$ and hence $\mathrm{c}_{B,A} = 1$.

Example 49.6. Consider the case where $A = K[y]_{\langle y \rangle}$ and $B = K[y, \boldsymbol{x}]_{\langle y, \boldsymbol{x} \rangle}/\langle y^2 - x_1^3, y^2 - x_2^4, \dots, y^2 - x_n^{n+2}, \dots \rangle$. Then observe that for each $n > 2$, we have

$$A'_n = \varphi^{-1}(\mathfrak{n}^n) = \mathfrak{m}^2 = A_2$$

since $y^2 = x_{n-2}^n$ in B. In particular, there does not exist an m such that $A'_m \subseteq \mathfrak{m}^3$. It follows that $\mathrm{S}_{B,A}(k) = \infty$ for $k \geq 2$ and hence $\mathrm{c}_{B,A} = \infty$.

Example 49.7. Consider the case where $A = K[y]_{\langle y \rangle}$ and $B = K[y,x]_{\langle y,x\rangle}/\langle y^3 - x_1^2, y^4 - x_2^2, \dots, y^{n+2} - x_n^2, \dots \rangle$. Then observe that for each $n > 2$, we have

$$A_2' = \varphi^{-1}(\mathfrak{n}^2) \subseteq \mathfrak{m}^n = A_n$$

since $y^n = x_{n-2}^2$ in B. In particular, we have $\mathrm{S}_{B,A}(k) = 2$ for $k \geq 2$ and hence $\mathrm{c}_{B,A} = 0$.

Example 49.8. Let R be a commutative ring and let $\mathfrak{p}$ be a prime ideal of R. Equip R with the $\mathfrak{p}$-filtration $R = (R_n)$ where $R_n = \mathfrak{p}^n$. Similary, equip $R_\mathfrak{p}$ with the $\mathfrak{p}R_\mathfrak{p}$-filtration $R_\mathfrak{p} = (R_{\mathfrak{p},n})$ where $R_{\mathfrak{p},n} = \mathfrak{p}^n R_\mathfrak{p}$. Let $\rho \colon R \to R_\mathfrak{p}$ be the canonical localization map given by $\rho(r) = r/1$ for all $r \in R$. Then

$$\mathfrak{p}^{(n)} := \rho^{-1}(\mathfrak{p}^n R_\mathfrak{p}) = \{r \in R \mid rs \in \mathfrak{p}^n \text{ for some } s \in R\backslash\mathfrak{p}\}$$

is called the nth symbolic power of $\mathfrak{p}$. It is the smallest $\mathfrak{p}$-primary ideal which contains $\mathfrak{p}^n$.

49.4.1 Questions

For "nice" local ring homorphisms $A \to B$, the following properties should hold:

1. we have $\mathrm{c}_{B,A} \in \mathbb{Q} \cap [0, \infty]$,
2. if $B \to C$ is another local ring homomorphism, then $\mathrm{c}_{C,B}\mathrm{c}_{B,A} \geq \mathrm{c}_{C,A}$ (where equality holds when something nice happens).

The question we ask now is, what are the "nice" local ring homomorphisms which give rise to those properties? For instance, here's how property (1) could be proved: suppose there exists $k_0 \in \mathbb{N}$ such that

$$\mathrm{c}_{B,A} := \lim_{k\to\infty} \mathrm{S}_{B,A}(k)/k = \mathrm{S}_{B,A}(k_0)/k_0.$$

Then clearly $\mathrm{c}_{B,A} \in \mathbb{Q} \cap [0, \infty]$. Next, suppose that

$$\mathrm{c}_{C,A} = \frac{\mathrm{S}_{C,A}(k_0)}{k_0} \quad \text{and} \quad \mathrm{c}_{B,A} = \frac{\mathrm{S}_{B,A}(k_0)}{k_0}$$

Then if A is not Artinian, we have

$$\begin{aligned}
\mathrm{c}_{C,B} &\geq \frac{\mathrm{S}_{C,A}(\mathrm{S}_{B,A}(k_0))}{\mathrm{S}_{B,A}(k_0)} \\
&\geq \frac{\mathrm{S}_{C,A}(k_0)}{\mathrm{S}_{B,A}(k_0)} \\
&= \frac{\mathrm{c}_{C,A}}{\mathrm{c}_{B,A}},
\end{aligned}$$

so this gives us the inequality $\mathrm{c}_{C,B}\mathrm{c}_{B,A} \geq \mathrm{c}_{C,A}$.

Proposition 49.8. *Let $A \to B \to C$ be local ring homomorphisms. Then*

$$\mathrm{c}_{C,B}\mathrm{c}_{B,A} \geq \mathrm{c}_{C,A}.$$

Proof. □

49.5 Artin-Rees Lemma

Let $M = (M_n)$ be a filtered R-module and assume that $M_n = 0$ for all $n < 0$. For each $k \geq 1$, we define another filtration on M_0: set $M^k = (M_n^k)_{n\in\mathbb{N}}$ where

$$M_n^k = \begin{cases} M_n & \text{if } 0 \leq n \leq k \\ R_{n-k}M_k & \text{if } k < n \end{cases}$$

Thus M^k approximates M to the kth spot, meaning

$$\begin{aligned}
M_0 &= M_0^k \\
M_1 &= M_1^k \\
M_2 &= M_2^k \\
&\vdots \\
M_k &= M_k^k,
\end{aligned}$$

however after the kth spot, M^k usually descends much faster than M: in particular we always have $M_n^k := R_{n-k}M_k \subseteq M_n$ for $k < n$, but we need not have the reverse inclusion. We call M^k the **kth approximation** of M. $M_1 = M_1^k, M_2 = M_2^k, \dots, M_k = M_k^k$, but after the kth spot, M^k may diverge from M. Note that $(\mathrm{bl}(M^k))_{k\in\mathbb{N}}$ is an ascending sequence of $\mathrm{bl}(M)$ submodules whose union is $\mathrm{bl}(M)$.

Lemma 49.2. *(Criterion for stability). $\overline{M}$ is a finitely-generated $\mathrm{B}_Q(R)$-module if and only if (M_n) is Q-stable.*

49.5.1 Artin-Rees Lemma

Lemma 49.3. *(Artin-Rees Lemma) Let $M = (M_n)$ be a stable Q-filtered module and let $L \subseteq M_0$ be an R_0-submodule. Equip L with the induced filtration, $L = (L \cap M_n)$. Then L is a stable Q-filtered module.*

Proof. By Proposition (**??**), we know that $(M_n \cap N)$ is a Q-filtration of N since it is the sequence obtained from the inverse image of the inclusion map $N \hookrightarrow M$. It remains to show that $(M_n \cap N)$ is stable. Appealing to (49.2), we just need to show that $\mathrm{B}_Q((M_n \cap N))$ is a finitely-generated $\mathrm{B}_Q(R)$-module. This is clear though: $\mathrm{B}_Q((M_n \cap N))$ is a $\mathrm{B}_Q(R)$-submodule of $\mathrm{B}_Q((M_n))$ which is finitely-generated, and since $\mathrm{B}_Q(R)$ is Noetherian, $\mathrm{B}_Q((M_n \cap N))$ must be finitely-generated too. □

49.5.2 Consequences of Artin-Rees Lemma

We begin with an alternative proof of Krull's Intersection Theorem:

Lemma 49.4. *(Krull's Interesection Theorem) Let $(R, \mathfrak{m})$ be a Noetherian local ring, let Q be an ideal in R, and let M be a finitely-generated R-module. Then*

$$\bigcap_{n\in\mathbb{N}} Q^n M = 0.$$

Proof. Set $N := \bigcap_{n\in\mathbb{N}} Q^n M$. By Artin-Rees, the Q-filtration $(N \cap Q^n M)$ is stable. Thus there exists a positive integer k such that

$$\begin{aligned} QN &= Q\left(N \cap Q^k M\right) \\ &= N \cap Q^{k+1} M \\ &= N, \end{aligned}$$

and by Nakayama's lemma, this implies $N = 0$. □

Proposition 49.9. *Let R be a Noetherian ring, let $\mathfrak{p}$ be a prime ideal of R, and let I be an ideal of R. For any homomorphism $\varphi\colon I \to R/\mathfrak{p}$, there exists a positive integer d such that φ factors through*

$$I/(\mathfrak{p}^d \cap I) \cong (\mathfrak{p}^d + I)/\mathfrak{p}^d.$$

Proof. By Artin-Rees, $(I \cap \mathfrak{p}^n)$ is a stable $\mathfrak{p}$-filtration. Therefore this exists a positive integer d such that $I \cap \mathfrak{p}^d = \mathfrak{p}\left(I \cap \mathfrak{p}^{d-1}\right)$. This implies $I \cap \mathfrak{p}^d \subset \ker \varphi$. □

Proposition 49.10. *Let A be a ring, Q an ideal in A, and let*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be a short exact sequence of A-modules. Then

$$0 \longrightarrow B_Q(M_1) \longrightarrow B_Q(M_2) \longrightarrow B_Q(M_3)$$

is exact.

Proof. □

49.6 Weierstrauss Preparation Theorem

Throughout this subsection, we study the complete local ring $\Bbbk[\![\boldsymbol{x}]\!] = \Bbbk[\![x_1, \dots, x_n]\!]$ where $\Bbbk$ is a field.

Definition 49.9. Let $f \in \Bbbk[\![\boldsymbol{x}]\!]$. We say f is **x_n-general of order** m if

$$f(\mathbf{0}, x_n) = x_n^m \cdot g(x_n), \quad g(0) \neq 0.$$

In other words, if $f = \sum_{i=0}^{\infty} a_i x_n^i$ where $a_i \in \Bbbk[\![x_1, \dots, x_{n-1}]\!]$, then f is x_n-general of order m if and only if $a_0, a_1, \dots, a_{m-1} \in \langle x_1, \dots, x_{n-1}\rangle$ and a_m is a unit.

Example 49.9. Let $f \in \Bbbk[\![x,y,z]\!]$ be given by

$$f = 2x + xy - x^3 + x^3z + 3y^4 + 4x^5 + y^5 + 5z^6 + x^7yz + 6y^{10} + y^8z^2 + 7z^{10} - z^{11} + \cdots$$

Then

$$\begin{aligned} f(x,0,0) &= x(2 - x^2 + 4x^4 + \cdots) \\ f(0,y,0) &= y^4(3 + y + 6y^6 + \cdots) \\ f(0,0,z) &= z^6(5 + 7z^4 - z^5 + \cdots). \end{aligned}$$

Thus f is x-general of order 1, y-general of order 4, and z-general of order 6.

Example 49.10. Suppose that f is x_n-general of order m and $u \in \Bbbk[\![\boldsymbol{x}]\!]$ is a unit. Then uf is also x_n-general of order m. Indeed, if $f = \sum_{i=0}^{\infty} a_i x_n^i$ and $u = \sum_{i=0}^{\infty} b_i x_n^i$ where $a_i, b_i \in \Bbbk[\![x_1, \dots, x_{n-1}]\!]$, then $uf = \sum_{j=0}^{\infty} c_j x_n^j$ where $c_j = \sum_{i=0}^{j} b_i a_{j-i}$. It is straightforward to check that $c_0, c_1, \dots, c_{m-1} \in \langle x_1, \dots, x_{n-1} \rangle$ and c_m is a unit.

Lemma 49.5. *Let $f \in \Bbbk[\![\boldsymbol{x}]\!]$ and express it as $f = \sum_{i \geq m} f_i$ where f_i is homogeneous of degree i and where $f_m \neq 0$. Assume that there exists $\boldsymbol{a} = (a_1, \dots, a_{n-1}) \in \Bbbk^{n-1}$ such that $f_m(\boldsymbol{a}, 1) \neq 0$. Then*

$$f_m(\boldsymbol{x} + \boldsymbol{a}x_n, x_n) = f_m(x_1 + a_1x_n, \dots, x_{n-1} + a_{n-1}x_n, x_n)$$

is x_n-general of order m.

Remark 70. If $\Bbbk$ is infinite, then such an $\boldsymbol{a}$ always exists. On the other hand, if $\Bbbk$ is finite, and $f_m(\boldsymbol{a}, 1) = 0$ for all $\boldsymbol{a} \in \Bbbk^{n-1}$, then one can use the transformation $x_i \mapsto x_i + x_n^{\alpha_i}$ and $x_n \mapsto x_n$ for suitable $\alpha_1, \dots, \alpha_{n-1}$ to obtain an x_n-general power series $f(x_1 + x_n^{\alpha_1}, \dots, x_{n-1} + x_n^{\alpha_{n-1}}, x_n)$.

Proof. We have

$$f_m(\boldsymbol{x} + \boldsymbol{a}x_n, x_n) = f_m(\boldsymbol{a}, 1)x_n^m + \text{terms of lower degree with respect to } x_n$$

because of Taylor's formula. On the other hand, $f_i(\boldsymbol{x} + \boldsymbol{a}x_n, x_n)$ are homogeneous polynomials of degree i. This implies $f(\boldsymbol{x} + \boldsymbol{a}x_n, x_n)$ is x_n-general of order m. □

Theorem 49.6. *(Weierstrass Division Theorem) Let $f, g \in \Bbbk[\![\boldsymbol{x}]\!]$ such that f is x_n-general of order m. Then there exists uniquely determined $q \in \Bbbk[\![\boldsymbol{x}]\!]$ and $r_0, \dots, r_{m-1} \in \Bbbk[\![x_1, \dots, x_{n-1}]\!]$ such that*

$$g = qf + r, \quad \text{with } r = \sum_{i=0}^{m-1} r_i x_n^i.$$

Proof. We define two $\Bbbk[\![x_1, \dots, x_{n-1}]\!]$-linear maps $\rho, \eta \colon \Bbbk[\![\boldsymbol{x}]\!] \to \Bbbk[\![\boldsymbol{x}]\!]$. Let $p = \sum_{i=0}^{\infty} a_i x_n^i$ where $a_i \in \Bbbk[\![x_1, \dots, x_{n-1}]\!]$. Then

$$\rho(p) = \sum_{i=0}^{m-1} a_i x_n^i \quad \text{and} \quad \eta(p) = \frac{p - \rho(p)}{x_n^m} = \sum_{i=0}^{\infty} a_{m+i} x_n^i.$$

To prove the theorem, we just need to find $q \in \Bbbk[\![\boldsymbol{x}]\!]$ such that $\eta(g) = \eta(qf)$. Indeed, in this case we'd have $g - qf \in \ker \eta$ which implies $r := \rho(g - qf) = g - qf$ would give us the required decomposition. Note that $\eta(f)$ is a unit since f is x_n-general of order m. Now observe that

$$\begin{aligned} \eta(g) &= \eta(qf) \\ &= \eta(q\rho(f) + q\eta(f)x_n^m) \\ &= \eta(q\rho(f)) + q\eta(f), \end{aligned}$$

where we used the fact that $\rho(q\eta(f)x_n^m) = 0$. To this end, let $v = q\eta(f)$, let $w = -\rho(f)/\eta(f)$, and let $u = \eta(g)$. Then it is sufficient to find v such that

$$v = u + \eta(vw) = u + H(v),$$

where we set $H(p) := \eta(pw)$. By assumption we have $w \in \langle x_1, \dots, x_{n-1} \rangle \subseteq \Bbbk[\![\boldsymbol{x}]\!]$, thus if $p \in \langle x_1, \dots, x_{n-1} \rangle^i$ then $H(p) \in \langle x_1, \dots, x_{n-1} \rangle^{i+1}$. Now we can iterate

$$\begin{aligned} v &= u + H(v) \\ &= u + H(u + H(v)) \\ &= u + H(u) + H^2(v) \\ &\vdots \\ &= u + H(u) + H^2(u) + \cdots + H^k(u) + H^{k+1}(v) \end{aligned}$$

We just saw that $H^i(u) \in \langle x_1, \dots, x_{n-1} \rangle^i$ and $H^{k+1}(v) \in \langle x_1, \dots, x_{n-1} \rangle^{k+1}$. Therefore $v := \sum_{i=0}^{\infty} H^i(u)$ converges and satisfies the equation $v = u + H(v)$, and is therefore uniquely determined by this property. □

Definition 49.10. A **Weierstrass polynomial** is a polynomial in x_n of the form $w = x_n^m + \sum_{i=0}^{m-1} a_i x_n^i$ where $a_i \in \Bbbk[\![x_1,\dots,x_{n-1}]\!]$ such that $a_i \in \langle x_1,\dots,x_{n-1}\rangle$ for all $0 \le i \le m-1$.

Corollary 41. *Let $f \in \Bbbk[\![\boldsymbol{x}]\!]$ be x_n-general of order m. Then there exists a unit $u \in \Bbbk[\![\boldsymbol{x}]\!]$ and a Weierstrass polynomial w of degree m with respect to x_n such that $f = uw$. Furthermore, u and w are uniquely determined.*

Proof. By Theorem (49.6), there exists q, q', r, r' such that $x_n^m = qf + r$ and $f = q'x_n^m + r'$. In particular, note that

$$\begin{aligned} x_n^m &= qf + r \\ &= q(q'x_n^m + r') + r \\ &= qq'x_n^m + r + r' \end{aligned}$$

implies q is a unit whose inverse is $q' = 1/q$. Therefore we have

$$f = q'(x_n^m - r) = up$$

where we set $u = q'$ and $w = x_n^m - r$. □

Corollary 42. *Let $f \in \Bbbk[\![\boldsymbol{x}]\!]$ be x_n-general of order m. Then $\Bbbk[\![\boldsymbol{x}]\!]/f$ is a free $\Bbbk[\![x_1,\dots,x_{n-1}]\!]$-module of rank m.*

Proof. The Weierstrass Division Theorem implies that $\Bbbk[\![\boldsymbol{x}]\!]/f$ is a finitely generated $\Bbbk[\![x_1,\dots,x_{n-1}]\!]$-module generated by $1, x_n, \dots, x_n^{m-1}$. The uniqueness of the division implies this is also a basis. □

Corollary 43. *Let $\Bbbk$ be a field. Then $\Bbbk[\![\boldsymbol{x}]\!] = \Bbbk[\![x_1,\dots,x_n]\!]$ is noetherian.*

Proof. We prove by induction on n. Suppose I is a nonzero ideal of $\Bbbk[\![x_1]\!]$. Choose $f \in I$ such that $f \neq 0$ and $m = \operatorname{ord} f$ is minimal. Then $f = x_1^m u$ where u is a unit. Obviously we have $I = \langle x_1^m\rangle$ in this case. Now assume $\Bbbk[\![x_1,\dots,x_{n-1}]\!]$ is noetherian and let I be a nonzero ideal of $\Bbbk[\![\boldsymbol{x}]\!]$ and let f be a nonzero element of I. By using Lemma (49.5) if necessary, we may assume that f is x_n-general. By the induction assumption, $\Bbbk[\![x_1,\dots,x_{n-1}]\!]$ is noetherian, and hence $\Bbbk[\![x_1,\dots,x_{n-1}]\!][x_n]$ is noetherian. Therefore $\widetilde{I} := I \cap \Bbbk[\![x_1,\dots,x_{n-1}]\!][x_n]$ is finitely generated, say $\widetilde{I} = \langle f_1,\dots,f_m\rangle$. We claim that $I = \langle f, f_1,\dots,f_m\rangle$. Indeed, let $g \in I$, then using the Weierstrass Division Theorem, we can write $g = qf + r$ with $r \in \widetilde{I} = \langle f_1,\dots,f_m\rangle$. □

Corollary 44. *Let $\boldsymbol{y} = y_1,\dots,y_m$ and let M be a finitely generated $\Bbbk[\![\boldsymbol{x},\boldsymbol{y}]\!]$-module. If $\dim_{\Bbbk}(M/\boldsymbol{x}M) < 0$, then M is a finitely generated $\Bbbk[\![\boldsymbol{x}]\!]$-module.*

Proof. We prove this by induction on m. First we consider the case $m = 1$. As $M/\boldsymbol{x}M$ is a finite dimensional $\Bbbk$-vector space, it follows from the Cayley-Hamiltonian theorem applied to the multiplication by y_1 map that $M/\boldsymbol{x}M \xrightarrow{y_1} M/\boldsymbol{x}M$, for suitable $c_i \in \Bbbk$ and $k \ge 1$ we have

$$f := y_1^k + c_{k-1}y_1^{k-1} + \cdots + c_1 y_1 + c_0 \in \operatorname{Ann}(M/\boldsymbol{x}M).$$

This implies $fM \subseteq \boldsymbol{x}M$, so applying again the Cayley-Hamiltonian theorem to the $\Bbbk[\![\boldsymbol{x}, y_1]\!]$-linear multiplication by f map $M \xrightarrow{f} M$, we obtain

$$g := f^l + h_{l-1}f^{l-1} + \cdots + h_1 f + h_0 \in \operatorname{Ann} M,$$

for suitable $h_i \in \langle \boldsymbol{x}, y_1\rangle^{l-i}$ and $l \ge 1$. Therefore M is a finitely generated $(\Bbbk[\![\boldsymbol{x}, y_1]\!]/g)$-module. By construction, g is y_1-general, so $\Bbbk[\![\boldsymbol{x}, y_1]\!]/g$ is finite over $\Bbbk[\![\boldsymbol{x}]\!]$. This implies that M is a finitely generated $\Bbbk[\![\boldsymbol{x}]\!]$-module.

Now assume the corollary is true for $m-1$ where $m \ge 2$. Note that $\dim_{\Bbbk}(M/\boldsymbol{x}M) < \infty$ implies $\dim_{\Bbbk}(M/\langle \boldsymbol{x}, y_1,\dots,y_{m-1}\rangle M) < 0$. Thus by the $m = 1$ case, we conclude that M is a finitely generated $\Bbbk[\![\boldsymbol{x}, y_1,\dots,y_{m-1}]\!]$-module. Then by induction we conclude that M is a finitely generated $\Bbbk[\![\boldsymbol{x}]\!]$-module. □

Remark 71. Note this corollary isn't true if we replace the power series rings with usual polynomial rings. For instance, consider $M = \Bbbk[x,y]/I$ where $I = \langle x^2 - x, xy - y\rangle$. Then $M/xM = \Bbbk$ which obviously has finite $\Bbbk$-dimension, however M is not a finitely generated $\Bbbk[x]$-module. Indeed, if it were, then $M/\langle x-1\rangle \simeq \Bbbk[y]$ would be a finite-dimensional vector space over $\Bbbk \simeq \Bbbk[x]/\langle x-1\rangle$, which it clearly isn't.

Definition 49.11. An **analytic** $\Bbbk$-algebra A is a $\Bbbk$-algebra of the form $A = \Bbbk[\![\boldsymbol{x}]\!]/I$.

Corollary 45. *Let A and B be analytic $\Bbbk$-algebras and let $\varphi\colon A \to B$ be a morphism of local rings (so $\varphi\mathfrak{m} \subseteq \mathfrak{n}$ where $\mathfrak{m}$ is the maximal ideal of A and $\mathfrak{n}$ is the maximal ideal of B). Then B is finite over A if and only if the fiber of B over $\mathfrak{m}$ is finite over $\Bbbk$ (i.e. if and only if $\dim_{\Bbbk}(B/(\varphi\mathfrak{m})B) < \infty$).*

Proof. One implication is trivial. For the second, assume the fiber of B over $\mathfrak{m}$ is finite. Write $A = \Bbbk[\![\boldsymbol{x}]\!]/I = \Bbbk[\![x_1,\dots,x_n]\!]/I$ and $B = \Bbbk[\![\boldsymbol{y}]\!]/J = \Bbbk[\![y_1,\dots,y_m]\!]/J$. Then B is a finitely generated $\Bbbk[\![\boldsymbol{x},\boldsymbol{y}]\!]$-module where the module structure is defined via φ; given $b \in B$, we have $x_j b = \varphi(\overline{x}_j)b$ and $y_i b = \overline{y}_i b$. Furthermore, we have $B/\boldsymbol{x}B = B/\varphi(\mathfrak{m})B$. Now the statement is a consequence of Corollary (44) □

49.6.1 Implicit and Inverse Function Theorem

In this subsubsection, we want to explain how power series rings satisfy analogs of the implicit and inverse function theorem. First, let us recall the usual implicit function theorem: let $F\colon \mathbb{R}^{n+m} \to \mathbb{R}^m$ be a continuously differentiable function, let $(\boldsymbol{a}, \boldsymbol{b}) = (a_1, \dots, a_n, b_1, \dots, b_m)$ be a point in zero set $\mathrm{V}(F) = \{p \in \mathbb{R}^{n+m} \mid f(p) = 0\}$. Recall that the Jacobian of F at $(\boldsymbol{a}, \boldsymbol{b})$ is given by the matrix

$$\mathrm{J}_F(\boldsymbol{a},\boldsymbol{b}) = \begin{pmatrix}\mathrm{J}_{F,\boldsymbol{x}}(\boldsymbol{a},\boldsymbol{b}) & \mathrm{J}_{F,\boldsymbol{y}}(\boldsymbol{a},\boldsymbol{b})\end{pmatrix} = \begin{pmatrix} \partial_{x_1} F_1(\boldsymbol{a},\boldsymbol{b}) & \cdots & \partial_{x_n} F_1(\boldsymbol{a},\boldsymbol{b}) & \partial_{y_1} F_1(\boldsymbol{a},\boldsymbol{b}) & \cdots & \partial_{y_m} F_1(\boldsymbol{a},\boldsymbol{b}) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \partial_{x_1} F_m(\boldsymbol{a},\boldsymbol{b}) & \cdots & \partial_{x_n} F_m(\boldsymbol{a},\boldsymbol{b}) & \partial_{y_1} F_m(\boldsymbol{a},\boldsymbol{b}) & \cdots & \partial_{y_m} F_m(\boldsymbol{a},\boldsymbol{b}) \end{pmatrix}$$

The implicit function theorem states that if $\mathrm{J}_{F,\boldsymbol{y}}(\boldsymbol{a}, \boldsymbol{b})$ is invertible (i.e. its determinant is nonzero), then there exists an open neighborhood $U \subseteq \mathbb{R}^n$ of $\boldsymbol{a}$ and a unique function $g\colon U \to \mathbb{R}^m$ (which is necessarily continuously differentiable) such that $g(\boldsymbol{a}) = \boldsymbol{b}$ and $(\boldsymbol{x}, g(\boldsymbol{x})) \in \mathrm{V}(F)$ for all $\boldsymbol{x} \in U$. In other words, locally we can express $\mathrm{V}(F)$ as a graph of another function. Furthermore, the Jacobian of g is given by

$$\mathrm{J}_g(\boldsymbol{x}) = -\mathrm{J}_{F,\boldsymbol{y}}(\boldsymbol{x}, g(\boldsymbol{x}))^{-1} \mathrm{J}_{F,\boldsymbol{x}}(\boldsymbol{x}, g(\boldsymbol{x}))$$

Example 49.11. Let $F\colon \mathbb{R}^3 \to \mathbb{R}^2$ be given by

$$\begin{aligned} F(x, y_1, y_2) &= F(x, \boldsymbol{y}) \\ &= (F_1(x, \boldsymbol{y}), F_2(x, \boldsymbol{y})) \\ &= (x^2 + y_1 y_2, x^2 - y_1 + y_2). \end{aligned}$$

The determinant of the Jacobian $\mathrm{J}_{F,\boldsymbol{y}}$ is given by

$$\begin{aligned} \Delta_{F,\boldsymbol{y}} &:= |\mathrm{J}_{F,\boldsymbol{y}}| \\ &= \left| \begin{pmatrix} y_2 & y_1 \\ -1 & 1 \end{pmatrix} \right| \\ &= y_2 + y_1. \end{aligned}$$

Now let $a = 3$ and let $(a, \pm\boldsymbol{b}) = (6, 36 \pm 6\sqrt{32}, -36 \pm 6\sqrt{32})$. Clearly we have $\Delta_{F,\boldsymbol{y}}(a, \pm\boldsymbol{b}) \neq 0$. Locally around $(a, \pm\boldsymbol{b})$, we can implicitly write:

$$y_1 \;=\; \frac{1}{2}\left(x^2 \pm x\sqrt{x^2 - 4}\right) \quad \text{and} \quad y_2 = \frac{1}{2}\left(-x^2 \pm x\sqrt{x^2 - 4}\right).$$

Theorem 49.7. *(Implicit Function Theorem) Let $\mathbb{k}$ be a field and let $F \in \mathbb{k}[\![\boldsymbol{x}, y]\!] = \mathbb{k}[\![x_1, \dots, x_n, y]\!]$ such that $F(\boldsymbol{x}, 0) \in \langle \boldsymbol{x} \rangle$ and $\partial_y F(\boldsymbol{x}, 0) \notin \langle \boldsymbol{x} \rangle$. Then there exists a unique $g \in \langle \boldsymbol{x} \rangle \mathbb{k}[\![\boldsymbol{x}]\!]$ such that $F(\boldsymbol{x}, g(\boldsymbol{x})) = 0$.*

Theorem 49.8. *(Implicit Function Theorem) Let $F \in \mathbb{k}[\![\boldsymbol{x}, y]\!] = \mathbb{k}[\![x_1, \dots, x_n, y]\!]$ such that $\mathfrak{m} \in \mathrm{V}(F) \cap \mathrm{D}(\partial_y F)$ where $\mathfrak{m} = \langle \boldsymbol{x}, y \rangle$ (i.e. such that $F \in \mathfrak{m}$ and $\partial_y F \notin \mathfrak{m}$). Then there exists a unique $g \in \langle \boldsymbol{x} \rangle \mathbb{k}[\![\boldsymbol{x}]\!]$ such that $\mathrm{V}(F) \subseteq \langle \boldsymbol{x}, y - g \rangle$. $F(\boldsymbol{x}, g(\boldsymbol{x})) = 0$.*

Proof. The conditions $F(\boldsymbol{x}, 0) \in \langle \boldsymbol{x} \rangle$ and $\partial_y F(\boldsymbol{x}, 0) \notin \langle \boldsymbol{x} \rangle$ says that F has the form

$$F(\boldsymbol{0}, y) = cy + \text{higher terms in } y,$$

with $c \neq 0$, that is, F is y-general of order 1. Thus the Weierstrass Preparation Theorem implies that $F = u(y - g)$ where $g \in \mathbb{k}[\![\boldsymbol{x}]\!]$ and $u \in \mathbb{k}[\![\boldsymbol{x}, y]\!]$ is a unit. □

Theorem 49.9. *(Inverse Function Theorem) Let $\mathbb{k}$ be a field and let $\boldsymbol{f} = f_1, \dots, f_n \in \mathbb{k}[\![\boldsymbol{x}]\!]$ such that $f_1(\boldsymbol{0}) = \cdots = f_n(\boldsymbol{0}) = 0$. Then the $\mathbb{k}$-algebra homomorphism $\varphi\colon \mathbb{k}[\![\boldsymbol{x}]\!] \to \mathbb{k}[\![\boldsymbol{x}]\!]$ defined by $\varphi(x_i) = f_i$ is an isomorphism if and only if $\det \mathrm{J}_{\boldsymbol{f}}(\boldsymbol{0}) \neq 0$.*

Remark 72. The condition that $f_1(\boldsymbol{0}) = \cdots = f_n(\boldsymbol{0}) = 0$ is equivalent to saying $f_1, \dots, f_n \in \mathfrak{m}$ where $\mathfrak{m} = \langle \boldsymbol{x} \rangle$. The condition that $\det \mathrm{J}_{\boldsymbol{f}}(\boldsymbol{0}) \neq 0$ is equivalent to saying $\Delta_{\boldsymbol{f}} \notin \mathfrak{m}$ where $\Delta_{\boldsymbol{f}} = \det((\partial_{x_j} f_i))$.

Let $R = \mathbb{k}[\![\alpha, t]\!]$ and let $f \in R$ be given by $f = \alpha^2 + 3t\alpha + 1$. Then f is a unit in R, thus $R/f = 0$.

49.7 Maps from Power Series Rings

Let R be a ring. Recall that R-algebra homomorphims from the polynomial ring $R[\boldsymbol{x}] = R[x_1, \dots, x_n]$ to an R-algebra A are uniquely determined by where they send the x_i. The power series ring has a similar property, but only in the case where A is complete.

Theorem 49.10. *Assume that A is complete with respect to an ideal $\mathfrak{a}$ and let $\boldsymbol{f} = f_1, \dots, f_n$ be a sequence of elements in $\mathfrak{a}$.*

1. *There is a unique R-algebra homomorphism $\varphi\colon R[\![\boldsymbol{x}]\!] \to A$ sending x_i to f_i for each i and taking convergent sequences to convergent sequences. This map takes a power series $g(\boldsymbol{x})$ to $g(\boldsymbol{f})$.*

2. *If the induced map $\varphi\colon R[\![\boldsymbol{x}]\!] \to A/\mathfrak{a}$ is an epimorphism and $\langle \boldsymbol{f} \rangle = \mathfrak{a}$, then φ is an epimorphism.*

Proof. 1. The unique R-algebra map $R[\boldsymbol{x}] \to A/\mathfrak{a}^k$ sending x_i to the class of f_i factors through

$$R[\![\boldsymbol{x}]\!]/\langle \boldsymbol{x} \rangle^k = R[\boldsymbol{x}]/\langle \boldsymbol{x} \rangle^k \to A/\mathfrak{a}^k$$

and thus induces unique maps $R[\![\boldsymbol{x}]\!] \to A/\mathfrak{a}^k$ sending x_i to the class of f_i. Since A is the inverse limit of the $A/\mathfrak{a}^k$, there is a unique map $\varphi\colon R[\![\boldsymbol{x}]\!] \to A$ sending x_i to f_i, as required. The image of $g + \langle \boldsymbol{x} \rangle^k$ in $A/\mathfrak{a}^k$ is $g(\boldsymbol{f}) + \mathfrak{a}^k$ for every k, so the image of g in A is $g(\boldsymbol{f})$, which makes sense precisely because A is complete with respect to $\mathfrak{a}$.

2. It follows from our hypothesis that the map $\langle \boldsymbol{x} \rangle / \langle \boldsymbol{x} \rangle^2 \to \mathfrak{a}/\mathfrak{a}^2$ is surjective, hence the induced map $\operatorname{gr}\varphi\colon \operatorname{gr}_{\boldsymbol{x}} R \to \operatorname{gr}_{\mathfrak{a}} A$ is also surjective. Now let g be a nonzero element in A and let k be the largest number such that $g \in \mathfrak{a}^k$ (note that since A is complete we have $\bigcap_k \mathfrak{a}^k = 0$). Since $\operatorname{gr}\varphi$ is a surjection we may find a $g_1 \in \langle \boldsymbol{x} \rangle^k$ whose initial form is carred to the initial form of g. It follows that $g - \varphi(g_1) \in \mathfrak{a}^{k+1}$. Iterating this process, we obtain a sequence of elements $g_l \in \langle \boldsymbol{x} \rangle^{k+l-1}$ such that $g = \sum_{l=1}^{\infty} g_l$. Because φ preserves infinite sums, this yields $g = \varphi(\sum_{l=1}^{\infty} g_l)$, and we are done.

□

50 Modules of Finite Length

Let M be an R-module. A **chain of R-submodules** $\mathcal{M}$ of M, or **R-chain** for short, is a strictly descending finite sequence of R-submodules of M of the form

$$\mathcal{M} := (M = M_0 \supset M_1 \supset \cdots \supset M_i \supset M_{i+1} \supset \cdots \supset M_n = 0).$$

In this case, we say the chain $\mathcal{M}$ has **length** n and we denote this by $\operatorname{length}(\mathcal{M}) = n$. We set $\mathrm{C}_R(M)$ to be the set of all chains R-chains of M. The **length** of M is defined to be the supremum of the lengths of all R-chains of M:

$$\ell_R(M) := \sup\{\operatorname{length}(\mathcal{M}) \mid \mathcal{M} \in \mathrm{C}_R(M)\}.$$

Definition 50.1. Let A be a ring and let M be an A-module.

1. Let $\mathcal{C}(M)$ denote the set of all **chains of submodules** of M, that is,

$$\mathcal{C}(M) := \{\mathcal{M} = (M = M_0 \supset M_1 \supset \cdots \supset M_n = 0) \mid M_i \neq M_{i+1}\}.$$

2. If $\mathcal{M} = (M = M_0 \supset M_1 \supset \cdots \supset M_n = 0) \in \mathcal{C}(M)$, then $\operatorname{length}(\mathcal{M}) = n$.

3. If $\operatorname{length}(M) < \infty$, then we say M is **Artinian**. If A is Artinian as an A-module, then we say A is an **Artinian ring**.

Remark 73. The set $\mathcal{C}(M)$ forms a poset in the following way: Given $\mathcal{M}, \mathcal{M}' \in \mathcal{C}(M)$, we say $\mathcal{M}' \geq \mathcal{M}$ if we can obtain $\mathcal{M}$ by removing some submodules in the chain $\mathcal{M}'$.

Definition 50.2. Let A be a ring, M an A-module, and $\mathcal{M} := (M = M_0 \supset M_1 \supset \cdots \supset M_n = 0)$ a chain of submodules of M.

1. We say $\mathcal{M}$ is a **composition series** for M if M_i/M_{i+1} is a nonzero simple module for each i.

2. We define the **length** of M, denoted $\operatorname{length}(M)$, to be the least length of a composition series for M.

Remark 74.

1. If $\mathcal{M}$ is not a composition series, then there exists some i such that M_i/M_{i+1} is not simple. Thus, there exists a nonzero proper submodule M'/M_{i+1} of M_i/M_{i+1}. Let $\mathcal{M}'$ be the chain of submodules of M given by $\mathcal{M}' = (M = M_0 \cdots \supset M_i \supset M' \supset M_{i+1} \supset \cdots \supset M_n = 0)$. Then $\mathcal{M}' \geq \mathcal{M}$ and $\text{length}(\mathcal{M}') = \text{length}(\mathcal{M}) + 1$. So a composition series must be maximal with respect to the partial order.

2. A simple module must be generated by any nonzero element. Thus, if $\mathcal{M}$ is a composition series, then each $M_i/M_{i+1} \cong A/\mathfrak{p}$ for some maximal ideal $\mathfrak{p}$, which may be described by $\mathfrak{p} = \text{Ann}\,(M_i/M_{i+1})$.

Theorem 50.1. *Let A be a ring, and let M be an A-module. Then M has a finite composition series if and only if M is Artinian and Noetherian. If M has a finite composition series $\mathcal{M} := (M = M_0 \supset M_1 \supset \cdots \supset M_n = 0)$ of length n, then:*

1. *Every chain of submodules of M has length less than or equal to n, and can be refined to a composition series.*

2. *The sum of the localization maps $M \to M_{\mathfrak{p}}$, for $\mathfrak{p}$ a prime ideal, gives an isomorphism of A-modules*

$$M \cong \bigoplus_{\mathfrak{p}} M_{\mathfrak{p}},$$

where the sum is taken over all maximal ideals $\mathfrak{p}$ such that some $M_i/M_{i+1} \cong A/\mathfrak{p}$. The number of M_i/M_{i+1} isomorphic to $A/\mathfrak{p}$ is the length of $M_{\mathfrak{p}}$ as an $A_{\mathfrak{p}}$-module, and is thus independent of the composition series chosen.

3. *We have $M = M_{\mathfrak{p}}$ if and only if M is annihilated by some power of $\mathfrak{p}$.*

Proof. First suppose that M is Artinian and Noetherian, so that it satisfies both ascending chain condition and descending chain condition on submodules. By the ascending chain condition we may choose a maximal proper submodule M_1, a maximal proper submodule M_2 of M_1, and so on. By the descending chain condition this sequence of submodules must terminate, and it can only terminate when some $M_n = 0$. In this case, $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$ is a compostion series for M.

1. Suppose $N \subset M$ is a proper submodule. We shall show that $\text{length}(N) < \text{length}(M)$. The idea is simple: We intersect the terms of the given composition series for M with N and derive a shorter composition series for N. The quotient $(N \cap M_i)/(N \cap M_{i+1})$ is isomorphic to

$$(N \cap M_i + M_{i+1})/M_{i+1} \subset M_i/M_{i+1}.$$

Since M_i/M_{i+1} is simple, we have either $(N \cap M_i)/(N \cap M_{i+1}) = 0$ or else $(N \cap M_i)/(N \cap M_{i+1})$ is simple and $N \cap M_i + M_{i+1} = M_i$. We claim that the latter possibility cannot happen for every i. Assuming on the contrary that it did, we prove by descending induction on i that $N \supset M_i$ for every i, and we get a contradiction from the statement $N \supset M_0 = M$. If $i = n$, then clearly $N \supset M_i$. Supposing by induction that $N \supset M_{i+1}$, we see that $N \cap M_i = N \cap M_i + M_{i+1} = M_i$, and it follows that $N \supset M_i$. From these facts, we see that the sequence of submodules

$$N \supset N \cap M_1 \supset \cdots \supset N \cap M_n = 0$$

can be changed, by leaving out the terms $N \cap M_i$ such that $N \cap M_i = N \cap M_{i+1}$, to a composition series for N whose length is less than n. Since we could do this for any composition series for M, we get

$$\text{length}(N) < \text{length}(M).$$

Suppose now that $M = N_0 \supset N_1 \supset \cdots \supset N_k$ is a chain of submodules. We shall show by induction on $\text{length}(M)$ that $k \leq \text{length}(M)$. This is obvious if $\text{length}(M) = 0$, since then $M = 0$. By the argument above, $\text{length}(N_1) < \text{length}(M)$; so by induction, the length of the chain $N_1 \supset \cdots \supset N_k$ is $k - 1 \leq \text{length}(N_1)$. Since $\text{length}(N_1) < \text{length}(M)$, it follows that $k \leq \text{length}(M)$. From the definition of length, it now follows that every maximal chain of submodules has length n, and every chain of submodules can be refined to a maximal chain. Further, n is a uniform bound on the lengths of all ascending or descending chains of submodules, so that M has both ascending chain condition and descending chain condition.

2. It suffices to show that the given map becomes an isomorphism after localizing at any maximal ideal $\mathfrak{q}$ of A. This will be easy once we understand what happens when we localize a module of finite length. We begin with the case when M has length 1, that is, when M is a simple module. In this case, $M \cong A/\mathfrak{p}$ for some maximal ideal $\mathfrak{p} = \text{Ann}(M)$. If $\mathfrak{p} = \mathfrak{q}$, then since $A/\mathfrak{q}$ is a field, the elements outside of $\mathfrak{q}$ acts as units

on $A/\mathfrak{q}$, and we see that $(A/\mathfrak{q})_\mathfrak{q} = A/\mathfrak{q}$. If on the other hand $\mathfrak{p} \neq \mathfrak{q}$, then since $\mathfrak{p}$ is maximal, $\mathfrak{p} \not\subset \mathfrak{q}$, so $\mathfrak{p}_\mathfrak{q} = A_\mathfrak{q}$. Thus

$$(A/\mathfrak{p})_\mathfrak{q} = A_\mathfrak{q}/\mathfrak{p}_\mathfrak{q} = 0.$$

It follows in particular from this that if $\mathfrak{q}$ and $\mathfrak{q}'$ are distinct prime ideals, then $(M_\mathfrak{q})_{\mathfrak{q}'} = 0$. We now return to the general case, where $\mathrm{length}(M) = n < \infty$. The composition series for M localizes to a sequence of submodules

$$M_\mathfrak{q} = (M_0)_\mathfrak{q} \supset (M_1)_\mathfrak{q} \supset \cdots \supset (M_n)_\mathfrak{q} = 0.$$

The modules M_i/M_{i+1} have length 1, so the case already treated shows that $(M_i/M_{i+1})_\mathfrak{q} = M_i/M_{i+1}$ if $\mathfrak{q} = \mathrm{Ann}\,(M_i/M_{i+1})$ and $(M_i/M_{i+1})_\mathfrak{q} = 0$ otherwise. Thus $M_\mathfrak{q}$ has a finite composition series corresponding to the subseries of the one for M, obtained by keeping only those $(M_i)_\mathfrak{q}$ such that $M_i/M_{i+1} \cong A/\mathfrak{q}$. In particular, if none of the modules M_i/M_{i+1} is isomorphic to $A/\mathfrak{q}$, then $M_\mathfrak{q} = 0$; and if $\mathfrak{q}$ and $\mathfrak{q}'$ are distinct maximal ideals, then $(M_\mathfrak{q})_{\mathfrak{q}'} = 0$. Now consider the map

$$\alpha : M \to \bigoplus_{\mathfrak{p}} M_\mathfrak{p},$$

where the sum is taken over all maximal ideals $\mathfrak{p}$ such that some $M_i/M_{i+1} \cong A/\mathfrak{p}$. We see from the above that we could harmlessly extend the sum to all maximal ideals; the new terms are all 0. For any maximal ideal $\mathfrak{q}$ and any module M, we have $(M_\mathfrak{q})_\mathfrak{q} = M_\mathfrak{q}$, so the identity map is one part of the localization of α:

$$\alpha_\mathfrak{q} : M_\mathfrak{q} \to \left(\bigoplus_{\mathfrak{p} \in \mathrm{Max}(A)} M_\mathfrak{p} \right)_\mathfrak{q} = \bigoplus_{\mathfrak{p} \in \mathrm{Max}(A)} (M_\mathfrak{p})_\mathfrak{q}.$$

But if $\mathfrak{p} \neq \mathfrak{q}$ and M has finite length, then we have seen that $(M_\mathfrak{p})_\mathfrak{q} = 0$. Thus $\alpha_\mathfrak{q}$ is the identity map for every maximal ideal $\mathfrak{q}$, and it follows that α is an isomorpism.

3. Suppose that M is annihilated by a power of a maximal ideal $\mathfrak{p}$. If $\mathfrak{q} \neq \mathfrak{p}$ is another maximal ideal, then $\mathfrak{p}$ contains an element not in $\mathfrak{q}$. This element acts as a unit on $M_\mathfrak{q}$. Thus, by part 2, $M \cong M_\mathfrak{p}$. Conversely suppose that $M \cong M_\mathfrak{p}$. The preceeding description of localization shows that every factor $M_i/M_{i+1} \cong A/\mathfrak{p}$. By induction, we see that $\mathfrak{p}^d M \subset M_d$, and in particular $\mathfrak{p}^n M = 0$.

∎

Example 50.1. Let $A = K[x,y]$, $I = \langle x^3, x^2y, xy^2, y^3 \rangle$, and $M = A/I$. We want to calculate the length of M. By Theorem (50.1, it suffices to find a composition series for M and calculate its length. A composition series for M is given by

$$0 = M_6 \subset M_5 \subset M_4 \subset M_3 \subset M_2 \subset M_1 \subset M_0 = M,$$

where

$$\begin{aligned} M_5 &= \langle x^2, xy^2, y^3 \rangle / I \\ M_4 &= \langle x^2, y^2 \rangle / I \\ M_3 &= \langle x^2, xy, y^2 \rangle / I \\ M_2 &= \langle x, y^2 \rangle / I \\ M_1 &= \langle x, y \rangle / I, \end{aligned}$$

and $M_i/M_{i+1} \cong A/\langle x, y \rangle$ for all i. Thus, $\mathrm{length}(M) = 6$.

Lemma 50.2. *Let $R \to S$ be a ring map and let M be an S-module. Then $\ell_S(M) \leq \ell_R(M)$. If $R \to S$ is surjective, then we have equality.*

Proof. If $\mathcal{M}$ is an S-chain of M, then $\mathcal{M}$ is also an R-chain of M (since each M_i in $\mathcal{M}$ is also an R-module). This shows that $\ell_S(M) \leq \ell_R(M)$. Now assume that $R \to S$ is surjective. Then any R-submodule of M is automatically an S-submodule of M. So in this case, an R-chain of M is also an S-chain of M. This implies $\ell_R(M) \leq \ell_S(M)$ which implies $\ell_R(M) = \ell_S(M)$. ∎

Corollary 46. *Let R be a ring with maximal ideal $\mathfrak{m}$ and let M be an R-module such that $\mathfrak{m}M = 0$. Then the length of M as an R-module agrees with the dimension of M as a $\Bbbk$-vector space where $\Bbbk := R/\mathfrak{m}$.*

Example 50.2. Let $R = \Bbbk[x]/\langle x^2 \rangle = M$ and let $\mathcal{M} = (M \supset \langle x \rangle \supset 0)$. Note that

51 Injective Modules

Definition 51.1. Let E be an R-module. We say E is **injective** if for every injective homorphisms $\varphi\colon M \to N$ and for every homomorphism $\psi\colon M \to E$ there exists a homomorphism $\widetilde{\psi}\colon N \to E$ such that $\widetilde{\psi} \circ \varphi = \psi$. In this case, we say $\widetilde{\psi}$ **extends** ψ **along** φ. If φ is the inclusion map $M \subset N$, then we will simply say $\widetilde{\psi}$ **extends** ψ. We illustrate this with the following diagram:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi"'] & N \arrow[dl, dashed, "\widetilde{\psi}"] \\ E & \end{tikzcd}$$

An equivalent definition of being injective is given in the following proposition:

Proposition 51.1. *Let E be an R-module. Then E is injective if and only if the contravariant functor $\mathrm{Hom}_R(-, E)$ is exact.*

Proof. Suppose that E is injective. Let

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

be an exact sequence of R-modules. Since $\mathrm{Hom}_R(-, E)$ is left exact, we only need to check that

$$\mathrm{Hom}_R(M, E) \xrightarrow{\varphi^*} \mathrm{Hom}_R(M', E) \longrightarrow 0$$

is exact at $\mathrm{Hom}_R(M', E)$. This is equivalent to showing that φ^* is surjective. Let $\lambda \in \mathrm{Hom}_R(M', E)$. Since E is injective, and $\varphi : M' \to M$ is a monomorphism, there exists $\widetilde{\lambda} \in \mathrm{Hom}_R(M', E)$ such that $\varphi^*(\widetilde{\lambda}) = \widetilde{\lambda} \circ \varphi = \lambda$. But $\varphi^*(\widetilde{\lambda}) = \widetilde{\lambda} \circ \varphi$, so φ^* is surjective. In fact, this map is surjective if and only if E is injective by definition. □

Lemma 51.1. *Let E an R-module. The following statements are equivalent:*

1. *E is an injective R-module;*
2. *Every short exact sequence of the form*

$$0 \longrightarrow E \longrightarrow M \longrightarrow N \longrightarrow 0 \tag{163}$$

   splits.

3. *If E is a submodule of an R-module M, then E is a direct summand of M.*

Proof. We first show 2 implies 1. Suppose that any short exact sequence of the form (363) splits. This means, equivalently, that any injective R-linear map out of E splits. Let $\varphi\colon M \to N$ be an injective R-linear map and let $\psi\colon M \to E$ be any R-linear map. We need to construct a map $\widetilde{\psi}\colon N \to E$ such that $\widetilde{\psi}\varphi = \psi$. To do this, consider the pushout module

$$E +_M N = (E \times N)/\{(\psi(u), -\varphi(u)) \mid u \in M\}$$

together its natural maps $\iota_1\colon E \to E +_M N$ and $\iota_2\colon N \to E +_M N$, given by $\iota_1(v) = [v, 0]$ and $\iota_2(w) = [0, w]$ for all $v \in E$ and $w \in N$ where $[v, w]$ denotes the equivalence class in $E +_M N$ with (v, w) as one of its representatives. Observe that

$$\begin{aligned} \iota_1(\psi(u)) &= [\psi(u), 0] \\ &= [0, \varphi(u)] \\ &= \iota_2(\varphi(u)) \end{aligned}$$

for all $u \in M$. Therefore, we have a commutative diagram

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi"'] & N \arrow[d, "\iota_2"] \\ E \arrow[r, "\iota_1"'] & E +_M N \end{tikzcd}$$

We claim that ι_1 is injective. Indeed, suppose $v \in \ker \iota_1$. Then $[v, 0] = 0$ implies if $(v, 0) = (\psi(u), -\varphi(u))$ for some $u \in M$. Then $\varphi(u) = 0$ implies $u = 0$ since φ is injective, and therefore

$$\begin{aligned} v &= \psi(u) \\ &= \psi(0) \\ &= 0. \end{aligned}$$

Thus ι_1 is injective. Therefore by hypothesis the map $\iota_1 \colon E \to E +_M N$ splits, say by $\lambda \colon E +_M N \to E$, where $\lambda\iota_1 = 1_E$. Finally, we obtain a map $\widetilde{\psi} \colon N \to E$ by setting $\widetilde{\psi} := \lambda\iota_2$. Then

$$\begin{aligned} \widetilde{\psi}\varphi &= \lambda\iota_2\varphi \\ &= \lambda\iota_1\psi \\ &= \psi, \end{aligned}$$

shows that $\widetilde{\psi}$ has the desired property.

Now we will show 1 implies 2. Suppose that E is an injective R-module. Let $\varphi \colon E \to M$ be an injective homomorphism. Since E is an injective R-module and since $1_E \colon E \to E$ is an injective R-module homomorphism, there exists an R-linear map $\widetilde{\varphi} \colon M \to E$ such that $\widetilde{\varphi}\varphi = 1_E$. That is, $\widetilde{\varphi}$ splits $\varphi \colon E \to M$.

Now we will show 2 implies 3. Suppose that any short exact sequence of the form (363) splits. Let M be an R-module such that $E \subseteq M$. Then the short exact sequence

$$0 \longrightarrow E \xrightarrow{\iota} M \xrightarrow{\pi} M/E \longrightarrow 0$$

splits, where $\iota \colon E \to M$ denotes the inclusion map and $\pi \colon M \to M/E$ denotes the quotient map. Therefore we may choose a $\widetilde{\pi} \colon M/E \to M$ such that $\pi\widetilde{\pi} = 1_{M/E}$. We claim that

$$M = E \oplus \widetilde{\pi}(M/E).$$

Indeed, they are both submodules of M. Furthermore, observe that we have $E \cap \widetilde{\pi}(M/E) = \{0\}$. Indeed, suppose $u \in E \cap \widetilde{\pi}(M/E)$. Then $u \in E$ implies $\pi(u) = 0$. Also $u \in \widetilde{\pi}(M/E)$ implies $u = \widetilde{\pi}(\overline{v})$ for some $\overline{v} \in M/E$. Therefore

$$\begin{aligned} 0 &= \widetilde{\pi}(0) \\ &= \widetilde{\pi}\pi(u) \\ &= \widetilde{\pi}\pi\widetilde{\pi}(\overline{v}) \\ &= \widetilde{\pi}(\overline{v}) \\ &= u. \end{aligned}$$

Finally, note that if $u \in M$, then we can write

$$u = u - \widetilde{\pi}\pi(u) + \widetilde{\pi}\pi(u),$$

where $\widetilde{\pi}\pi(u) \in \widetilde{\pi}(M/E)$ and where $u - \widetilde{\pi}\pi(u) \in E$ since

$$\begin{aligned} \pi(u - \widetilde{\pi}\pi(u)) &= \pi(u) - \pi\widetilde{\pi}\pi(u) \\ &= \pi(u) - \pi(u) \\ &= 0 \end{aligned}$$

implies $u - \widetilde{\pi}\pi(u) \in \ker \pi = E$. This implies $M = E + \widetilde{\pi}(M/E)$.

Finally we show 3 implies 2. Suppose that E satisfies the property that if E is a submodule of an R-module M, then it must be a direct summand of M. We show that any short exact sequence of the form (363) splits by showing that any injective R-linear map out of E splits.

Step 1: Before we show that any injective R-linear map out of E splits, we need to show that if $\varphi \colon E \to F$ is an isomorphism of R-modules, then F satisfies the same property as E; namely if N is an R-module such that $F \subseteq N$, then F is a direct summand of N. Let $\varphi \colon E \to F$ be an isomorphism, let $\psi \colon F \to E$ denote its inverse, and let N be an R-module such that $F \subseteq N$. We define an R-module $\psi(N)$, where as a set we have

$$\psi(N) = E \cup \{\psi(v) \mid v \in N \backslash F\},$$

where $\psi(v)$ is understood to be a formal symbol if $v \in N \backslash F$ and is understood to be an element in E if $v \in F$. Here, E is *literally* a subset of $\psi(N)$. We extend the R-linear structure on E to an R-linear structure on $\psi(N)$ by defining addition and scalar multiplication by

$$\psi(v_1) + \psi(v_2) = \psi(v_1 + v_2) \quad \text{and} \quad a\psi(v) = \psi(av).$$

for all $v, v_1, v_2 \in N \backslash F$ and $a \in R$. Defining the R-linear structure on $\psi(N)$ in this way makes it so that $\psi \colon F \to E$ and $\varphi \colon E \to F$ extends to an isomorphism $\psi \colon N \to \psi(N)$ with corresponding inverse $\varphi \colon \psi(N) \to N$. With this construction in place, we see that E is *literally* a submodule of $\psi(N)$. Therefore $\psi(N)$ is an internal direct sum, say

$$\psi(N) = E \oplus K,$$

where K is another submodule of $\psi(N)$ such that $E \cap K = \{0\}$ and $E + K = \psi(N)$. Then since $\varphi \colon \psi(N) \to N$ is an isomorphism, we see that

$$\begin{aligned} N &= \varphi(E) \oplus \varphi(K) \\ &= F \oplus \varphi(K). \end{aligned}$$

Thus F satisfies the same property as E.

Step 2: Now we will show that any injective R-linear map out of E splits. Let $\varphi \colon E \to M$ be any injective R-linear map. We claim that $\varphi \colon E \to M$ splits if and only if $\iota \colon \varphi(E) \to M$ splits, where ι denotes the inclusion map. Indeed, denote $\varphi^{-1} \colon E \to \varphi(E)$ to be the inverse of $\varphi \colon E \to \varphi(E)$. If $\varphi \colon E \to M$ splits, then there exists an R-linear map $\widetilde{\varphi} \colon M \to E$ such that $\widetilde{\varphi}\varphi = 1_E$. Then $\varphi\widetilde{\varphi} \colon M \to \varphi(E)$ splits $\iota \colon \varphi(E) \to M$ since

$$\begin{aligned} (\varphi\widetilde{\varphi}\iota)(\varphi(u)) &= \varphi\widetilde{\varphi}(\varphi(u)) \\ &= \varphi(\widetilde{\varphi}\varphi(u)) \\ &= \varphi(u) \end{aligned}$$

for all $\varphi(u) \in \varphi(E)$. Similarly, if $\iota \colon \varphi(E) \to M$ splits, then there exists an R-linear map $\widetilde{\iota} \colon M \to \varphi(E)$ such that $\widetilde{\iota\iota} = 1_{\varphi(E)}$. Then $\varphi^{-1}\widetilde{\iota} \colon M \to E$ splits $\varphi \colon E \to M$ since

$$\begin{aligned} (\varphi^{-1}\widetilde{\iota}\varphi)(u) &= (\varphi^{-1}\widetilde{\iota})(\varphi(u)) \\ &= (\varphi^{-1}\widetilde{\iota})(\iota\varphi(u)) \\ &= (\varphi^{-1}\widetilde{\iota\iota})(\varphi(u)) \\ &= (\varphi^{-1})(\varphi(u)) \\ &= u \end{aligned}$$

for all $u \in E$. Thus to show that $\varphi \colon E \to M$ splits, it suffices to show that $\iota \colon \varphi(E) \to M$ splits. In this case, $\varphi(E)$ is a submodule of M, and by step 1, we see that M is an internal direct sum, say

$$M = \varphi(E) \oplus K$$

for some R-module $K \subseteq M$. The projection map $\pi_1 \colon M \to \varphi(E)$ is easily seen to split the inclusion map $\iota \colon \varphi(E) \to M$. $\square$

51.1 Baer's Criterion

Let E be an R-module. If we want to determine if E is injective, then it turns out that we do not necessarily need to check that the condition in Definition (51.1) holds for *every* injective homomorphism $\varphi \colon M \to N$; we only need to check that it holds for every morphism of the type $I \subset R$ where I is an ideal in R. This is called Baer's Criterion. Before we show this, let us first show that we need only consider inclusions $M \subset N$:

Proposition 51.2. *Let E be an R-module. Then E is injective if and only if for every inclusion of R-modules $M \subset N$ and for every homomorphism $\psi \colon M \to E$ there exists a homomorphism $\widetilde{\psi} \colon N \to E$ such that $\widetilde{\psi}|_M = \psi$.*

Proof. One direction is obvious. To prove the other direction, let $\varphi \colon M \to N$ be an injective homomorphism of R-modules and let $\psi \colon M \to E$ be a homorphism. Since φ is injective, it induces an isomorphism $\varphi \colon M \to \varphi(M)$ of R-modules. Let φ^{-1} be the inverse homomorphism to this isomorphism. Then $\varphi(M) \subset N$ and $\psi \circ \varphi^{-1} \colon \varphi(M) \to E$ is a homomorphism, and so by hypothesis, there exists $\widetilde{\psi} \colon N \to E$ such that $\widetilde{\psi}|_{\varphi(M)} = \psi \circ \varphi^{-1}$. This implies

$$\begin{aligned} \widetilde{\psi} \circ \varphi &= \widetilde{\psi}|_{\varphi(M)} \circ \varphi \\ &= \psi \circ \varphi^{-1} \circ \varphi \\ &= \psi. \end{aligned}$$

Therefore E is injective. $\square$

Now we will state and prove Baer's Criterion:

Theorem 51.2. *(Baer's Criterion) Let E be an R-module. Then E is injective if and only if for every ideal $I \subset R$ and for every homomorphism $\psi\colon I \to E$ there exists a morphism $\widetilde{\psi}\colon R \to E$ such that $\widetilde{\psi}|_I = \psi$.*

Proof. One direction is obvious. For the other direction, let $M \subset N$ be an inclusion of A-modules and let $\psi\colon M \to E$ be a homomorphism. Define the partially ordered set $(\mathscr{F}, \leq)$ where

$$\mathscr{F} := \{\psi'\colon M' \to N \mid M \subset M' \subset N \text{ and } \psi' \text{ extends } \psi\}.$$

and the where partial order $\leq$ is defined by

$$\psi' \leq \psi'' \text{ if and only if } \psi'' \text{ extends } \psi'.$$

If $\mathscr{T}$ is a totally ordered subset of $\mathscr{F}$, then it has an upper bound (namely we take the direct limit of a all $\psi' \in \mathscr{T}$). Therefore by Zorn's lemma, there is a homomorphism $\psi'\colon N' \to E$ with $M \subset N' \subset N$ which is maximal with respect to the property that ψ' extends ψ. We claim that $N' = N$. We will prove this by contradiciton: assume that $N' \neq N$. Choose an element $u \in N \backslash N'$ and consider the ideal

$$I = \{a \in R \mid au \in N'\}.$$

It is a nonempty proper ideal of R since $0 \in I$ and $1 \notin I$. By hypothesis, the composite

$$I \xrightarrow{\cdot u} N' \xrightarrow{\psi'} E$$

extends to a homomorphism $\widetilde{\psi}\colon R \to E$. Define $\psi''\colon N' + Ru \to E$ by the formula

$$\psi''(v + au) = \psi'(v) + \widetilde{\psi}(a)$$

for all $v + au \in N' + Rn$. To see that this is well-defined, suppose $v_1 + a_1u$ and $v_2 + a_2u$ represent the same element in $N' + Ru$. Then $v_2 - v_1 = (a_1 - a_2)u$ implies $a_1 - a_2 \in I$. Therefore $\widetilde{\psi}(a_1 - a_2) = \psi'((a_1 - a_2)u)$, and so

$$\begin{aligned}
\psi''(v_2 + a_2u) &= \psi'(v_2) + \widetilde{\psi}(a_2) \\
&= \psi'(v_2 - (v_2 - v_1))) + \widetilde{\psi}(a_1 + (a_2 - a_1)) \\
&= \psi'(v_2 + (a_1 - a_2)u) + \widetilde{\psi}(a_1 + (a_2 - a_1)) \\
&= \psi'(v_1) + \psi'((a_1 - a_2)u) + \widetilde{\psi}(a_1) + \psi'((a_2 - a_1)u) \\
&= \psi'(v_1) + \widetilde{\psi}(a_1).
\end{aligned}$$

Thus ψ'' is well-defined. We also note that ψ'' extends ψ'. Since ψ' was maximal, this leads to a contradiction. So we must have $N' = N$. □

Remark 75. Saying that every map $\varphi\colon I \to E$ extends to a map $\widetilde{\varphi}\colon R \to E$ is equivalent to saying $\mathrm{Ext}^1_R(R/I, E) = 0$. To see this, consider the short exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

Applying the contravariant functor $\mathrm{Hom}_R(-, E)$, we obtain the long exact sequence

$$\begin{tikzcd}
\mathrm{Hom}_R(I,E) & \mathrm{Hom}_R(R,E) \arrow[l] & \mathrm{Hom}_R(R/I,E) \arrow[l] & 0 \arrow[l] \\
 & 0 \cong \mathrm{Ext}^1_R(R,E) & \mathrm{Ext}^1_R(R/I,E) \arrow[l] &
\end{tikzcd}$$

It's easy to check that this exact sequence implies $\mathrm{Ext}^1_R(R/I, E) \cong 0$ if and only if $\mathrm{Hom}_R(R, E) \to \mathrm{Hom}_R(I, E)$ is surjective.

51.2 Localization, Direct Sums, and Direct Products of Injective Modules

Lemma 51.3. *Let E an R-module, let $\{E_\lambda\}_{\lambda\in\Lambda}$ be a colletion of R-modules indexed by a set Λ, and let S be a multiplicatively closed subset of R. Then*

1. *$\prod_{\lambda\in\Lambda} E_\lambda$ is injective if and only if all the E_λ are injective.*
2. *If R is Noetherian, then $\bigoplus_{\lambda\in\Lambda} E_\lambda$ is injective if and only if all the E_λ are injective.*
3. *If R is Noetherian and E is an injective, then E_S is an injective R_S-module.*
4. *E is injective if and only if any monomorphism $\varphi\colon E\to M$ splits, that is, there exists a morphism $\psi\colon M\to E$ such that $\psi\circ\varphi=\mathrm{id}_E$.*

Proof.
1. Since

$$\mathrm{Hom}_R\left(M,\prod_{\lambda\in\Lambda}E_\lambda\right)\cong\prod_{\lambda\in\Lambda}\mathrm{Hom}_R\left(M,E_\lambda\right)$$

for all R-modules M, the functor $\mathrm{Hom}_R\left(-,\prod_{\lambda\in\Lambda}E_\lambda\right)$ is exact if and only if the functors $\mathrm{Hom}_R\left(-,E_\lambda\right)$ are exact for all $\lambda\in\Lambda$.

2. First assume that $\bigoplus_{\lambda\in\Lambda}E_\lambda$ is injective. Let $\lambda\in\Lambda$, let I be an ideal in R, and let $\varphi\colon I\to E_\lambda$ be an R-module homomorphism. Since $\bigoplus_{\lambda\in\Lambda}E_\lambda$ is injective, the composition

$$I\to E_\lambda\hookrightarrow\bigoplus_{\lambda\in\Lambda}E_\lambda$$

extends to a map $\widetilde{\varphi}\colon R\to\bigoplus_{\lambda\in\Lambda}E_\lambda$. Letting $\pi_\lambda\colon\bigoplus_{\lambda\in\Lambda}E_\lambda\to E_\lambda$ denote the projection to the λth component, the map $\pi_\lambda\circ\widetilde{\varphi}$ extends φ. Thus E_λ is injective for all $\lambda\in\Lambda$. Note that this direction did not depend on the fact that R is Noetherian.

Converesely, assume each E_λ is injective. By Theorem (77.2), it is enough to show that for an ideal I of R, any homomorphism $\varphi\colon I\to\bigoplus_{\lambda\in\Lambda}E_\lambda$ extends to R. Since R is Noetherian, I is finitely generated, and so there exists a finite subset $\{\lambda_1,\dots,\lambda_n\}$ of Λ such that

$$\begin{aligned}\operatorname{im}\varphi&\subseteq\bigoplus_{i=1}^n E_{\lambda_i}\\&\cong\prod_{i=1}^n E_{\lambda_i}.\end{aligned}$$

From (1), we know that $\prod_{i=1}^n E_{\lambda_i}$ is injective, and therefore we may extend φ. Thus $\bigoplus_{\lambda\in\Lambda}E_\lambda$ is injective.

3. Let $\varphi\colon I_S\to E_S$ be an R_S-module homomorphism. Since R is a Noetherian ring, the ideal I is finitely presented, and thus there exists $\psi\colon I\to E$ such that $\psi_S=\varphi$. Since E is injective, we may choose an extension $\widetilde{\psi}\colon R\to E$ of ψ. Then $\widetilde{\psi}_S\colon R_S\to E_S$ is an extension of $\varphi\colon I_S\to E_S$.

4. One direction is obvious, so we only prove the nonobvious direction. Assume that any injective R-linear map out of E splits. Let $\varphi\colon M\to N$ be an injective R-linear map and let $\psi\colon M\to E$ be any R-linear map. We need to construct a map $\widetilde{\psi}\colon N\to E$ such that $\widetilde{\psi}\circ\varphi=\psi$. To do this, consider the pushout module

$$E+_M N=(E\times N)/\{(\psi(u),-\varphi(u))\mid u\in M\}$$

together its natural maps $\iota_1\colon E\to E+_M N$ and $\iota_2\colon N\to E+_M N$, given by

$$\iota_1(v)=[v,0]\qquad\text{and}\qquad\iota_2(w)=[0,w]$$

for all $v\in E$ and $w\in N$ where $[v,w]$ denotes the equivalence class in $E+_M N$ with (v,w) as one of its representatives. Observe that

$$\begin{aligned}\iota_1(\psi(u))&=[\psi(u),0]\\&=[0,\varphi(u)]\\&=\iota_2(\varphi(u))\end{aligned}$$

for all $u\in M$. Therefore, we have a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\iota_2} \\ E & \xrightarrow[\iota_1]{} & E +_M N \end{array}$$

We claim that ι_1 is injective. Indeed, suppose $v \in \ker \iota_1$. Then $[v, 0] = [0, 0]$ implies if $(v, 0) = (\psi(u), -\varphi(u))$ for some $u \in M$. Then $\varphi(u) = 0$ implies $u = 0$ since φ is injective, and therefore

$$\begin{aligned} v &= \psi(u) \\ &= \psi(0) \\ &= 0. \end{aligned}$$

Thus ι_1 is injective. Therefore by hypothesis the map $\iota_1 \colon E \to E +_M N$ splits, say by $\lambda \colon E +_M N \to E$, where $\lambda \circ \iota_1 = 1_E$. Finally, we obtain a map $\widetilde{\psi} \colon N \to E$ by setting $\widetilde{\psi} := \lambda \circ \iota_2$. Then

$$\begin{aligned} \widetilde{\psi} \circ \varphi &= \lambda \circ \iota_2 \circ \varphi \\ &= \lambda \circ \iota_1 \circ \psi \\ &= \psi, \end{aligned}$$

shows that $\widetilde{\psi}$ has the desired property. □

Proposition 51.3. *Let R be a ring. Then R is Noetherian if and only if every direct sum of injective R-modules is injective.*

Proof. We proved one direction in Lemma (76.1). For the other direction, assume R is not Noetherian. Then R contains a strictly ascending chain of ideals

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots.$$

Let $I = \bigcup_j I_j$. The natural maps

$$I \hookrightarrow R \to R/I_j \hookrightarrow \mathrm{E}_R(R/I_j)$$

give us a homomorphism $I \to \prod_j \mathrm{E}_R(A/I_j)$, whose image lies in the submodule $\bigoplus_j \mathrm{E}_R(R/I_j)$. To see this, note for $x \in I$, we must have $x \in I_k$ for some k. This implies the image of x lies in the submodule $\bigoplus_{j=1}^{k-1} \mathrm{E}_R(R/I_j)$.

Therefore we have a homomorphism $\varphi \colon I \to \bigoplus_j \mathrm{E}_R(R/I_j)$. But φ does not extend to a homomorphism $R \to \bigoplus_j \mathrm{E}_R(R/I_j)$. □

Proposition 51.4. *Let $R \to S$ be a flat ring map. If E is an injective as an S-module, then E is injective as an R-module.*

Proof. This is true because

$$\mathrm{Hom}_R(M, E) \cong \mathrm{Hom}_R(M \otimes_R S, E)$$

and the fact that tensoring with S is exact. □

Proposition 51.5. *Let $R \to S$ be an epimorphism of rings. If E is an injective as an R-module, then E is injective as an S-module.*

Proof. This is true because

$$\mathrm{Hom}_R(N, E) = \mathrm{Hom}_S(N, E)$$

for any S-module N. □

51.3 Divisible Modules

Definition 51.2. Let M be an R-module. We say M is **divisible** if $aM = M$ for every nonzerodivisor $a \in R$.

51.3.1 Image of divisible module is divisible

Proposition 51.6. *Let $\varphi \colon M \twoheadrightarrow N$ be a surjective map of R-modules and suppose M is divisible. Then N is divisible.*

Proof. Let $a \in R$ be a nonzerodivisor and let $v \in N$. We must find a $v' \in N$ such that $av' = v$. It will then follow that $aN = N$, which will imply N is divisible. Since φ is surjective, we may choose a $u \in M$ such that $\varphi(u) = v$. Since M is divisible, we may choose a $u' \in M$ such that $au' = u$. Then setting $v' = \varphi(u')$, we have

$$\begin{aligned} av' &= a\varphi(u') \\ &= \varphi(au') \\ &= \varphi(u) \\ &= v. \end{aligned}$$

Thus N is divisible. □

51.3.2 Injectives modules are divisible (with converse being true in a PID)

Proposition 51.7. *Let M be an R-module. If M is injective, then M is divisible. The converse holds if R is a PID.*

Proof. Suppose M is injective and let $a \in R$ be a nonzerodivisor. Then the map $\varphi \colon M \to aM$, given by

$$\varphi(u) = au$$

for all $u \in M$ is an injective R-linear map. Thus we obtain a splitting map of φ, say $\psi \colon aM \to M$. Thus if $u \in M$, then we have

$$\begin{aligned} u &= (\psi\varphi)(u) \\ &= \psi(\varphi(u)) \\ &= \psi(au) \\ &= a\psi(u). \end{aligned}$$

This implies $M = aM$, that is, M is divisible.

For the converse direction, assume that R is a PID and that M is a divisible R-module. Let $\varphi \colon \langle x \rangle \to M$ be a homomorphism, where $\langle x \rangle$ is an ideal in R. Let $a \in R$ be a nonzerodivisor and set $u = \varphi(x)$. Since $M = xM$, we have $u = xv$ for some $v \in M$. Then the map $\widetilde{\varphi} \colon R \to M$, given by

$$\widetilde{\varphi}(a) = av$$

for all $a \in R$, extends φ. Indeed, it is clearly R-linear. Also

$$\begin{aligned} \widetilde{\varphi}(bx) &= (bx)v \\ &= b(xv) \\ &= bu \\ &= b\varphi(x) \\ &= \varphi(bx) \end{aligned}$$

for all $bx \in \langle x \rangle$. It follows from Baer's Criterion that M is injective. □

Example 51.1. Since $\mathbb{Z}$ is a PID and $\mathbb{Q}/\mathbb{Z}$ is divisible as a $\mathbb{Z}$-module, Proposition (77.9) implies $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module.

51.3.3 Decomposition of module over PID

Proposition 51.8. *Assume that R is a PID and let M be any R-module. Then M may be decomposed as $M = D \oplus N$ where D is divisible and N has no nontrivial divisible subgroups.*

Proof. We first argue using Zorn's Lemma that M contains a maximal divisible submdoule. Consider the partially ordered set $(\mathscr{F}, \subseteq)$, where $\mathscr{F}$ is the family of all divisible submodules of M:

$$\mathscr{F} = \{D \subseteq M \mid D \text{ is divisible submodule of } M\},$$

and where the partial order $\subseteq$ is set inclusion. Note that $\mathscr{F}$ is nonempty since the zero module is divisible. Let $\{D_i \mid i \in I\}$ be a totally ordered subset of $\mathscr{F}$. We claim that

$$\bigcup_{i \in I} D_i$$

is a divisible submodule of M, and hence an upper bound of $\{D_i \mid i \in I\}$.

To see this, we first show that $\bigcup_{i \in I} D_i$ is a submodule of M. Indeed, it is nonempty since $0 \in \bigcup_{i \in I} D_i$. Also, if $a \in R$ and $u, v \in \bigcup_{i \in I} D_i$, then there exists an $i \in I$ such that $u, v \in D_i$ since $\{D_i \mid i \in I\}$ is totally ordered, and so

$$au + v \in D_i \subseteq \bigcup_{i \in I} D_i.$$

Thus $\bigcup_{i \in I} D_i$ is a submodule of M.

Now we show that $\bigcup_{i \in I} D_i$ is divisible. Let a be a nonzero divisor in R and let u be an element in $\bigcup_{i \in I} D_i$. Then there exists an $i \in I$ such that $u \in D_i$, and as D_i is divisible, there exists a

$$v \in D_i \in \bigcup_{i \in I} D_i$$

such that $av = u$. It follows that $\bigcup_{i \in I} D_i$ is divisible.

Thus the conditions for Zorn's Lemma are satisfied and so there exists a maximal divisible submodule of M, say $D \subseteq M$. Since every divisible module over a PID is injective, we see that D is injective, and thus we have a direct sum decomposition of M say

$$M = D \oplus N$$

where N is a submodule of M. To finish the proof, assume for a contradiction that N has a nontrivial divisible submodule, say $L \subseteq N$. We claim that $D + L$ is a divisible submodule of M which properly contains D. Indeed, it is divisible since if $a \in R$ is a nonzerodivisor and $x + y \in D + L$ where $x \in D$ and $y \in L$, then we can choose $u \in D$ and $v \in L$ such that $au = x$ and $av = y$ since D and L are divisible, and so

$$\begin{aligned} a(u+v) &= au + av \\ &= x + y \end{aligned}$$

implies $D + L$ is divisible. It also properly contains D since $L \subseteq N$ is nontrivial. Thus $D + L$ is a divisible submodule of M which properly contains D. This is a contradiction as D was chosen to be a maximal divisible submodule of M. □

Proposition 51.9. *Let A be an integral domain. Then its quotient field $Q(A)$ is an injective A-module.*

Proof. We show this using Baer's criterion. Let $\varphi : I \to Q(A)$ be an A-linear map where I is an ideal of A. If $I = 0$, extend by the zero map. Otherwise, let $0 \neq x \in I$ and define the map $\widetilde{\varphi} : A \to Q(A)$ by $a \mapsto a\varphi(x)/x$. This map is obviously A-linear and if $y \in I$, then

$$\begin{aligned} \widetilde{\varphi}(y) &= \frac{y\varphi(x)}{x} \\ &= \frac{\varphi(yx)}{x} \\ &= \frac{x\varphi(y)}{x} \\ &= \varphi(y). \end{aligned}$$

□

51.4 Embedding a Module into an Injective Module

Let M be an R-module. We can always find a projective R-module P together with a surjective R-linear map $\pi\colon P \twoheadrightarrow M$. In fact, we can even choose P to be free. Is the dual version of this construction achievable? In other words, can we find an injective R-module E together with an injective map $\iota\colon M \to E$? The answer is yes, but it's not so obvious at first how to do this. To get this result, we first need a lemma which comes in handy from time to time.

Lemma 51.4. *Let S be an R-algebra, let E be an injective R-module, and let P a projective S-module. Then $\mathrm{Hom}_R(P, E)$ is an injective S-module.*

Proof. The functor $\mathrm{Hom}_S(-, \mathrm{Hom}_R(P, E))$ is exact if and only if the functor $\mathrm{Hom}_R(- \otimes_S P, E)$ is exact, by tensor-hom adjunction. Now notice that the functor $- \otimes_S P$ is exact since P is projective (and hence flat), and the functor $\mathrm{Hom}_R(-, E)$ is exact since E is injective. Thus $\mathrm{Hom}_R(- \otimes_S P, E)$ is a composition of exact functors, and so it must be exact too. □

To show that M can be embedded into an injective R-module, we first consider the case where $R = \mathbb{Z}$. Once we are able to do this in the case where $R = \mathbb{Z}$, we will use Lemma (51.4) to get this construction to work over a general commutative ring R.

Lemma 51.5. *Let M be a $\mathbb{Z}$-module. Then there exists an injective module E together with an injective $\mathbb{Z}$-linear map $\iota\colon M \to E$.*

Proof. For all $\mathbb{Z}$-modules N, we define

$$N^\vee := \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z}).$$

We have a natural map $M \to M^{\vee\vee}$, denoted by $u \mapsto \widehat{u}$, where

$$\widehat{u}(\varphi) = \varphi(u)$$

for all $u \in M$ and $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. We claim that the map $M \to M^{\vee\vee}$ is injective. Indeed, suppose $u \in M$ with $u \neq 0$. Denote $n := \mathrm{ord}(u)$ and let $\varphi\colon \langle u \rangle \to \mathbb{Q}/\mathbb{Z}$ be the unique homomorphism such that

$$\varphi(u) = \begin{cases} [1/n] & \text{if } n < \infty \\ [1/2] & \text{if } n = \infty \end{cases}$$

In either case, $\varphi(u) \neq 0$. Since $\mathbb{Q}/\mathbb{Z}$ is injective, we can extend φ to a nonzero map $\widetilde{\varphi}\colon M \to \mathbb{Q}/\mathbb{Z}$. Then

$$\begin{aligned} \widehat{u}(\widetilde{\varphi}) &= \widetilde{\varphi}(u) \\ &= \varphi(u) \\ &\neq 0 \end{aligned}$$

implies $\widehat{u} \neq 0$. It follows that $M \to M^{\vee\vee}$ is injective.

Now let $\bigoplus_{\lambda \in \Lambda} \mathbb{Z} \to M^{\vee}$ be a surjection. Since the contraviarant functor $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ is left exact, we get an embedding

$$\begin{aligned} M &\rightarrowtail M^{\vee\vee} \\ &= \mathrm{Hom}_{\mathbb{Z}}\left(M^{\vee}, \mathbb{Q}/\mathbb{Z}\right) \\ &\rightarrowtail \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{\lambda \in \Lambda} \mathbb{Z}, \mathbb{Q}/\mathbb{Z}\right) \\ &\cong \prod_{\lambda \in \Lambda} \mathbb{Q}/\mathbb{Z}, \end{aligned}$$

where $\prod_{\lambda \in \Lambda} \mathbb{Q}/\mathbb{Z}$ is injective by Lemma (76.1). □

Now we prove it for an arbitrary commutative ring.

Theorem 51.6. *Let M be an R-module. Then there is an injective module E together with an injective R-linear map $\iota\colon M \to E$.*

Proof. First we consider M as a $\mathbb{Z}$-module. There exists a $\mathbb{Z}$-injective module E_1 together with an injective $\mathbb{Z}$-linear map $\iota_1\colon M \to E_1$, by Lemma (51.5). Since R is projective over itself, $\mathrm{Hom}_{\mathbb{Z}}(R, E_1)$ is injective as an R-module, by Lemma (51.4). Let $\iota\colon M \to \mathrm{Hom}_{\mathbb{Z}}(R, E_1)$ be given by

$$\iota(u)(a) = \iota_1(au)$$

for all $a \in R$ and $u \in M$. Then ι is R-linear and injective. Indeed, it is R-linear since ι_1 is $\mathbb{Z}$-linear. Also, it is injective since if $\iota(u) = 0$, then

$$\begin{aligned} 0 &= \iota(u)(1) \\ &= \iota_1(u), \end{aligned}$$

which implies $u = 0$ since ι_1 is injective. □

51.5 Injective Hulls

Let M be an R-module. We know that we can embed M into an injective R-module. We now would like to embed M into an injective R-module E where E is as "small" as possible. To get a sense of what this means, let us first define essential extensions.

51.5.1 Essential Extensions

Definition 51.3. Let $M \subseteq E$ be an inclusion of R-modules. We say E is an **essential extension** of M, denoted $M \subseteq_{\mathrm{e}} E$, if either of the three equivalent conditions are satisfied:

1. If N is a nonzero submodule of E, then $N \cap M$ is a nonzero submodule M;
2. If e is a nonzero element of E, then $\langle e \rangle \cap M$ is a nonzero submodule of M.
3. If N is a submodule of E and $N \cap M = 0$, then $N = 0$.

We say $M \subseteq_{\mathrm{e}} E$ is a **maximal** essential extension, denoted $M \subseteq_{\mathrm{m}} E$, if the following two conditions are satisfied:

1. If F is an R-module which contains E, then $M \subseteq F$ is not essential.
2. If F is an R-module which contains E, then there exists a nonzero submodule N of F such that $M \cap N = 0$.

Remark 76. If $\varphi\colon M \rightarrowtail E$ is an injective R-linear map, then we say $\varphi\colon M \rightarrowtail E$ is an essential extension if $\varphi(M) \subseteq E$ is an essential extension.

Lemma 51.7. *Let $M \subseteq E_1 \subseteq E_2$ be R-modules.*

1. *If $M \subseteq_e E_2$, then $M \subseteq_e E_1$ and $E_1 \subseteq_e E_2$.*
2. *If $M \subseteq_e E_1$ and $E_1 \subseteq_e E_2$, then $M \subseteq_e E_2$.*

Proof. 1. Let N_2 be a nonzero submodule of E_2. Since $M \subseteq_e E_2$, we have $N_2 \cap M \neq 0$. In particular, this implies

$$E_1 \cap N_2 \supseteq M \cap N_2 \neq 0.$$

Thus $E_1 \subseteq_e E_2$. Similarly, let N_1 be a nonzero submodule of E_1. Then N_1 is a nonzero submodule of E_2, and since $M \subseteq_e E_2$, we have $M \cap N_1 \neq 0$.. Thus $M \subseteq_e E_1$.

2. Let N be a nonzero submodule of E_2. Since $E_1 \subseteq_e E_2$, we have $N \cap E_1 \neq 0$. Since $N \cap E_1$ is a nonzero submodule of E_1 and $M \subseteq_e E_1$, we have

$$\begin{aligned} M \cap N &= (M \cap E_1) \cap N \\ &= M \cap (E_1 \cap N) \\ &\neq 0. \end{aligned}$$

It follows that $M \subseteq_e E_2$. □

Example 51.2. Let I be an ideal of R. Then

$$0 :_M I \subseteq_e \bigcup_{n=1}^{\infty} 0 :_M I^n.$$

Indeed, let u be a nonzero element in $\bigcup_{n=1}^{\infty} 0 :_M I^n$. Choose n is the smallest natural number such that $uI^n = 0$. Then

$$\begin{aligned} \langle u \rangle \cap (0 :_M I) &\supseteq uI^{n-1} \\ &\neq 0. \end{aligned}$$

Example 51.3. Consider the formal power series ring $R = K[[x]]$ where K is field and let $M = R_x/R$. Every element of M is killed by a power of the maximal ideal $\mathfrak{m} = \langle x \rangle$, hence

$$M = \bigcup_{n=1}^{\infty} 0 :_M \mathfrak{m}^n.$$

The **socle** of M is defined to be $\operatorname{soc} M := 0 :_M \mathfrak{m}$. Thus by the previous example, we have

$$\operatorname{soc} M \subseteq_e M.$$

It is easy to see that $\operatorname{soc} M$ is the 1-dimensional $\mathbb{C}$-vector space generated by $[1/x]$, that is, the image of $1/x$ in M. On the other hand,

$$\prod_{\mathbb{N}} \operatorname{soc} M \subseteq \prod_{\mathbb{N}} M$$

is not an essential extension since the element

$$([1/x^n]) \in \prod_{\mathbb{N}} M$$

does not have a nonzero multiple in $\prod_{\mathbb{N}} \operatorname{soc} M$.

51.5.2 Injective Modules are Modules with no Proper Essential Extensions

Lemma 51.8. *Let M be an R-module. Then M is an injective R-module if and only if M has no proper essential extensions.*

Proof. Suppose that M is injective and let $M \subseteq_e E$ be an essential extension. Since $M \subseteq E$ and M is injective, we see that M is a direct summand of E, say

$$E = M \oplus N$$

where N is some submodule of E such that $M \cap N = 0$. Since $M \subseteq_e E$ is an essential extension, it follows that $N = 0$; hence $E = M$. Thus M has no proper essential extensions.

Conversely, suppose that M has no proper essential extension. Embed M into an injective module E. By Zorn's Lemma, we can choose a submodule N of E which is maximal with respect to the property that $M \cap N = 0$. Then E/N is an essential extension of M by construction. Since M has no proper essential extensions, we must have $M \cong E/N$. In particular, this implies $E = M \oplus N$. Then M is injective since E is injective, by Lemma (76.1). □

51.5.3 Every Module has a Maximal Essential Extension

Lemma 51.9. *Let M be an R-module. Then M has a maximal essential extension.*

Proof. Embed M into an injective R-module E. We claim that there are maximal essential extensions of M in E. Define the partially ordered set

$$\mathcal{E} = \{E' \subseteq E \mid M \subseteq_{\mathrm{e}} E'\}$$

where the partial order is given by inclusion. Note that $\mathcal{E} \neq \emptyset$ since $M \subseteq_{\mathrm{e}} M$. If (E'_n) is a chain of essential extensions of M in $\mathcal{E}$, then $E' = \bigcup_{n=1}^{\infty} E'_n$ is again an essential extension of M. Therefore there exists a maximal element in $\mathcal{E}$ by Zorn's Lemma, say

$$M \subseteq_{\mathrm{e}} E' \subseteq E.$$

We claim that $M \subseteq_{\mathrm{m}} E'$. Indeed, suppose that $E' \subseteq_{\mathrm{e}} F$ where F is not necessarily contained in E. Since E is injective, we can extend the inclusion map $E' \subseteq E$ along the inclusion map $\iota\colon E' \to F$ and obtain R-linear map $\widetilde{\iota}\colon F \to E$ such that $\widetilde{\iota}|_{E'} = \iota$. Observe that

$$\begin{aligned} \ker \widetilde{\iota} \cap M &= \ker \iota \cap M \\ &= 0 \cap M \\ &= 0. \end{aligned}$$

Since F is an essential extension of M, it follows that $\ker \widetilde{\iota} = 0$. By maximality of E', we must have $E' = \widetilde{\iota}(F) \cong F$. It follows that $M \subseteq_{\mathrm{m}} E'$. □

51.5.4 Injective Hull Definition/Theorem

Theorem 51.10. *Let $M \subseteq E$ be an inclusion of R-modules. The following statements are equivalent:*

1. *E is a maximal essential exentsion of M.*
2. *E is injective, and is an essential extension of M.*
3. *E is minimal injective over M.*

*If E satisfies any of these three equivalent conditions, then we say E is an **injective hull** of M.*

Injective hulls are unique up to an isomorphism which restricts to the identity map in the following sense:

Lemma 51.11. *Let E and E' be injective hulls of M. Then there exists an isomorphism $\varphi\colon E \to E'$ which is the identity on M.*

Proof. The map $M \to E'$ can be extended, by injectivity of E, to a map $\varphi : E \to E'$. The map is identity on M and as before since $\ker \varphi \cap M = 0$, it follows by essentiality that φ is injective. Since E' was minimal injective, it follows that φ is surjective as well. □

We use the notation $E(M)$ to denote the injective hull of M, which by the previous lemma, is well-defined up to an isomorphism that fixes M.

Lemma 51.12.

1. *If E is an injective module containing M, then E contains a copy of $E(M)$.*
2. *If $N \supset_e M$, then N can be enlarged to a copy of $E(M)$ and $E(M) = E(N)$.*

Proof.

1. We know that there is a maximal essential extension of M contained in E.
2. A maximal essential extension of N is a maximal essential extension of M.

□

Lemma 51.13. *Let A be a ring, $M_i \subset E_i$ for all $i \in I$ be A-modules over A. Then*

$$\bigoplus_{i \in I} M_i \subset_e \bigoplus_{i \in I} E_i \quad \text{if and only if} \quad M_i \subset_e E_i$$

for all $i \in I$.

Lemma 51.14. *Let A be a ring and let $M_1, \ldots, M_n$ be A-modules. Then*

$$E\left(\bigoplus_{i=1}^{n} M_i\right) = \bigoplus_{i=1}^{n} E\left(M_i\right).$$

51.6 Injective Resolutions and Injective Dimension

Definition 51.4. Let M be an R-module and let (E, d) be an R-complex. We say E is an **injective resolution** of M over R if

1. $E^i = 0$ for all $i < 0$;
2. E^i is an injective R-module for each $i \in \mathbb{Z}$;
3. $\mathrm{H}^0(E) \cong M$ and $\mathrm{H}^i(E) = 0$ for all $i > 0$.

We say E is a **minimal injective resolution** if E^i is the injective hull of $\ker \mathrm{d}^i$ for all $i \in \mathbb{Z}$. The **injective dimension** of M, denoted $\mathrm{id}_R\, M$, is the length of this minimal injective resolution (which may be ∞):

$$\mathrm{id}_R\, M = \sup\{i \in \mathbb{Z} \mid E^i \neq 0\}$$

Proposition 51.10. *Let A be a Noetherian ring, M an A-module, and S a multiplicatively closed set. Then*

$$id_{A_S}(M_S) \leq id_A(M).$$

Proof. This follows from exactness of localization and Lemma (76.1). □

Proposition 51.11. *Let A be a ring and M an A-module. The following conditions are equivalent*

1. *$id(M) \leq n$;*
2. *$Ext_A^{n+1}(N, M) = 0$ for all A-modules N;*
3. *$Ext_A^{n+1}(A/I, M) = 0$ for all ideals I of A.*

Proof.
1 $\Longrightarrow$ 2 follows from the fact that $\mathrm{Ext}_A^{n+1}(N, M)$ can be computed from an injective resolution of M.
2 $\Longrightarrow$ 3 is trivial.
3 $\Longrightarrow$ 1: Let

$$0 \to M \to E^0 \to E^1 \to E^2 \to \cdots \to E^{n-1} \to C \to 0$$

be an exact sequence, where the modules E^j are injective. From the fact that $\mathrm{Ext}_A^i(A/I, E) = 0$ for $i > 0$ if E is an injective A-module, the above exact sequence yields the isomorphism

$$\mathrm{Ext}_A^1(A/I, C) \cong \mathrm{Ext}_A^{n+1}(A/I, M),$$

and so $\mathrm{Ext}_A^1(A/I, C) = 0$ for all ideals I of A. It follows that C is injective from Remark (75). □

We can sharpen Proposition (51.11) if A is a Noetherian ring. We first observe:

Lemma 51.15. *Let A be a Noetherian ring, M an A-module, N a finitely generated A-module, and $n > 0$ an integer. Suppose that $Ext_A^n(A/\mathfrak{p}, M) = 0$ for all $\mathfrak{p} \in Supp(N)$. Then $Ext_A^n(N, M) = 0$.*

Proof. N has a finite filtration whose factors are isomorphic to $A/\mathfrak{p}$ for certain $\mathfrak{p} \in \mathrm{Supp}(N)$. Hence the lemma follows from the additivity of the vanish of $\mathrm{Ext}_A^n(-, M)$. □

Corollary 47. *Let A be a Noetherian ring and M an A-module. The following are equivalent:*

1. *$id_A(M) \leq n$;*
2. *$Ext_A^{n+1}(A/\mathfrak{p}, M) = 0$ for all $\mathfrak{p} \in Spec(A)$.*

Proposition 51.12. *Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring, $\mathfrak{p}$ a prime ideal different from $\mathfrak{m}$, and M a finitely generated A-module. If $Ext_A^{n+1}(A/\mathfrak{q}, M) = 0$ for all prime ideals $\mathfrak{q} \in \mathbf{V}(\mathfrak{p})$, with $\mathfrak{q} \neq \mathfrak{p}$, then $Ext_A^n(A/\mathfrak{p}, M) = 0$.*

Proof. We choose an element $x \in \mathfrak{m} \backslash \mathfrak{p}$. The element is $(A/\mathfrak{p})$-regular, and therefore we get the exact sequence

$$0 \longrightarrow A/\mathfrak{p} \xrightarrow{\cdot x} A/\mathfrak{p} \longrightarrow A/\langle x, \mathfrak{p}\rangle \longrightarrow 0$$

which induces the exact sequence

$$\mathrm{Ext}_A^n(A/\mathfrak{p}, M) \xrightarrow{\cdot x} \mathrm{Ext}_A^n(A/\mathfrak{p}, M) \longrightarrow \mathrm{Ext}_A^{n+1}(A/\langle x, \mathfrak{p}\rangle, M).$$

Since $\mathbf{V}(x,\mathfrak{p}) \subset \{\mathfrak{q} \in \mathbf{V}(\mathfrak{p}) \mid \mathfrak{q} \neq \mathfrak{p}\}$, Lemma (51.15) and our assumption imply

$$\mathrm{Ext}^{n+1}_A(A/\langle x,\mathfrak{p}\rangle, M) = 0,$$

so that multiplication by x on the finitely generated A-module $\mathrm{Ext}^n_A(A/\mathfrak{p}, M)$ is a surjective homomorphism. The desired result follows from Nakayama's lemma. □

It is now easy to derive the following useful formula for the injective dimension of a finitely generated module.

Proposition 51.13. *Let $(A,\mathfrak{m},k)$ be a Noetherian local ring, and M a finitely generated A-module. Then*

$$id_A(M) = sup\{i \mid Ext^i_A(k,M) \neq 0\}.$$

Proof. We set $t = \sup\{i \mid \mathrm{Ext}^i_A(k,M) \neq 0\}$. It is clear that $\mathrm{id}_A(M) \geq t$. To prove the converse inequality, note that the repeated application of Proposition (51.12) yields $\mathrm{Ext}^i_A(A/\mathfrak{p}, M) = 0$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$ and all $i > t$. This implies $\mathrm{id}_A(M) \leq t$. □

Remark 77. To see how the repeated application of Proposition (51.12) yields $\mathrm{Ext}^i_A(A/\mathfrak{p}, M) = 0$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$ and all $i > t$, suppose $\mathfrak{p}$ has dimension 1. Thus, $\mathbf{V}(\mathfrak{p}) = \{\mathfrak{m}\}$. Then $\mathrm{Ext}^{t+1}(A/\mathfrak{m}, M) = 0$ implies $\mathrm{Ext}^t_A(A/\mathfrak{p}, M) = 0$ and $\mathrm{Ext}^{t+2}(A/\mathfrak{m}, M) = 0$ implies $\mathrm{Ext}^{t+1}_A(A/\mathfrak{p}, M) = 0$. Next, suppose $\mathfrak{q}$ has dimension 2. Then for all primes $\mathfrak{p} \in \mathbf{V}(\mathfrak{q})$ where $\mathfrak{q} \neq \mathfrak{p}$, we've just shown that $\mathrm{Ext}^{t+1}_A(A/\mathfrak{p}, M) = 0$, and this implies $\mathrm{Ext}^t_A(A/\mathfrak{q}, M) = 0$.

Proposition 51.14. *Let N be an R-module, let $x \in R$ be an R-regular and an N-regular element, and let (E, d) be a minimal injective resolution of N over R. Set $(\widetilde{E}, \widetilde{\mathrm{d}})$ to be the R-complex give by $\widetilde{E} = \bigoplus_i 0 :_{E^i} x$ and $\widetilde{\mathrm{d}} = \mathrm{d}|_{\widetilde{E}}$. In particular, $\widetilde{E} \cong \mathrm{Hom}^\star_R(R/x, E)$ as R-complexes. Then $\Sigma\widetilde{E}$ is a minimal injective resolution of N/xN over R/x. Thus*

$$\mathrm{id}_{R/x}(N/xN) \leq \mathrm{id}_R R - 1.$$

Furthermore, let M be an R-module which is annihilated by x, then

$$\mathrm{Ext}^{i+1}_R(M,N) \cong \mathrm{Ext}^i_{R/x}(M, N/xN)$$

for all $i \geq 0$.

Proof. By Lemma (51.4), we see that each $\widetilde{E}^i$ is an injective (R/x)-module. Furthermore, note that E^0 is an essential extension of N since E is a *minimal* injective resolution of N over R. In particular, since

$$\widetilde{E}^0 \cap N = 0 :_N x = 0,$$

we see that $\widetilde{E}^0 = 0$. It remains to show that $\mathrm{H}^0(\Sigma\widetilde{E}) \cong N/xN$ and $\mathrm{H}^i(\Sigma\widetilde{E}) \cong 0$ for all $i \geq 1$, or equivalently, that $\mathrm{H}^1(\widetilde{E}) \cong N/xN$ and $\mathrm{H}^i(\widetilde{E}) \cong 0$ for all $i \geq 2$. Note that $\mathrm{H}(\widetilde{E}) = \mathrm{Ext}_R(R/x, N)$ by definition. Computing this homology using the short exact sequence

$$0 \to R \xrightarrow{x} R \to R/x \to 0$$

gives us $\mathrm{Ext}^1_R(R/x, N) \cong N/xN$ and $\mathrm{Ext}^i_R(R/x, N) \cong 0$ for all $i \geq 2$. It follows that $\Sigma\widetilde{E}$ is an injective resolution of N/xN over R/x. To see that $\Sigma\widetilde{E}$ is minimal, note that $\ker \widetilde{\mathrm{d}}^n$ is the intersection of the essential submodule $\ker \mathrm{d}^n$ with $\widetilde{E}^n$, and is thus essential in $\widetilde{E}^n$. It follows at once that

$$\mathrm{id}_{R/x}(N/xN) \leq \mathrm{id}_R(N) - 1.$$

For the latter part of the proposition, note that every map from M to an E^i has image killed by x, so

$$\begin{aligned} \mathrm{Hom}^\star_R(M, E) &= \mathrm{Hom}^\star_R(M, \widetilde{E}) \\ &= \mathrm{Hom}^\star_{R/x}(M, \widetilde{E}) \\ &= \Sigma^{-1}\mathrm{Hom}^\star_{R/x}(M, \Sigma\widetilde{E}) \end{aligned}$$

Taking homology gives us the last statement of the proposition. □

Remark 78. Recall that if $(R,\mathfrak{m})$ is a local ring, M is a finitely-generated R-module, and $x \in \mathfrak{m}$ is an R-regular and M-regular element, then $\mathrm{pd}_{R/x}(M/xM) = \mathrm{pd}_R(M)$. The idea behind that proof is as follows: we start with a minimal projective resolution P of M over R and denote $p = \mathrm{pd}\, M$. Then one shows that P/xP is a minimal projective resolution of M/xM over R/xR. They key here however is that $(P/xP)_p = P_p/xP_p \neq 0$ by Nakayama's lemma.

51.7 Injective Modules over Noetherian Rings

Lemma 51.16. *Let R be a Noetherian ring, let S be a multiplicatively closed subset of R, and let M be an R-module. Then $E_R(M)_S \cong E_{R_S}(M_S)$.*

Proof. We show that $E_R(M)_S$ is an injective hull of the R_S-module M_S. We know from Lemma (76.1) that $E_R(M)_S$ is an injective R_S-module. It remains to be show that $E_R(M)_S$ is an essential extension of M_S. Choose $e/1 \in E_R(M)_S$ where $e \in E_R(M)$ such that $e/1 \neq 0$ (equivalently, $se \neq 0$ for any $s \in S$). We want to show that $\langle e/1 \rangle \cap M_S \neq 0$. This is equivalent to showing that there exists an $a \in R$ such that $ae \in M$ *and* for any $s \in S$ we have $sae \neq 0$. Let

$$I_1 := M :_R e = \{a \in R \mid ae \in M\}.$$

Since $E_R(M)$ is an essential extension of M, we have $ae \neq 0$ for some $a \in I_1$. Since R is Noetherian, I_1 is finitely generated, say

$$I_1 = \langle a_{1,1}, \ldots, a_{1,k_1} \rangle.$$

In particular, $a_{1,i}e \in M$ for each $1 \leq i \leq k_1$. We claim that there exists an $x \in I_1$ such that $sxe \neq 0$ for all $s \in S$. Indeed, assume for a contradiction that this is not the case. Then there exists an $s_1 \in S$ such that $s_1 a_{1,i} e = 0$ for all i. Let

$$I_2 := M :_R s_1 e = I_1 : s_1.$$

Since $E_R(M)$ is an essential extension of M and $s_1 e \neq 0$, we have $as_1 e \neq 0$ for some $a \in I_2$. This implies $I_2 \supsetneq I_1$, since I_1 annihilates $s_1 e$. Since R is Noetherian, I_2 is finitely generated, say

$$I_2 = \langle a_{2,1}, \ldots, a_{2,k_2} \rangle.$$

In particular, $a_{2,i}s_1 e \in M$ for each $1 \leq i \leq k_2$. Observe that if for some i, we have $sa_{2,i}s_1 e \neq 0$ for all $s \in S$, then setting $x = a_{2,i}s_1$ would give us a contradiction. Thus there exists an $s_2 \in S$ such that $s_2 a_{2,i} e = 0$ for all i. Proceeding inductively, we obtain a sequence of elements (s_n) in S and a sequence of ideals (I_n) such that $I_{n+1} = I_n : s_n$. Furthermore, this sequence of ideals (I_n) must be strictly ascending: since $E_R(M)$ is an essential extension of M and $s_n \cdots s_1 e \neq 0$, we have $as_n \cdots s_1 e \neq 0$ for some $a \in I_{n+1}$. This implies $I_{n+1} \supsetneq I_n$ since I_n annihilates $s_n \cdots s_1 e$. This is a contradiction since R is Noetherian. □

Proof. Note that $\bigoplus_{i=1}^n E(M_i)$ is injective, and by the previous lemma it is essential over $\bigoplus_{i=1}^n M_i$, hence we are done. □

In the next theorem, we determine the indecomposable injective A-modules of a Noetherian ring A. Recall that an A-module M is **decomposable** if there exist nonzero submodules M_1, M_2 of M such that $M = M_1 \oplus M_2$; otherwise it is **indecomposable**.

Theorem 51.17. *Let A be a Noetherian ring.*

1. *For all $\mathfrak{p} \in \text{Spec}(A)$, the module $E(A/\mathfrak{p})$ is indecomposable.*
2. *Let $E \neq 0$ be an injective A-module and let $\mathfrak{p} \in \text{Ass}(E)$. Then $E(A/\mathfrak{p})$ is a direct summand of E. In particular, if E is indecomposable, then $E \cong E(A/\mathfrak{p})$.*
3. *Let $\mathfrak{p}, \mathfrak{q} \in \text{Spec}(A)$. Then $E(A/\mathfrak{p}) \cong E(A/\mathfrak{q})$ if and only if $\mathfrak{p} = \mathfrak{q}$.*

Proof.

1. Suppose $E(A/\mathfrak{p})$ is decomposable. Then there exist nonzero submodules N_1, N_2 of $E(A/\mathfrak{p})$ such that $N_1 \cap N_2 = 0$. It follows that

   $$(N_1 \cap (A/\mathfrak{p})) \cap (N_2 \cap (A/\mathfrak{p})) = (N_1 \cap N_2) \cap (A/\mathfrak{p}) = 0.$$

   On the other hand, since $A/\mathfrak{p} \subset_e E(A/\mathfrak{p})$ is an essential extension, we have

   $$N_1 \cap (A/\mathfrak{p}) \neq 0 \neq N_2 \cap (A/\mathfrak{p}).$$

   This contradicts the fact that $A/\mathfrak{p}$ is a domain: $N_1 \cap (A/\mathfrak{p})$ and $N_2 \cap (A/\mathfrak{p})$ are ideals in $A/\mathfrak{p}$. Denoting these ideals as I_1 and I_2 respectively, in a domain we have $I_1 \cap I_2 = 0$ implies either $I_1 = 0$ or $I_2 = 0$.
2. $A/\mathfrak{p}$ may be considered as a submodule of E since $\mathfrak{p} \in \text{Ass}(E)$. It follows that there exists an injective hull $E(A/\mathfrak{p})$ of $A/\mathfrak{p}$ such that $E(A/\mathfrak{p}) \subset E$. As $E(A/\mathfrak{p})$ is injective, it is a direct summand of E.
3. Statement 3 follows from the next lemma.

□

Lemma 51.18. *Let A be a Noetherian ring, $\mathfrak{p} \in Spec(A)$, and M a finitely generated A-module. Then*

1. *$Ass(M) = Ass(E(M))$; in particular, one has $\{\mathfrak{p}\} = Ass(E(A/\mathfrak{p}))$.*
2. *$k(\mathfrak{p}) \cong Hom_{A_\mathfrak{p}}(k(\mathfrak{p}), E(A/\mathfrak{p})_\mathfrak{p}) \cong Hom_A(A/\mathfrak{p}, E(A/\mathfrak{p}))_\mathfrak{p}$.*

Proof.

1. It is clear that $\text{Ass}(M) \subset \text{Ass}(E(M))$. Conversely, suppose $\mathfrak{p} \in \text{Ass}(E(M))$. Then there exists $e \in E(M)$ such that $\mathfrak{p} = 0 : e$. Since $M \subset_e E(M)$ is essential, we have $Ae \cap M \neq 0$. Thus, there exists $a \in A \backslash \mathfrak{p}$ such that $ae \in M$. Then
$$\begin{aligned} 0 : ae &= (0 : e) : a \\ &= \mathfrak{p} : a \\ &= \mathfrak{p}, \end{aligned}$$
implies $\mathfrak{p} \in \text{Ass}(M)$.
2. Since $E(A/\mathfrak{p})_\mathfrak{p} \cong E_{A_\mathfrak{p}}(k(\mathfrak{p}))$, we assume that $(A, \mathfrak{m}, k)$ is local and $\mathfrak{p} = \mathfrak{m}$ is the maximal ideal. The k-vector space $\text{Hom}_A(k, E(k))$ may be identified with
$$V = \{e \in E(k) \mid \mathfrak{m}e = 0\} = \text{Soc}(E(k)),$$
which contains k. If $V \neq k$, then there exists a nonzero vector subspace W of V with $k \cap W = 0$. This, however, contradicts the essentiality of the extension $k \subset E(k)$. The second isomorphism follows from
$$\text{Hom}_{A_\mathfrak{p}}(k(\mathfrak{p}), E(A/\mathfrak{p})_\mathfrak{p}) = \text{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}, E(A/\mathfrak{p})_\mathfrak{p}) \cong \text{Hom}_{A_\mathfrak{p}}((A/\mathfrak{p})_\mathfrak{p}, E(A/\mathfrak{p})_\mathfrak{p}) \cong \text{Hom}_A(A/\mathfrak{p}, E(A/\mathfrak{p}))_\mathfrak{p}$$

□

The importance of the indecomposable injective A-modules results from the following:

Theorem 51.19. *Let A be a Noetherian ring. Every injective A-module E is a direct sum of indecomposable injective A-modules, and this decomposition is unique in the following sense: for any $\mathfrak{p} \in Spec(A)$, the number of indecomposable summands in the decomposition of E which are isomorphic to $E(A/\mathfrak{p})$ depends only on E and $\mathfrak{p}$ (and not on the particular decomposition). In fact, this number equals*
$$dim_{k(\mathfrak{p})} \left(Hom_{A_\mathfrak{p}}(k(\mathfrak{p}), E_\mathfrak{p}) \right).$$

Proof. Consider the set $\mathcal{I}$ of all subsets of the set of indecomposable injective submodules of E with the property: if $\mathcal{F} \in \mathcal{I}$, then the sum of all modules belonging to $\mathcal{F}$ is direct. The set $\mathcal{I}$ is partially ordered by inclusion. By Zorn's lemma it has a maximal element $\mathcal{F}'$. Let F be the sum of all the modules in $\mathcal{F}'$. The module F is a direct sum of injective modules, and hence is itself injective. Therefore F is a direct summand of E, and we can write $E = F \oplus H$, where H is injective since it is a direct summand of E. Suppose $H \neq 0$, then there exists $\mathfrak{p} \in \text{Ass}(H)$, and so $E(A/\mathfrak{p})$ is a direct summand of H. Thus we may enlarge $\mathcal{F}'$ by $E(A/\mathfrak{p})$, contradicting the maximality of $\mathcal{F}'$. We conclude that $H = 0$ and $E = F$.

Suppose that $E = \bigoplus_{\lambda \in \Lambda} E_\lambda$ is the given decomposition. Then
$$\text{Hom}_{A_\mathfrak{p}}(k(\mathfrak{p}), E_\mathfrak{p}) \cong \text{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), \bigoplus_{\lambda \in \Lambda} (E_\lambda)_\mathfrak{p}\right) \cong \bigoplus_{\lambda \in \Lambda} \text{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), (E_\lambda)_\mathfrak{p}\right),$$
where we used the fact that $k(\mathfrak{p})$ is finitely generated in the second isomorphism. By Lemma (51.18), we have
$$\bigoplus_{\lambda \in \Lambda} \text{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), (E_\lambda)_\mathfrak{p}\right) \cong \bigoplus_{\lambda \in \Lambda_0} \text{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), (E_\lambda)_\mathfrak{p}\right)$$
where $\Lambda_0 = \{\lambda \in \Lambda \mid E_\lambda \cong E(A/\mathfrak{p})\}$. If we again use Lemma (51.18), we finally get
$$\text{Hom}_{A_\mathfrak{p}}(k(\mathfrak{p}), E_\mathfrak{p}) \cong \bigoplus_{\lambda \in \Lambda_0} \text{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), (E_\lambda)_\mathfrak{p}\right) \cong k(\mathfrak{p})^{\Lambda_0}$$

□

Theorem 51.20. *Let A be a Noetherian ring and E an injective A-module. Then*
$$E \cong \bigoplus_i E_A(A/\mathfrak{p}_i),$$
where $\mathfrak{p}_i$ are prime ideals of A. Moreover, any such direct sum is an injective A-module.

Proof. Let E be an injective A-module. By Zorn's Lemma, there exists a maximal family $\{E_i\}$ of injective submodules of E such that $E_i \cong E_A(A/\mathfrak{p}_i)$, and their sum in E is a direct sum. Let $E' = \bigoplus_i E_i$, which is an injective module, and hence is a direct summand of E. There exists an A-module E'' such that $E = E' \bigoplus E''$. If $E'' \neq 0$, pick a nonzero element $x \in E''$. Let $\mathfrak{p}$ be an associated prime of Ax. Then $A/\mathfrak{p} \hookrightarrow Ax \subseteq E''$, so there is a copy of $E_A(A/\mathfrak{p})$ contained in E'' and $E'' = E_A(A/\mathfrak{p}) \bigoplus E'''$, contradicting the maximality of the family $\{E_i\}$. □

Theorem 51.21. *Let A be a Noetherian ring, $\mathfrak{p}$ be a prime ideal of A, $E = E_A(A/\mathfrak{p})$ and let $k = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Then*

1. *If $x \in A \backslash \mathfrak{p}$, then $E \xrightarrow{\cdot x} E$ is an isomorphism, and so $E = E_\mathfrak{p}$.*
2. *$0 :_E \mathfrak{p} = k$.*
3. *$k \subseteq E$ is an essential extension of $A_\mathfrak{p}$-modules and $E = E_{A_\mathfrak{p}}(k)$.*
4. *E is $\mathfrak{p}$-torsion and $Ass(E) = \{\mathfrak{p}\}$.*
5. *$Hom_{A_\mathfrak{p}}(k, E) = k$ and $Hom_{A_\mathfrak{p}}(k, E_A(A/\mathfrak{q})_\mathfrak{p}) = 0$ for primes $\mathfrak{q} \neq \mathfrak{p}$.*

Proof.

1. Since $A/\mathfrak{p}$ is a domain and $Q(A/\mathfrak{p}) = k$, Proposition (51.9) tells us that k is an essential extension of $A/\mathfrak{p}$, so E contains a copy of k and we may assume $A/\mathfrak{p} \subseteq k \subseteq E$. Multiplication by $x \in A \backslash \mathfrak{p}$ is injective on k, and hence also on its essential extension E. The submodule xE is injective, so it is a direct summand of E. But $k \subseteq xE \subseteq E$ are essential extensions, so $xE = E$.
2. $0 :_E \mathfrak{p} = 0 :_E \mathfrak{p}A_\mathfrak{p}$ is a vector space over the field k, and hence the inclusion $k \subseteq 0 :_E \mathfrak{p}$ splits. But $k \subseteq 0 :_E \mathfrak{p} \subseteq E$ is an essential extension, so $0 :_E \mathfrak{p} = k$.
3. The containment $k \subseteq E$ is an essential extension of A-modules, hence also of $A_\mathfrak{p}$-modules. Suppose $E \subseteq M$ is an essential extension of $A_\mathfrak{p}$-modules, pick $m \in M$. Then m has a nonzero multiple $(a/s)m \in E$, where $s \in A \backslash \mathfrak{p}$. But then am is a nonzero multiple of m in E, so $E \subseteq M$ is an essential extension of A-modules, and therefore $M = E$.
4. Let $\mathfrak{q} \in \text{Ass}(E)$. Then there exists $x \in E$ such that $Ax \subseteq E$ and $0 :_A x = \mathfrak{q}$. Since $A/\mathfrak{p} \subseteq E$ is essential, x has a nonzero multiple $y = ax$ in $A/\mathfrak{p}$. But then the $\mathfrak{p} = 0 :_A y = 0 :_E ax = (0 :_E x) :_A a$ implies $\mathfrak{q} = \mathfrak{p}$. Therefore $\text{Ass}(E) = \{\mathfrak{p}\}$. Now suppose $x \in E$. Then $0 :_E x$ must be $\mathfrak{p}$-primary since $\mathfrak{p}$ is the only associated prime of $0 :_E x \hookrightarrow E$. In particular, $0 :_E x \supset \mathfrak{p}^n$ for some n, and this proves our claim.
5. For the first assertion,
$$\text{Hom}_{A_\mathfrak{p}}(k, E) = \text{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}, E) \cong 0 :_E \mathfrak{p}A_\mathfrak{p} = k.$$
For the first assertion, if $\mathfrak{q} \subsetneq \mathfrak{p}$, then $\mathfrak{q}^n \subsetneq \mathfrak{p}$. Therefore since $E_A(A/\mathfrak{q})$ is $\mathfrak{q}$-torsion, we see that $E_A(A/\mathfrak{q})_\mathfrak{p} = 0$ if $\mathfrak{q} \subsetneq \mathfrak{p}$. In the case $\mathfrak{q} \subseteq \mathfrak{p}$, we have
$$\text{Hom}_{A_\mathfrak{p}}(k, E_A(A/\mathfrak{q})_\mathfrak{p}) \cong 0 :_{E_A(A/\mathfrak{q})_\mathfrak{p}} \mathfrak{p}A_\mathfrak{p} = 0 :_{E_A(A/\mathfrak{q})} \mathfrak{p}A_\mathfrak{p}.$$
If this is nonzero, then there is a nonzero element of $E_A(A/\mathfrak{q})$ killed by $\mathfrak{p}$, which forces $\mathfrak{q} = \mathfrak{p}$ since $\text{Ass}(E_A(A/\mathfrak{q})) = \{\mathfrak{q}\}$.

□

Theorem 51.22. *Let A be a Noetherian ring and $\mathfrak{p}$ be a prime ideal of A. Then*

1. *If $x \in A \backslash \mathfrak{p}$, then $E_A(A/\mathfrak{p}) \xrightarrow{\cdot x} (A/\mathfrak{p})$ is an isomorphism, and so $E_A(A/\mathfrak{p}) = E_A(A/\mathfrak{p})_\mathfrak{p}$.*
2. *$Hom_A(A/\mathfrak{p}, E_A(A/\mathfrak{p})) = 0 :_{E_A(A/\mathfrak{p})} \mathfrak{p} = 0 :_{E_A(A/\mathfrak{p})_\mathfrak{p}} k(\mathfrak{p}) = 0 :_{E_{A_\mathfrak{p}}(k(\mathfrak{p}))} k(\mathfrak{p}) = Hom_{A_\mathfrak{p}}(k(\mathfrak{p}), E_{A_\mathfrak{p}}(k(\mathfrak{p})) = k(\mathfrak{p})$.*
3. *$Ass(E_A(A/\mathfrak{p})) = \{\mathfrak{p}\}$ and $E_A(A/\mathfrak{p})$ is $\mathfrak{p}$-torsion.*
4. *$Hom_{A_\mathfrak{p}}(k(\mathfrak{p}), E_A(A/\mathfrak{q})_\mathfrak{p}) = 0$ for primes $\mathfrak{q} \neq \mathfrak{p}$.*

Proof.

1. Since $A/\mathfrak{p}$ is a domain and $Q(A/\mathfrak{p}) = k$, Proposition (51.9) tells us that k is an essential extension of $A/\mathfrak{p}$, so E contains a copy of k and we may assume $A/\mathfrak{p} \subseteq k \subseteq E$. Multiplication by $x \in A \backslash \mathfrak{p}$ is injective on k, and hence also on its essential extension E. The submodule xE is injective, so it is a direct summand of E. But $k \subseteq xE \subseteq E$ are essential extensions, so $xE = E$.

2. $0 :_E \mathfrak{p} = 0 :_E \mathfrak{p}A_\mathfrak{p}$ is a vector space over the field k, and hence the inclusion $k \subseteq 0 :_E \mathfrak{p}$ splits. But $k \subseteq 0 :_E \mathfrak{p} \subseteq E$ is an essential extension, so $0 :_E \mathfrak{p} = k$.

3. The containment $k \subseteq E$ is an essential extension of A-modules, hence also of $A_\mathfrak{p}$-modules. Suppose $E \subsetneq M$ is an essential extension of $A_\mathfrak{p}$-modules, pick $m \in M$. Then m has a nonzero multiple $(a/s)m \in E$, where $s \in A \backslash \mathfrak{p}$. But then am is a nonzero multiple of m in E, so $E \subsetneq M$ is an essential extension of A-modules, and therefore $M = E$.

4. Let $\mathfrak{q} \in \operatorname{Ass}(E)$. Then there exists $x \in E$ such that $Ax \subseteq E$ and $0 :_A x = \mathfrak{q}$. Since $A/\mathfrak{p} \subseteq E$ is essential, x has a nonzero multiple $y = ax$ in $A/\mathfrak{p}$. But then the $\mathfrak{p} = 0 :_A y = 0 :_E ax = (0 :_E x) :_A a$ implies $\mathfrak{q} = \mathfrak{p}$. Therefore $\operatorname{Ass}(E) = \{\mathfrak{p}\}$. Now suppose $x \in E$. Then $0 :_E x$ must be $\mathfrak{p}$-primary since $\mathfrak{p}$ is the only associated prime of $0 :_E x \hookrightarrow E$. In particular, $0 :_E x \supset \mathfrak{p}^n$ for some n, and this proves our claim.

5. For the first assertion,
$$\operatorname{Hom}_{A_\mathfrak{p}}(k, E) = \operatorname{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}, E) \cong 0 :_E \mathfrak{p}A_\mathfrak{p} = k.$$
For the first assertion, if $\mathfrak{q} \subsetneq \mathfrak{p}$, then $\mathfrak{q}^n \subsetneq \mathfrak{p}$. Therefore since $E_A(A/\mathfrak{q})$ is $\mathfrak{q}$-torsion, we see that $E_A(A/\mathfrak{q})_\mathfrak{p} = 0$ if $\mathfrak{q} \subsetneq \mathfrak{p}$. In the case $\mathfrak{q} \subseteq \mathfrak{p}$, we have
$$\operatorname{Hom}_{A_\mathfrak{p}}(k, E_A(A/\mathfrak{q})_\mathfrak{p}) \cong 0 :_{E_A(A/\mathfrak{q})_\mathfrak{p}} \mathfrak{p}A_\mathfrak{p} = 0 :_{E_A(A/\mathfrak{q})} \mathfrak{p}A_\mathfrak{p}.$$
If this is nonzero, then there is a nonzero element of $E_A(A/\mathfrak{q})$ killed by $\mathfrak{p}$, which forces $\mathfrak{q} = \mathfrak{p}$ since $\operatorname{Ass}(E_A(A/\mathfrak{q})) = \{\mathfrak{q}\}$.

□

Theorem 51.23. *Let A be a Noetherian ring and let E be an injective A-module. Then*
$$E = \bigoplus_{\mathfrak{p} \in Spec(A)} E_A(A/\mathfrak{p})^{\alpha_\mathfrak{p}}$$
and the numbers $\alpha_\mathfrak{p}$ are independent of the direct sum decomposition.

Proof. By Theorem (51.20), there is a direct sum
$$E \cong \bigoplus_i E_A(A/\mathfrak{p}_i).$$
Theorem (51.22) implies $\alpha_\mathfrak{p}$ is the dimension of the $k(\mathfrak{p})$-vector space
$$\operatorname{Hom}_{A_\mathfrak{p}}(k(\mathfrak{p}), E_\mathfrak{p}),$$
which does not depend on the decomposition. □

52 Flatness

Flat modules are a type of module in abstract algebra that have important properties that distinguish them from other modules. A module is said to be flat if it satisfies a certain homological condition called the flatness condition. In particular, a flat module is one that preserves exactness under tensor product. That is, if we have a short exact sequence of modules, and we tensor it with a flat module, the resulting sequence is also exact.

52.1 Definition of Flatness

Definition 52.1. Let F be an R-module.

1. We say F is **flat** if for every injective R-linear map $\varphi \colon M \to N$, the induced map $1 \otimes \varphi \colon F \otimes_R M \to F \otimes_R N$ is again injective. An R-algebra A is called flat if it is flat as an R-module.

2. We say F is **faithfully flat** if for every R-linear map $\varphi \colon M \to N$, the map $\varphi \colon M \to N$ is injective if and only the induced map $1 \otimes \varphi \colon F \otimes_R M \to F \otimes_R N$ is injective. An R-algebra A is called faithfully flat if it is faithfully flat as an R-module.

An equivalent definition of being flat is given in the following proposition:

Proposition 52.1. *Let F be an R-module. Then F is flat if and only if the covariant function $F \otimes_R -$ is exact.*

Proof. Suppose that F is flat. Let

$$0 \longrightarrow M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0$$

be an exact sequence of R-modules. Since $F \otimes_R -$ is right exact, we only need to check that

$$0 \longrightarrow F \otimes_R M_1 \xrightarrow{1 \otimes \varphi_1} F \otimes_R M_2$$

is exact at $F \otimes_R M_1$. This is equivalent to showing $1 \otimes \varphi_1$ is injective, and this is holds since F is flat. Conversely, suppose $F \otimes_R -$ is exact. Let $\varphi \colon M \to N$ be any injective R-linear map. Since $F \otimes_R -$ is exact, the induced map $1 \otimes \varphi \colon F \otimes_R M \to F \otimes_R N$ is also injective. In other words, F is flat. □

Faithful flatness can also be characterized in terms of short exact sequences. In particular, F is faithfully flat if it satisfies the following property:

$$0 \longrightarrow M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0$$

is exact if and only if

$$0 \longrightarrow F \otimes_R M_1 \xrightarrow{1 \otimes \varphi_1} F \otimes_R M_2 \xrightarrow{1 \otimes \varphi_2} F \otimes_R M_3 \longrightarrow 0$$

Here's an alternative characterization of faithful flatness:

Proposition 52.2. *Let F be a flat R-module. The following are equivalent:*

1. *F is faithfully flat.*
2. *if M is a nonzero R-module, then $F \otimes_R M$ is nonzero too.*
3. *for all $\mathfrak{p} \in \operatorname{Spec} R$, the fiber $F \otimes_R \kappa(\mathfrak{p})$ is nonzero.*
4. *for all maximal ideals $\mathfrak{m}$ of R, the fiber $F/\mathfrak{m}F$ is nonzero.*

Proof. Suppose F is faithfully flat and let M be a nonzero R-module such that $F \otimes_R M = 0$. Then since F is faithfully flat, exactness of the $F \otimes_R 0 \to F \otimes_R M \to F \otimes_R 0$ implies exactness of $0 \to M \to 0$ which implies $M = 0$, which is a contradiction. That (2) implies (3) which implies (4) is obvious. Now assume (4) holds. Let $M := (M_1 \to M_2 \to M_3)$ be a complex and suppose that $F \otimes_R M = (F \otimes_R M_1 \to F \otimes_R M_2 \to F \otimes_R M_3)$ is exact at $F \otimes_R M_2$. Let H be the homology of M at M_2 and assume for a contradiction that $H \neq 0$. Choose any nonzero $x \in H$ and let $I = 0 : x$ be its annihilator ideal. Since $x \neq 0$, we see that I is a proper ideal of R, thus there exists a maximal ideal of R which contains I. However since $R/I \subseteq H$ and F is flat, we have

$$\begin{aligned} 0 &\neq F/\mathfrak{m}F \\ &\subseteq F/IF \\ &\subseteq F \otimes_R H \\ &= 0, \end{aligned}$$

which is a contradiction. □

Corollary 48. *Let $(R, \mathfrak{m}, \Bbbk)$ be a local noetherian ring and let F be a flat R-module. Then F is faithfully flat if and only if $F_{\Bbbk} := F \otimes_R \Bbbk \neq 0$.*

Proof. This follows trivially from (52.2) (and in fact we don't even need a noetherian hypothesis), but we wish to prove one direction in another way. In particular, assume that $F_{\Bbbk} \neq 0$. We will show that if $F \otimes_R M = 0$ then $M = 0$ for all R-modules M. In fact, it suffices to prove this property for all finitely generated R-modules M, so let M be a finitely generated R-module such that $F \otimes_R M = 0$. Then

$$\begin{aligned} F \otimes_R M = 0 &\implies F_{\Bbbk} \otimes_{\Bbbk} M_{\Bbbk} = 0 && \\ &\implies M_{\Bbbk} = 0 && \text{since } F_{\Bbbk} \neq 0 \\ &\implies M = 0 && \text{Nakayama's Lemma} \end{aligned}$$

□

Remark 79. In a moment, we will see that if F is a finitely generated R-module where $R = (R, \mathfrak{m}, \Bbbk)$ is a local ring, then F is flat if and only if it is free, in which case $\dim_{\Bbbk} F_{\Bbbk} = \operatorname{rank}_R F$. In this case we see that faithful flatness just means that F is free and $\neq 0$.

Example 52.1. Let S be a multiplicatively closed subset of R. Then R_S is a flat R-module. Indeed, this follows from the fact that $R_S \otimes_R -$ is an exact functor. On the other hand, R_S need not be faithfully flat. Indeed, suppose M is a nonzero R-module such that every element of M is annihilated by some element of S (i.e. for every $m \in M$ there exists $s \in S$ such that $sm = 0$). Then we will have $R_S \otimes_R M \simeq M_S = 0$. For example, take $R = \mathbb{Z}$ and let $S = \mathbb{Z}\backslash\{0\}$ so that $R_S = \mathbb{Q}$, and let $M = \mathbb{Z}/n\mathbb{Z}$ for some positive integer $n \geq 2$. Then $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$ even though $\mathbb{Z}/n\mathbb{Z} \neq 0$. Thus $\mathbb{Z} \to \mathbb{Q}$ is not faithfully flat.

Example 52.2. Let $F = \varinjlim F_i$ be a directed colimit of flat R-modules F_i. Then F itself is flat. Indeed, this follows from the fact that tensor products commutes with colimits. In particular, every free module is flat (and in fact faithfully flat if $\neq 0$).

Theorem 52.1. *(Lazard) An R-module is flat if and only if it is a filtered colimit of finite free R-modules.*

Proposition 52.3. *Let $\phi\colon A \to B$ be a faithfully flat map. Then the sequence*

$$0 \longrightarrow A \longrightarrow B \longrightarrow B \otimes_A B \tag{164}$$

where the last map sends $b \mapsto b \otimes 1 - 1 \otimes b$ is exact.

Proof. Suppose that $\phi\colon A \to B$ has a section, so a ring map $\sigma\colon B \to A$ such that $\sigma\phi = 1$. Then it is clear that ϕ must be injective. Let $b \in B$ such that $b \otimes 1 = 1 \otimes b$ in $B \otimes_A B$. The map $\sigma \otimes 1\colon B \otimes_A B \to B$ sends $b \otimes 1 \mapsto \sigma(b)$ and $1 \otimes b \mapsto b$, so $b = \sigma(b) \in A$, hence $b \in A$ (note that faithful flatness was not used here). For the general case, flat descent states that we can check exactness of our sequence above after applying the functor $- \otimes_A B$. If we set $A' = B$, $B' = B \otimes_A B$, then our sequence becomes

$$0 \longrightarrow A' \longrightarrow B' \longrightarrow B' \otimes_{A'} B' \tag{165}$$

where the last map is still $b' \mapsto b' \otimes 1 - 1 \otimes b'$. But in this case we have a trivial section $m\colon B' = B \otimes_A B \to B = A'$ of ϕ which is simply multiplication of B as an A-algebra. □

Example 52.3. Let $x \in R$. Then R/x not a flat R-module. Indeed, let I be any finitely generated ideal in R. Then

$$I/Ix \cong I \otimes_R R/x \to I\,(R/x) \cong I/(I \cap x)$$

is injective if and only if $Ix = I \cap x$. In particular, if I contains x, then this map is not injective.

Example 52.4. Let $R = K[x]$ and $A = K[x,y]/\langle xy, y^2\rangle$. Then A is an R-algebra via the unique map $\varphi\colon R \to A$ such that $\varphi(x) = \overline{x}$, but A is not flat as an R-module since $\langle x\rangle \otimes_R A \to \overline{x}A$ is not injective. For instance, $x \otimes \overline{y} \mapsto \overline{xy} = 0$ in xA, but $x \otimes \overline{y} \neq 0$ in $\langle x\rangle \otimes_A B$.

Example 52.5. Let $A = \mathbb{k}[t]$, let $B = \mathbb{k}[t,x]/\langle x^2 - x, x(t^3 - t)\rangle$, and let $\iota\colon A \to B$ be the inclusion map. Then B is not flat as an A-module. Indeed, let $\mathfrak{m} = \langle t\rangle$. Then the map $\mathfrak{m} \otimes_A B \to \mathfrak{m}B$ is not injective since $t \otimes x(t^2 - 1) \mapsto 0$ in B yet $t \otimes x(t^2 - 1) \neq 0$ in $\mathfrak{m} \otimes_A B$.

Let A be a flat R-algebra. Observe that for any ideal I of R, we have an isomorphism $\varphi\colon I \otimes_R A \to IA$ which is defined on elementary tensors by $\varphi(x \otimes a) = xa$ where $x \in I$ and $a \in A$. Indeed, if $\iota\colon I \to R$ denotes the inclusion map, then φ is just the composite $\varphi = \eta_A \circ (\iota \otimes 1_A)$ where $\iota \otimes 1_A\colon I \otimes_R A \to R \otimes_R A$ is injective since ι is injective and since A is flat over R, and where $\eta_A\colon R \otimes_R A \to A$ is the isomorphism defined on elementary tensors by $\eta_A(r \otimes a) = ra$ where $r \in R$ and $a \in A$.

Remark 80. Let $\iota\colon A \to B$ be an inclusion of $\mathbb{k}$-algebras. Geometrically speaking, the inclusion map $\iota\colon A \to B$ of $\mathbb{k}$-algebras corresponds to the projection $\pi\colon Y \to X$ of affine $\mathbb{k}$-schemes, where $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, and $\pi\colon Y \to X$ is defined by $\pi(\mathfrak{q}) = A \cap \mathfrak{q}$ for all primes $\mathfrak{q}$ of B. Notice that π is continuous with respect to the Zariski topology, for if $\mathrm{D}(a) = U$ is an open subset of X, then

$$\pi^{-1}(U) = \pi^{-1}(\mathrm{D}(a)) = \mathrm{D}(\iota(a)) = V.$$

That is, for all primes $\mathfrak{q}$ of B, we have $a \notin A \cap \mathfrak{q}$ if and only if $a \notin \mathfrak{q}$ for all $a \in A$. The restriction map $\pi|_V\colon V \to U$ corresponds to the inclusion map $A_a \hookrightarrow B_a$ of $\mathbb{k}$-algebras.

Given a prime $\mathfrak{p}$ of A, the fiber of $\pi\colon Y \to X$ at $\mathfrak{p}$, denoted $Y_{\mathfrak{p}}$, is the pullback of $\pi\colon Y \to X$ with respect to the morphism $\varepsilon\colon X_{\mathfrak{p}} \to X$ where we denote $X_{\mathfrak{p}} = \operatorname{Spec}(A/\mathfrak{p})$ and where $\varepsilon\colon X_{\mathfrak{p}} \to X$ is the morphism which corresponds to the $\mathbb{k}$-algebra homomorphism $A \to A/\mathfrak{p}$. In particular, the $\mathbb{k}$-algebra which corresponds to $Y_{\mathfrak{p}}$ is

$$B \otimes_A A/\mathfrak{p} \simeq B/\mathfrak{p}B.$$

Note that the map $Y_{\mathfrak{p}} \to X_{\mathfrak{p}}$ corresponds to the inclusion of $\mathbb{k}$-algebras $A/\mathfrak{p} \to B/\mathfrak{p}B$.

Proposition 52.4. *Suppose F is a flat R-module. Then $\operatorname{Tor}^R_+(F,N) = 0$ for all R-modules N.*

Proof. We prove by induction on $i \geq 1$ that $\mathrm{Tor}_i^R(F,N) = 0$ for all R-modules N. The base case $i = 1$ was proven above, so assume we have proven the proposition for some $i \geq 1$. Let N be an R-module, let $\varphi\colon G \twoheadrightarrow N$ be a surjective R-module homomorphism where G is free, and set $K = \ker\varphi$. Then we obtain an exact sequence of Tor modules:

$$0 = \mathrm{Tor}_{i+1}^R(F,G) \longrightarrow \mathrm{Tor}_{i+1}^R(F,N) \longrightarrow \mathrm{Tor}_i^R(F,K) = 0.$$

where we used the fact that G is free to obtain $\mathrm{Tor}_{i+1}^R(F,G) = 0$ and where we used the induction hypothesis to obtain $\mathrm{Tor}_i^R(F,K) = 0$. It follows that $\mathrm{Tor}_{i+1}^R(F,N) = 0$, and since N was arbitrary, we have proved the proposition by induction. □

Corollary 49. *Let*

$$0 \longrightarrow F_1 \longrightarrow F_2 \longrightarrow F_3 \longrightarrow 0 \tag{166}$$

be a short exact sequence of R-modules such that F_3 is flat. Then F_1 is flat if and only if F_2 is flat.

52.1.1 Flat Descent and Finte Projective Descent

Proposition 52.5. *The property of being flat is stable under base change.*

Proof. Let $R \to R'$ be a ring homomorphism and let M be a flat R-module. We need to show that $M' := M \otimes_R R'$ is a flat R'-module. To see this, let $N_1' \rightarrowtail N_2'$ be an injective R'-module homomorphism. We want to show that the induced map $M' \otimes_{R'} N_1' \to M' \otimes_{R'} N_2'$ is also injective. Note that for any R-module N', we have natural isomorphisms:

$$M' \otimes_{R'} N' = (M \otimes_R R') \otimes_{R'} N' \simeq M \otimes_R (R' \otimes_{R'} N') \simeq M \otimes_R N'.$$

In particular, the map $M' \otimes_{R'} N_1' \to M' \otimes_{R'} N_2'$ corresponds to the map $M \otimes_R N_1' \to M \otimes_R N_2'$ which is injective since M is R-flat. □

Proposition 52.6. *Let $R \to R'$ be a faithfully flat ring map, let M be an R-module, and set $M' = M \otimes_R R'$.*

1. *M is R-flat if and only if M' is R'-flat.*
2. *M is finitely presented as an R-module if and only if M' is a finitely presented R'-module.*
3. *M is a finite projective R-module if and only if M' is a finite projective R'-module.*

Proof. 1. If M is R-flat, then M' is R'-flat since flatness is stable under base change Conversely, assume that M' is R'-flat. Let

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0 \tag{167}$$

be a short exact sequence of R-modules. Then

$$0 \longrightarrow N_1 \otimes_R R' \otimes_{R'} M' \longrightarrow N_2 \otimes_R R' \otimes_{R'} M' \longrightarrow N_3 \otimes_R R' \otimes_{R'} M' \longrightarrow 0 \tag{168}$$

is exact since R' is R-flat and M' is R'-flat. By the associative and cancellative properties of tensor products, we may write this last short exact sequence as

$$0 \longrightarrow N_1 \otimes_R R' \otimes_R M \longrightarrow N_2 \otimes_R R' \otimes_R M \longrightarrow N_3 \otimes_R R' \otimes_R M \longrightarrow 0 \tag{169}$$

Finally, faithful flatness implies

$$0 \longrightarrow N_1 \otimes_R M \longrightarrow N_2 \otimes_R M \longrightarrow N_3 \otimes_R M \longrightarrow 0 \tag{170}$$

is exact. It follows that M is R-flat.

2. One direction is clear. For the other direction assume that M' is finitely presented as an R'-module. First let us show that M is finitely generated. Let $u_1', \dots, u_{m'}'$ be generators of M' as an R'-module. Then there exists $r_1', \dots, r_m' \in R'$ and $u_1, \dots, u_m \in M$ such that

$$u_j' = \sum_{i=1}^{m} u_i \otimes r_i'.$$

Consider the short exact sequence of R-modules

$$R^m \xrightarrow{\varphi} M \twoheadrightarrow N \longrightarrow 0 \tag{171}$$

where $\varphi = (u_1, \ldots, u_m)$ and where $N = \operatorname{coker} \varphi$. Tensoring (171) with $- \otimes_R R'$ gives us a surjective $\varphi \otimes 1 \colon R'^m \twoheadrightarrow M'$ and in particular we have $N \otimes_R R' = 0$. Since $R \to R'$ is faithfully flat, this implies $N = 0$.

Next let us show that M is finitely presented. Let $L = \ker \varphi$. Since $R \to R'$ is flat, we see that $L' := L \otimes_R R'$ is the kernel of the base change $R'^m \to M'$. Since M' is finitely presented, it follows that L' is finitely generated as an R'-module. However by the argument as above, we see that L' being finitely generated as an R'-module implies L is finitely generated as an R-module.

3. This follows from (1) and (2) as well as the fact that a module is finite projective if and only if it is finitely presented and flat.

□

52.2 Criterion for Flatness Using Tor

Let F be an R-module. If we want to determine if F is flat, then it turns out that we do not necessarily need to check that $\varphi \otimes 1_F \colon M \otimes_R F \to N \otimes_R F$ is injective for *every* injective R-linear map $\varphi \colon M \to N$; we only need to check that $\varphi \otimes 1_F$ is injective for a special class of injective R-linear map $\varphi \colon M \to N$. In particular, we only need to check that it holds for all maps of the form $\iota \colon I \to R$ where I is a finitely generated ideal of R and where ι is the inclusion map. Let us note that for arbitrary ideals I of R with inclusion denoted $\iota \colon I \to R$, the map $\iota \otimes_R F$ is injective if and only if $\operatorname{Tor}_1^R(R/I, F) = 0$. Indeed, applying $- \otimes_R F$ to the short exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

gives us the exact sequence

$$0 \cong \operatorname{Tor}_1^R(R, F) \longrightarrow \operatorname{Tor}_1^R(R/I, F) \longrightarrow I \otimes_R F \longrightarrow F. \tag{172}$$

From the exact sequence (172), we see that $I \otimes_R F \to F$ being injective is equivalent to $\operatorname{Tor}_1^R(R/I, F) = 0$. Thus if F is flat, then certanly we have $\operatorname{Tor}_1^R(R/I, F) = 0$.

Theorem 52.2. *F is a flat R-module if and only if $\operatorname{Tor}_1^R(R/I, F) = 0$ for all finitely generated ideals I of R.*

Proof. If F is flat, then $I \otimes_R F \to F$ is injective for all finitely generated ideals I of R, and as noted above, this is equivalent to $\operatorname{Tor}_1^R(R/I, F) = 0$ for all finitely generated ideals I of R (and in fact arbitrary ideals I of R). Now we prove the converse. Assume $\operatorname{Tor}_1^R(R/I, F) = 0$ for all finitely generated ideals I of R. What we need to show is that, for any injective map R-linear map $\varphi \colon M \to N$, the induced map $\varphi \otimes 1 \colon M \otimes_R F \to N \otimes_R F$ is injective. We break the proof down into two cases.

Case 1: First consider the case where $\varphi \colon M \to N$ has the form $I \subseteq R$ where I is an arbitary ideal of R (so not necessarily finitely generated). Assume for a contradiction that $I \otimes_R F \to F$ is not injective. Then there exists a nonzero tensor $\sum_i x_i \otimes f_i$ in $I \otimes_R F$ such that $\sum_i x_i f_i = 0$. Let I_0 be the ideal of R generated by the x_i. Then note that the tensor $\sum_i x_i \otimes f_i$ belongs to $I_0 \otimes_R F$. By assumption, it must be zero in $I_0 \otimes_R F$, and therefore its image in $I \otimes_R F$ has to be zero as well, which is a contradiction. Thus if $\operatorname{Tor}_1^R(R/I, F) = 0$ for all finitely generated ideals I of R, then $I \otimes_R F \to F$ is injective for all arbitary ideals I of R which is equivalent to $\operatorname{Tor}_1^R(R/I, F) = 0$ for all abitrary ideals I of R.

Case 2: Now we consider the more general case where $\varphi \colon M \to N$ is an arbitrary injective R-linear map. By replacing M with $\varphi(M)$ if necessary, we may assume that M is a submodule of N and that $\varphi \colon M \to N$ has the form $\iota \colon M \to N$ where ι is the inclusion map. Once again, assume for a contradiction that $\iota \otimes 1_F \colon M \otimes_R F \to N \otimes_R F$ is not injective. Then there exists a nonzero tensor $\sum_{i=1}^k m_i \otimes f_i$ in $M \otimes_R F$ such that $\sum_i \iota(m_i) \otimes f_i = 0$. Let N_0 by the submodule of N generated by the $\iota(m_i)$. Then $\iota \otimes 1_F$ lands in $N_0 \otimes_R F$, and if view it as a map $\iota \otimes 1_R \colon M \otimes_R F \to N_0 \otimes_R F$, then it would still not be injective. Thus by replacing N with N_0 if necessary, we may assume that N is finitely generated. Thus we can find an increasing chain

$$M = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_t = N$$

of R-submodules of N such that $M_{i+1}/M_i \cong R/I_i$ for some ideal I_i of R for all $0 \leq i \leq t$. Since the map $M \otimes_R F \to N \otimes_R F$ is equal to the composite of the maps $M_i \otimes_R F \to M_{i+1} \otimes_R F$, it follows that one of theese maps is not injective, say $M_i \otimes_R F \to M_{i+1} \otimes_R F$ is not injective. So by replacing M with M_i and N with M_{i+1} if necessary, we may assume that $N/M \cong R/I$ for some ideal I of R. Now we apply Tor to the short exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow R/I \longrightarrow 0$$

and we obtain

$$0 = \mathrm{Tor}_1^R(R/I, F) \longrightarrow M \otimes_R F \longrightarrow N \otimes_R F.$$

where $\mathrm{Tor}_1^R(R/I, F) = 0$ was shown in case 1. It follows that $M \otimes_R F \to N \otimes_R F$, which gives us our desired contradiction. $\square$

52.3 Relational Criterion for Flatness

Let M be an R-module. Suppose that we have a relation of the form

$$\sum_i r_i m_i = 0, \tag{173}$$

where $r_i \in R$, where $m_i \in M$, and where the sum (173) is understood to be finite. We will say (173) is a trivial relation if there exists $r_{ij} \in R$ and $\widetilde{m}_j \in M$ indexed over finite sets $\mathcal{I}$ and $\mathcal{J}$ such that

$$\sum_j r_{ij}\widetilde{m}_j = m_i \text{ for all } i \in \mathcal{I} \quad \text{and} \quad \sum_i r_i r_{ij} = 0 \text{ for all } j \in \mathcal{J}.$$

Indeed, in this case, the only reason why (173) holds is because of some annihilation happening in R:

$$\begin{aligned}\sum_i r_i m_i &= \sum_i r_i \left(\sum_j r_{ij}\widetilde{m}_j\right) \\ &= \sum_j \left(\sum_i r_i r_{ij}\right)\widetilde{m}_j \\ &= \sum_j 0\widetilde{m}_j \\ &= 0.\end{aligned}$$

On the other hand, consider $R = \mathbb{Z}$ and $M = \mathbb{Z}/2$. If $r = 2$ and $m = \overline{1}$, then we have $rm = 0$ and this relation is not trivial in the sense above. We want to show that M is flat if and only if all relations of the form (173) are trivial. We begin with a lemma:

Lemma 52.3. *Let $\mathcal{I}$ be an indexing set, let $m_i \in M$ for all $i \in \mathcal{I}$ where $m_i = 0$ for all but finitely many $i \in \mathcal{I}$, and let $N = \langle n_i \mid i \in \mathcal{I}\rangle$. Then $\sum_i m_i \otimes n_i = 0$ if and only if there exists an indexing set $\mathcal{J}$ and there exists exists finitely many $r_{ij} \in R$ and finitely many $\widetilde{m}_j \in M$ such that*

$$\sum_j r_{ij}\widetilde{m}_j = m_i \textit{ for all } i \in \mathcal{I} \quad \textit{and} \quad \sum_i n_i r_{ij} = 0 \textit{ for all } j \in \mathcal{J}.$$

Proof. One direction is clear, so we just prove the other direction. Suppose $\sum_i m_i \otimes n_i = 0$ and let

$$\widetilde{F} \xrightarrow{\varphi} F \xrightarrow{\pi} N \longrightarrow 0$$

be a presentation of N such that there is a basis $\{\widetilde{e}_j\}_{j\in\mathcal{J}}$ of $\widetilde{F}$ and $\{e_i\}_{i\in\mathcal{I}}$ of F with

$$\varphi(\widetilde{e}_j) = \sum_i r_{ij}e_i \quad \text{and} \quad \pi(e_i) = n_i$$

for all $i \in \mathcal{I}$ and $j \in \mathcal{J}$. Now apply $M \otimes_R -$ to the presentation to get an exact sequence:

$$M \otimes_R \widetilde{F} \xrightarrow{1\otimes\varphi} M \otimes_R F \xrightarrow{1\otimes\pi} M \otimes N \longrightarrow 0$$

Then $\sum_i m_i \otimes n_i = 0$ implies $\sum_i m_i \otimes e_i \in \ker \pi$ which implies there exists some finite sum $\sum_j \widetilde{m}_j \otimes \widetilde{e}_j$ in $M \otimes_R \widetilde{F}$ such that such that

$$\begin{aligned}\sum_i m_i \otimes e_i &= (1\otimes\varphi)(\sum_j \widetilde{m}_j \otimes \widetilde{e}_j) \\ &= \sum_j \widetilde{m}_j \otimes \varphi(\widetilde{e}_j) \\ &= \sum_j \widetilde{m}_j \otimes \left(\sum_i r_{ij}e_i\right) \\ &= \sum_i \left(\sum_j r_{ij}\widetilde{m}_j\right) \otimes e_i.\end{aligned}$$

This implies $m_i = \sum_j r_{ij}\widetilde{m}_j$ since $M \otimes_R F$ is a free R-module with basis $\{e_i\}$. To show $\sum_i r_{ij} n_i = 0$, note that $\sum_i r_{ij} n_i = \pi(\varphi(\widetilde{e}_j)) = 0$. □

Proposition 52.7. *M is flat if and only if all relations of the form (173) are trivial relations.*

Proof. Assume that M is flat and suppose we have the relation (173). Set I to be the ideal generated by the r_i. Since M is flat, the map $I \otimes_R M \to M$, induced by $I \subset R$, is injective. This implies $\sum_i r_i \otimes m_i = 0$, and the result follows from Lemma (52.3).

Conversely, assume that all relations of the form (173) are trivial, and let $I \subseteq R$ be a finitely generated ideal. By Theorem (52.2), it suffices to prove that $\mathrm{Tor}_1^R(R/I, M) = 0$, or equivalently, that the induced map $I \otimes_R M \to M$ is injective. Let $\sum_i r_i \otimes m_i \in I \otimes_R M$ such that $\sum_i r_i m_i = 0$. Then again by Lemma (52.3), we see that $\sum_i r_i \otimes m_i = 0$. Thus $I \otimes_R M \to M$ is injective. □

Corollary 50. *Let R be a principal ideal ring and let M be an R-module. Then is flat if and only if*

$$0 :_M r = (0 :_R r)M$$

for all $r \in R$. In particular, if R is a principal ideal domain, then M is flat if and only if it is torsion-free.

Corollary 51. *Assume $R = \Bbbk[\varepsilon]$ where $\Bbbk$ is a field and $\varepsilon^2 = 0$. Then M is flat if and only if*

$$0 :_M \varepsilon = \varepsilon M.$$

In other words, M is flat if and only if the multiplication by ε map induces an isomorphism $M/\varepsilon M \cong \varepsilon M$.

Corollary 52. *Let A be a valuation domain and let M be an A-module. Then M is flat if and only if M is torsion-free.*

Corollary 53. *Let A be a Dedekind domain and let M be a Dedekind domain. Then M is flat if and only if M is torsion-free.*

Proof. Note that M is torsion-free as an A-module if and only if $M_\mathfrak{m}$ is torsion-free as an $A_\mathfrak{m}$-module for all maximal ideals $\mathfrak{m}$ of A. Similarly, M is flat as an R-module if and only if $M_\mathfrak{m}$ is flat as an $A_\mathfrak{m}$-module for all maximal ideals $\mathfrak{m}$ of A. Thus the corollary follows from the characterization of A being a Dedekind domain is equivalent to $A_\mathfrak{m}$ is a valuation domain for all maximals ideals $\mathfrak{m}$ of A. □

52.3.1 Finitely Generated Flat Modules over Local Ring are Free

Proposition 52.8. *Let $(R, \mathfrak{m}, \Bbbk)$ be a local ring and let M be a flat R-module. Moreover, let $u_1, \dots, u_k \in M$ such that their classes $\overline{u}_1, \dots, \overline{u}_k$ in $M/\mathfrak{m}M$ are $\Bbbk$-linearly independent. Then $u_1, \dots, u_k$ are R-linearly independent. In particular, a finitely generated R-module is flat if and only if it is free.*

Proof. We use induction on k. Let $k = 1$ and assume $ru_1 = 0$ for some $r \in R$. Using Proposition (52.7), we obtain $\widetilde{u}_j \in M$ and $r_j \in R$ such that $\sum_j r_j \widetilde{u}_j = u_1$ and $rr_j = 0$ for all j. But $u_1 \notin \mathfrak{m}M$ implies $r_j \notin \mathfrak{m}$ for some j, and therefore $r = 0$. We now assume the proposition is proved for some $k \geq 1$. Suppose $\sum_{i=1}^{k+1} r_i u_i = 0$. We use Proposition (52.7) again and obtain $\widetilde{u}_j \in M$ and $r_{ij} \in R$ such that $\sum_j r_{ij}\widetilde{u}_j = u_i$ for all i and $\sum_i r_{ij} r_j = 0$ for all j. Because $u_{k+1} \notin \mathfrak{m}M$, we have $r_{k+1,j} \notin \mathfrak{m}$ for some j. This implies

$$\begin{aligned} 0 &= \sum_{i=1}^{k} r_i u_i + r_{k+1} u_{k+1} \\ &= \sum_{i=1}^{k} r_i u_i + \sum_{i=1}^{k} (-r_{ij}/r_{k+1,j}) r_i u_{k+1} \\ &= \sum_{i=1}^{k-1} r_i (u_i - (r_{ij}/r_{k+1,j}) u_k). \end{aligned}$$

The induction hypothesis implies that $r_1 = \cdots = r_k = 0$, and therefore $r_{k+1} = 0$ by the base case. □

52.4 More Properties of Flat Modules

Lemma 52.4. *Let M be a flat R-module, let $\{M_\lambda\}_{\lambda \in \Lambda}$ be a colletion of R-modules indexed by a set Λ, and let S be a multiplicatively closed subset of R. Then*

1. *$\bigoplus_{\lambda \in \Lambda} M_\lambda$ is flat if and only if all the M_λ are flat.*
2. *M_S is a flat R_S-module, and hence a flat R-module.*

Proof.
1. Since we have isomorophisms

$$N \otimes_R \left(\bigoplus_{\lambda \in \Lambda} M_\lambda \right) \cong \bigoplus_{\lambda \in \Lambda} (N \otimes_R M_\lambda)$$

natural in N, the functor $- \otimes_R (\bigoplus_{\lambda \in \Lambda} M_\lambda)$ is exact if and only if the functors $- \otimes_R M_\lambda$ are exact for all $\lambda \in \Lambda$.

2. Let I_S be an ideal in R_S. Since localization is exact and commutes with tensors products, we see that $I \otimes_R M \to M$ is injective implies $I_S \otimes_{R_S} M_S \to M_S$ is injective. Therefore M_S is a flat R_S-module. To see that M_S is a flat R-module, note that

$$\begin{aligned} I \otimes_R M_S &\cong I \otimes_R (R_S \otimes_{R_S} M_S) \\ &\cong (I \otimes_R R_S) \otimes_{R_S} M_S \\ &\cong I_S \otimes_{R_S} M_S. \end{aligned}$$

Thus injectivity of $I \otimes_R M_S \to M_S$ is equivalent to injectivity of $I_S \otimes_R M_S \to M_S$. □

Corollary 54. *Let P be a projective R-module. Then P is flat.*

Proof. First note that every free module is flat. Indeed, R is flat as an R-module and every free module is a direct sum copies of R. Thus Lemma (76.1) implies every free module is flat. Since P is projective, there exists an R-module K and a free R-module F such that $P \oplus K \cong F$. Then it follows Lemma (76.1) that P is flat since F is flat. □

52.4.1 Flat Modules are not necessarily Projective

Proposition 52.9. *$\mathbb{Q}$ is a flat $\mathbb{Z}$-module that is not projective.*

Proof. It follows from Proposition (78.4) that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module, so we just need to show that $\mathbb{Q}$ is not projective. Let $\varphi\colon \bigoplus_{i \in \mathbb{N}} \mathbb{Z} \to \mathbb{Q}$ be the unique $\mathbb{Z}$-linear map defined on the standard basis $\{e_n\}$ of $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}$ by

$$\varphi(e_n) = \frac{1}{n}$$

for all $n \in \mathbb{N}$, and let $\psi\colon \mathbb{Q} \to \mathbb{Q}$ be the identity map. Observe that φ is surjective since if $m/n \in \mathbb{Q}$, then $\varphi(me_n) = m/n$. However there is no $\widetilde{\psi}\colon \mathbb{Q} \to \bigoplus_{n \in \mathbb{N}} \mathbb{Z}$ such that $\psi = \varphi\widetilde{\psi}$. Indeed, observe that the injective map

$$\bigoplus_{n \in \mathbb{N}} \mathbb{Z} \to \prod_{n \in \mathbb{N}} \mathbb{Z}$$

induces the injective map

$$\mathrm{Hom}_{\mathbb{Z}} \left(\mathbb{Q}, \bigoplus_{n \in \mathbb{N}} \mathbb{Z} \right) \to \mathrm{Hom}_{\mathbb{Z}} \left(\mathbb{Q}, \prod_{n \in \mathbb{N}} \mathbb{Z} \right)$$

since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, -)$ is a left-exact covariant functor. Therefore the injection

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}} \left(\mathbb{Q}, \bigoplus_{n \in \mathbb{N}} \mathbb{Z} \right) &\to \mathrm{Hom}_{\mathbb{Z}} \left(\mathbb{Q}, \prod_{n \in \mathbb{N}} \mathbb{Z} \right) \\ &\cong \prod_{n \in \mathbb{N}} \mathrm{Hom}_{\mathbb{Z}} (\mathbb{Q}, \mathbb{Z}) \\ &\cong 0 \end{aligned}$$

implies

$$\mathrm{Hom}_{\mathbb{Z}} \left(\mathbb{Q}, \bigoplus_{n \in \mathbb{N}} \mathbb{Z} \right) \cong 0.$$

Thus the only $\mathbb{Z}$-linear map from $\mathbb{Q}$ to $\bigoplus_{n \in \mathbb{N}} \mathbb{Z}$ is the zero map. □

52.4.2 Flatness and projectiveness are stable under composition

Proposition 52.10. *Let $A \to B$ be a ring homomorphism and let C be a B-module.*

1. *If B is A-flat and C is B-flat, then C is A-flat.*

2. *If B is A-projective and C is B-projective, then C is A-projective.*

Proof. Suppose $M \rightarrowtail M'$ is an injective A-module homomorphism. We have a commutative diagram whose vertical arrows are isomorphisms:

$$\begin{tikzcd} C \otimes_A M \arrow[r] \arrow[d, "\simeq"] & C \otimes_A M' \arrow[d, "\simeq"] \\ (C \otimes_B B) \otimes_A M \arrow[r] \arrow[d, "\simeq"] & (C \otimes_B B) \otimes_A M' \arrow[d, "\simeq"] \\ C \otimes_B (B \otimes_A M) \arrow[r, tail] & C \otimes_B (B \otimes_A M') \end{tikzcd}$$

The bottom arrow is injective since B is A-flat and C is B-flat. Therefore $C \otimes_A M \rightarrowtail C \otimes_A M'$ is injective; whence C is A-flat.

Now suppose that $M \twoheadrightarrow M'$ is a surjective A-module homomorphism. We have a commutative diagram whose vertical arrows are isomorphisms:

$$\begin{tikzcd} \mathrm{Hom}_A(C, M) \arrow[r] \arrow[d, "\simeq"] & \mathrm{Hom}_A(C, M') \arrow[d, "\simeq"] \\ \mathrm{Hom}_A(C \otimes_B B, M) \arrow[r] \arrow[d, "\simeq"] & \mathrm{Hom}_A(C \otimes_B B, M') \arrow[d, "\simeq"] \\ \mathrm{Hom}_B(C, \mathrm{Hom}_A(B, M)) \arrow[r, two heads] & \mathrm{Hom}_B(C, \mathrm{Hom}_A(B, M')) \end{tikzcd}$$

The bottom arrow is surjective since B is A-projective and C is B-projective. Therefore $\mathrm{Hom}_A(C, M) \rightarrowtail \mathrm{Hom}_A(C, M')$ is surjective; whence C is A-projective. $\square$

52.5 Finite Projective and Finitely Presented Flat

Definition 52.2. Let M be an R-module.

1. We say M is **locally free** if there exists $\boldsymbol{s} = s_1, \dots, s_m \in R$ such that $\langle \boldsymbol{s} \rangle = R$ and M_{s_i} is a free R_{s_i}-module for each $1 \leq i \leq m$.

2. We say M is **finite locally free** if there exists $\boldsymbol{s} = s_1, \dots, s_m \in R$ such that $\langle \boldsymbol{s} \rangle = R$ and M_{s_i} is a finite free R_{s_i}-module for each $1 \leq i \leq m$.

3. We say M is **finite locally free** of **rank** k if there exists $\boldsymbol{s} = s_1, \dots, s_m \in R$ such that $\langle \boldsymbol{s} \rangle = R$ and M_{s_i} is isomorphic to $R_{s_i}^{\oplus k}$ as an R_{s_i}-module for each $1 \leq i \leq m$.

Lemma 52.5. *Let M be an R-module. The following are equivalent:*

1. *M is finitely presented and R-flat,*

2. *M is finite projective,*

3. *M is finitely presented and $M_{\mathfrak{p}}$ is $R_{\mathfrak{p}}$-free for all prime ideals $\mathfrak{p}$ of R.*

4. *M is finitely presented and $M_{\mathfrak{m}}$ is $R_{\mathfrak{m}}$-free for all maximal ideals $\mathfrak{m}$ of R.*

5. *M is finite and locally free,*

6. *M is finite locally free,*

7. *M is finite, for every prime $\mathfrak{p}$ the module $M_{\mathfrak{p}}$ is free, and the function $\rho_M \colon \mathrm{Spec}\, R \to \mathbb{Z}$ given by*

$$\mathfrak{p} \mapsto \dim_{\kappa(\mathfrak{p})} M \otimes_R \kappa(\mathfrak{p}),$$

is locally constant in the Zariski topology.

Proof. □

52.6 Base Change

Proposition 52.11. *Let $R \to S$ be a flat ring map. If E is an injective S-module, then E is injective as an R-module.*

Proof. This is true because $\mathrm{Hom}_R(M, E) = \mathrm{Hom}_S(M \otimes_R S, E)$ and the fact that tensoring with S is exact. □

52.7 Local Criteria for Flatness

In this section we give criteria for flatness over local rings. We shall weaken the condition $\mathrm{Tor}_1^R(R/I, M) = 0$ for all $I \subset R$ to just $\mathrm{Tor}_1^R(R/\mathfrak{m}, M) = 0$ for $\mathfrak{m}$ the maximal ideal.

Proposition 52.12. *Let M be an R-module. The following conditions are equivalent:*

1. *M is a flat R-module.*
2. *$M_\mathfrak{p}$ is a flat $A_\mathfrak{p}$-module for all prime ideals $\mathfrak{p}$.*
3. *$M_\mathfrak{m}$ is a flat $A_\mathfrak{m}$-module for all maximal ideals $\mathfrak{m}$.*

Proof.

(1 $\Longrightarrow$ 2): Let **A-Mod** denote the category of A-modules and let $\mathbf{A_\mathfrak{p}}$-**Mod** denote the category of $A_\mathfrak{p}$-modules. Then localization is full as a functor. In particular, every injective map of $A_\mathfrak{p}$-modules has the form $\varphi_\mathfrak{p} : N_\mathfrak{p} \to L_\mathfrak{p}$, where N and L are A-modules and φ is an injective map A-linear map from N to L. The map $i \otimes 1 : N \otimes_A M \to L \otimes_A M$ is also injective since M is flat as an A-module. Since localization is exact as a functor and commutes with tensor products, we have $i_\mathfrak{p} \otimes 1 : N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p} \to L_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}$ is an injective map of $A_\mathfrak{p}$-modules. Therefore $M_\mathfrak{p}$ is flat as an $A_\mathfrak{p}$-module.

(2 $\Longrightarrow$ 3): Trivial.

(3 $\Longrightarrow$ 1): Let φ denote the inclusion map $I \subset A$ be an ideal. We will show that $\mathrm{Ker}(1 \otimes \varphi) = 0$ by showing $\mathrm{Ker}(1 \otimes \varphi)_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m} \subset A$. Suppose $\mathfrak{m} \subset A$ is an arbitrary maximal ideal. By hypothesis, $M_\mathfrak{m}$ is a flat $A_\mathfrak{m}$-module. Since localization is exact as functor, the map $\varphi_\mathfrak{m} : I_\mathfrak{m} \subset A_\mathfrak{m}$ is injective, and since $M_\mathfrak{m}$ is flat as an $A_\mathfrak{m}$-module, the map $1 \otimes \varphi_\mathfrak{m} : I_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m} \to I_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m}$ is injective as well. Therefore

$$
\begin{aligned}
0 &\cong \mathrm{Ker}(1 \otimes \varphi_\mathfrak{m}) \\
&= \mathrm{Ker}((1 \otimes \varphi)_\mathfrak{m}) \\
&= \mathrm{Ker}(1 \otimes \varphi)_\mathfrak{m},
\end{aligned}
$$

which proves the claim. □

Lemma 52.6. *Let $(A, \mathfrak{m}, \Bbbk)$ be a local ring and let M be an A-module such that $\mathrm{Tor}_1^A(\Bbbk, M) = 0$. Then $\mathrm{Tor}_1^A(L, M)$ for all A-modules L of finite length.*

Proof. We use induction on the length. The case $\ell(L) = 1$ is clear because it implies $L \cong \Bbbk$. Assume now that $\ell(L) > 1$. Let $L' \subsetneq L$ be a proper submodule. We obtain the exact sequence

$$
\mathrm{Tor}_1^A(L', M) \longrightarrow \mathrm{Tor}_1^A(L, M) \longrightarrow \mathrm{Tor}_1^A(L/L', M)
$$

By the induction hypothesis, we have $\mathrm{Tor}_1^A(L', M) = 0 = \mathrm{Tor}_1^A(L/L', M)$. This implies $\mathrm{Tor}_1^A(L, M) = 0$. □

Theorem 52.7. *Let $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ be noetherian local rings such that B is an A-algebra with $\mathfrak{m}B \subseteq \mathfrak{n}$ and let N be a finitely generated B-module. Then N is A-flat if and only if $\mathrm{Tor}_1^A(\Bbbk, N) = 0$ where we set $\Bbbk = A/\mathfrak{m}$.*

Proof. If N is A-flat, then $\mathrm{Tor}_1^A(\Bbbk, N) = 0$ by Theorem (52.2). Now assume that $\mathrm{Tor}_1^A(\Bbbk, N) = 0$. Let $\mathfrak{a}$ be an ideal of A. We have to prove that $\mathfrak{a} \otimes_A N \to N$ is injective, so let τ be in the kernel of that map. It suffices to show that

$$
\tau \in \bigcap_{n=1}^{\infty} \mathfrak{m}^n(\mathfrak{a} \otimes_A N) \subseteq \bigcap_{n=1}^{\infty} \mathfrak{n}^n(\mathfrak{a} \otimes_A N) = 0,
$$

where the last equality holds by Krull's Intersection Theorem (since B is noetherian and $\mathfrak{a} \otimes_A N$ is a finitely generated B-module). We will show that $\tau \in \mathfrak{m}^n(\mathfrak{a} \otimes_A N)$ for each $n \in \mathbb{N}$. Note that $\mathfrak{m}^n(\mathfrak{a} \otimes_A N)$ is the image of the map

$$\mathfrak{m}^n \mathfrak{a} \otimes_A N \to \mathfrak{a} \otimes_A N.$$

By Artin-Rees, there exists an integer n' such that $\mathfrak{m}^{n'} \cap \mathfrak{a} \subseteq \mathfrak{m}^n \mathfrak{a}$, so it is enough to prove that τ is in the image of the map

$$(\mathfrak{m}^n \cap \mathfrak{a}) \otimes_A N \to \mathfrak{a} \otimes_A N$$

for all $n \in \mathbb{N}$, or equivalently, that τ maps to 0 in $\overline{\mathfrak{a}} \otimes_A N$ where we set $\overline{\mathfrak{a}} = \mathfrak{a}/(\mathfrak{m}^n \cap \mathfrak{a})$. To this end, consider the following commutative diagram:

$$\begin{tikzcd}
\mathfrak{a} \otimes_A N \arrow[r] \arrow[d] & \overline{\mathfrak{a}} \otimes_A N \arrow[d, "\pi"] \\
N \arrow[r, "\beta"'] & \overline{A} \otimes_A N
\end{tikzcd}$$

where we set $\overline{A} = A/\mathfrak{m}^n$. We know that τ maps to 0 in $\overline{A} \otimes_A N$ by following the leftside of the diagram thus it suffices to prove that π is injective. To prove this, consider the following exact sequence

$$0 \longrightarrow \overline{\mathfrak{a}} \longrightarrow \overline{A} \longrightarrow A/(\mathfrak{a} + \mathfrak{m}^n) \longrightarrow 0$$

which induces an exact sequence

$$\mathrm{Tor}_1^A(A/(\mathfrak{a} + \mathfrak{m}^n), N) \longrightarrow \overline{\mathfrak{a}} \otimes_A N \xrightarrow{\pi} \overline{A} \otimes_A N.$$

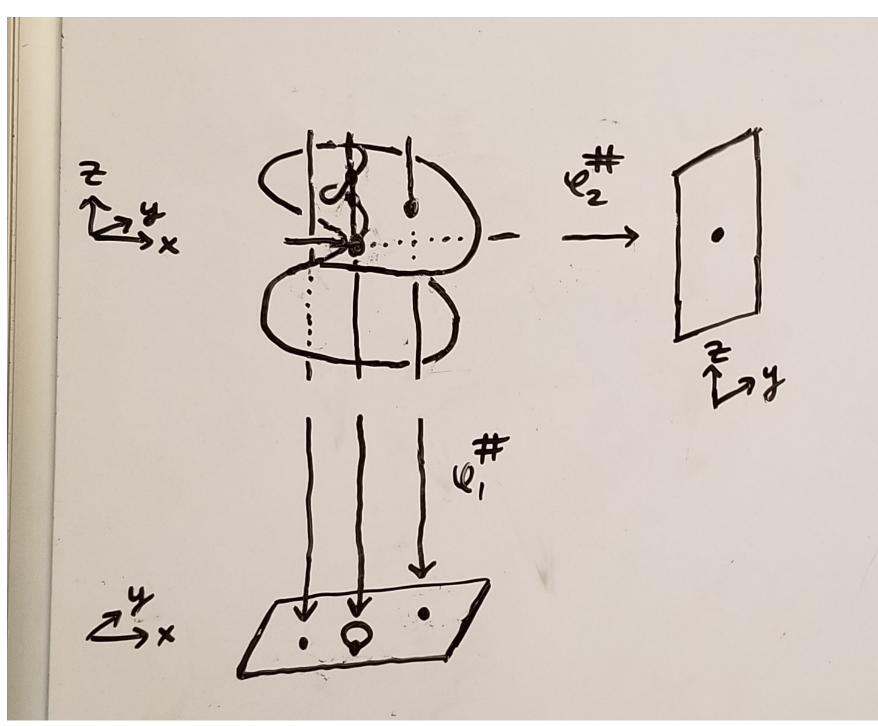
We have $\mathrm{Tor}_1^A(A/(\mathfrak{a} + \mathfrak{m}^n), N) = 0$ since $A/(\mathfrak{a} + \mathfrak{m}^n)$ is an A-module of finite length. □

52.8 Examples

Example 52.6. Let $A = K[x,y]$, $B = K[x,y,z]/\langle x - zy \rangle$, and $\varphi : A \to B$ be the map given by $\varphi(x) = x$ and $\varphi(y) = y$. Then Spec(A) corresponds tof the (x,y)-plane, and Spec(B) corresponds to the "blown up" (x,y)-plane. The map $\varphi : A \to B$, induces a map $\varphi^\# : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$. We calculate the inverse images of some points $\mathfrak{m}_{i,j} = \langle x - i, x - j \rangle$ in Max$(A) \subset$ Spec(A):

$$\begin{aligned}
\left(\varphi^\#\right)^{-1}(\mathfrak{m}_{0,0}) &= \langle x - zy, x, y \rangle = \langle x, y \rangle \\
\left(\varphi^\#\right)^{-1}(\mathfrak{m}_{1,0}) &= \langle x - zy, x - 1, y \rangle = \langle 1 \rangle = B \\
\left(\varphi^\#\right)^{-1}(\mathfrak{m}_{1,1}) &= \langle x - zy, x - 1, y - 1 \rangle = \langle x - 1, y - 1, z - 1 \rangle
\end{aligned}$$

So there is one point which maps to $\mathfrak{m}_{1,1}$, no points which maps to $\mathfrak{m}_{1,0}$, and a whole line of points which maps to $\mathfrak{m}_{0,0}$.



On the other hand, if we let $A = K[y,z]$ and $\varphi : A \to B$ be the map given by $\varphi(y) = y$ and $\varphi(z) = z$, then it's easy to see φ is a ring isomorphism.

Example 52.7. Let $A = K[y]$, $B = K[x,y]/\langle xy\rangle$, and $\varphi : A \to B$ be the map given by $\varphi(y) = y$. Then

$$\left(\varphi^{\#}\right)^{-1}(\mathfrak{m}_0) = \langle xy, y\rangle = \langle y\rangle$$
$$\left(\varphi^{\#}\right)^{-1}(\mathfrak{m}_1) = \langle xy, y-1\rangle = \langle x, y-1\rangle$$

52.9 Generic Freeness Lemma

The following result is often referred to as the "generic flatness lemma" though its conclusion is that a certain module is free, which is a stronger condition than flatness.

Theorem 52.8. *(Grothendieck's Generic Freeness Lemma) Let R be a noetherian domain, let S be a finitely generated R-algebra, and let N be a finite S-module. Then there exists a nonzero element $a \in R$ such that N_a is a free R_a-module. If in addition S is positively graded with R acting in degree 0 and N is a graded S-module, then a may be chosen so that each graded component of N_a is free over R.*

Proof. Let K be the quotient field of R. We do induction on $d := \dim(K \otimes_R S)$. In the case where $K \otimes_R S$ which we may think of as $d = -1$, there exists a nonzero $a \in R$ such that a annihilates $1 \in S$. In particular, a annihilates N, hence $N_a = 0$. Now assume $d > 0$. By Noether's normalization lemma, there exists a nonzero $c \in R$ such that S_c is module-finite over $S' := R_c[\boldsymbol{x}]$ where $\boldsymbol{x} = x_1, \dots, x_d$ are algebraically independent elements in S_c. In particular, this also implies $N' := N_c$ is a finite S'-module. Thus there exists a finite filtration of N' by S'-modules:

$$N' = N'_0 \supset N'_1 \supset \cdots \supset N'_m = 0$$

such that $N'_i/N'_{i+1} \cong S'/\mathfrak{q}_i$ where each $\mathfrak{q}_i$ is a prime ideal of S'. If $\mathfrak{q}_i \neq 0$, then $\dim(K \otimes_R (S'/\mathfrak{q}_i)) < d$, so by induction there exists an $a_i \in R$ such that $(S'/\mathfrak{q}_i)_{a_i}$ is a free R_{a_i}-module. If $\mathfrak{q}_i = 0$, then $S'/\mathfrak{q}_i = S'$ is a free R_c-module and we set $a_i = c$. Setting $a = a_0 \cdots a_{m-1}$, we see that the R_a-module N_a has a finite filtration by free R-modules and is thus free as required. If S and N are graded as above, then each $\mathfrak{q}_i$ may be taken to be homogeneous. In this case, the homogeneous components of $(S'/\mathfrak{q}_i)_a$ are free over R and the assertion follows in the graded case. $\square$

In algebraic geometry, generic flatness states that if X is an integral locally noetherian scheme, $f\colon Y \to X$ is a finite type morphism of schemes, and $\mathcal{G}$ is a coherent $\mathcal{O}_Y$-module, then there is a non-empty open subset U of X such that $\mathcal{G}|_V$ is flat over U where we set $V = f^{-1}U$.

52.10 More Flatness Results

Proposition 52.13. *Let $\phi\colon A \to B$ be a homomorphism of rings, let N and N' be finitely generated B-modules, and let $\varphi\colon N \to N'$ be a B-module homomorphism. Assume that N' is A-flat and that one of the following conditions are satisfied:*

1. *A and B are noetherian.*
2. *B is an A-algebra of finite presentation and N, N' are B-modules of finite presentation.*

Then the following assertions are equivalent:

1. *φ is injective and $N'/\varphi N$ is A-flat.*
2. *for every maximal ideal $\mathfrak{n}$ of B the morphism $\varphi \otimes 1\colon N \otimes_A \kappa(\mathfrak{p}) \to N' \otimes_A \kappa(\mathfrak{p})$ is injective where $\mathfrak{p} = \varphi^{-1}\mathfrak{n}$.*

Proposition 52.14. *(Lazard's theorem) Let A be a ring and let M be an A-module. The following assertions are equivalent:*

1. *M is A-flat.*
2. *M is a filtered colimit of finitely generated A-modules.*
3. *For every A-module L of finite presentation, then canonical map*

$$L^\vee \otimes_A M \to \operatorname{Hom}_A(L, M)$$

is surjective, where we set $L^\vee = \operatorname{Hom}_A(L, A)$.

53 Projective Modules

Definition 53.1. Let P be an R-module. We say P is **projective** if for every surjective homomorphism $\varphi\colon M \to N$ and for every homomorphism $\psi\colon P \to N$ there exists a homomorphism $\widetilde{\psi}\colon P \to M$ such that $\varphi \circ \widetilde{\psi} = \psi$. We illustrate this with the following diagram:

$$\begin{tikzcd} & P \arrow[d, "\psi"] \arrow[dl, dashed, "\widetilde{\psi}"'] \\ M \arrow[r, two heads, "\varphi"'] & N \end{tikzcd}$$

An equivalent definition of being injective is given in the following proposition:

Proposition 53.1. *Let E be an R-module. Then E is projective if and only if the covariant functor $\mathrm{Hom}_R(P, -)$ is exact.*

53.1 Properties of Projective Modules

53.1.1 Free Modules are Projective

Proposition 53.2. *Every free R-module is projective.*

Proof. Let F be a free R-module, let $\varphi\colon M \to N$ be a surjective R-module homomorphism, and let $\psi\colon F \to N$ be any R-module homomorphism. Let $\{e_i\}_{i\in I}$ be a basis for F as a free R-module. For each $i \in I$, we choose a $u_i \in M$ such that $\varphi(u_i) = \psi(e_i)$ (such a choice is possible as φ is surjective). We define $\widetilde{\psi}\colon F \to M$ to be the unique R-module homomorphism such that

$$\widetilde{\psi}(e_i) = u_i$$

for all $i \in I$. Then for all $i \in I$, we have

$$\begin{aligned}(\varphi \circ \widetilde{\psi})(e_i) &= \varphi(\widetilde{\psi}(e_i)) \\ &= \varphi(u_i) \\ &= \psi(e_i).\end{aligned}$$

It follows that $\varphi \circ \widetilde{\psi} = \psi$. □

53.1.2 Equivalent Conditions for being Projective

Proposition 53.3. *Let P be an R-module. The following statements are equivalent.*

1. *P is projective.*
2. *Every short exact sequence of the form*

$$0 \longrightarrow M \xrightarrow{\psi} N \xrightarrow{\varphi} P \longrightarrow 0 \tag{174}$$

splits.

3. *P is a direct summand of a free R-module.*

Proof. We first show 1 implies 2. Suppose P is projective. Then since $\varphi\colon N \to P$ is surjective, there exists an R-linear map $\widetilde{\varphi}\colon P \to N$ such that $\varphi \circ \widetilde{\varphi} = 1_P$. In other words, $\widetilde{\varphi}$ splits (174).

Next we show 2 implies 3. Suppose every short exact sequence of the form (174) splits. Let $\varphi\colon F \to P$ be a surjective R-linear map from a free module F to P and let K denote the kernel of this map. For instance, F could be the free module with generators δ_u for all $u \in P$, and $\varphi\colon F \to P$ could be the unique R-linear map given by $\varphi(\delta_u) = u$ for all $u \in P$. Then we have a short exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow 0$$

This short exact sequence splits by assumption, and thus we have $F \cong K \oplus P$. In other words, P is a direct summand of a free R-module.

Finally we show 3 implies 1. Suppose P is a direct summand of a free R-module, say $P \oplus K \cong F$ where F is free and K is some other R-module. Let $\pi_1\colon F \to P$ be the projection map, given by

$$\pi_1(u, v) = u$$

for all $(u,v) \in F$ and let $\iota_1 \colon P \to F$ be the inclusion map, given by

$$\iota_1(u) = (u,0)$$

for all $u \in P$. Now we want to show that P is projective, so let $\varphi \colon M \to N$ be a surjective R-linear map and let $\psi \colon P \to N$ be any other R-linear map. Since F is free, it is also projective, and so there exists an R-linear map $\phi \colon F \to M$ such that $\varphi \circ \phi = \psi \circ \pi_1$. Define $\widetilde{\psi} \colon P \to M$ by $\widetilde{\psi} = \phi \circ \iota_1$. Then

$$\begin{aligned}\varphi \circ \widetilde{\psi} &= \varphi \circ \phi \circ \iota_1 \\ &= \psi \circ \pi_1 \circ \iota_1 \\ &= \psi \circ 1_P \\ &= \psi.\end{aligned}$$

Thus P is projective. □

53.1.3 Projective Modules over Local Ring are Free

Lemma 53.1. *Every projective R-module is free if and only if every countably generated projective R-module is free.*

Lemma 53.2. *Let M be a countably generated R-module. Suppose any direct summand N of M satisfies the following property: any element of N is contained in a free direct summand of N. Then M is free.*

Proof. Let (u_n) be a countable sequence of generators for M. Note that M is a direct summand of itself. Since $u_1 \in M$, we see that it is contained in a free direct summand of M, say F_1. Write

$$M = F_1 \oplus M_1.$$

Next, M_1 is a direct summand of M. If $M_1 = 0$, then $M = F_1$ and we are done, so (by reindexing if necessary) we may assume that $u_2 \notin F_1$. Then $u_2 \in M_1$, and so it is contained in a free direct summand of M_1, say F_2. Write

$$\begin{aligned}M &= F_1 \oplus M_1 \\ &= F_1 \oplus F_2 \oplus M_2.\end{aligned}$$

Continuining in this manner, we construct a sequence of free R-modules (F_n) such that $u_n \in F_n$ for all n. In particular, we have

$$M = \bigoplus_{n=1}^{\infty} F_n.$$

Therefore F is free. □

Lemma 53.3. *Let $A = (a_{i,j})$ be an $n \times n$ matrix over a local ring $(R, \mathfrak{m})$. If $a_{i,i}$ is a unit for all i and $a_{i,j}$ is a nonunit for all $i \neq j$, then* $\det A$ *is a unit.*

Proof. The Leibniz formula for the determinant of A is given by

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Observe that if $\sigma \neq 1$, then $\prod_{i=1}^{n} a_{i,\sigma(i)} \in \mathfrak{m}$. Indeed, there exists some i such that $\sigma(i) \neq i$, and thus $a_{i,\sigma(i)} \in \mathfrak{m}$ which implies the product belongs to $\mathfrak{m}$ too. On the other hand, $\prod_{i=1}^{n} a_{i,i} \in R \backslash \mathfrak{m}$ since $R \backslash \mathfrak{m}$ is multiplicatively closed. Therefore we can express $\det A$ as a unit plus a nonunit. This implies $\det A$ is a unit. □

Lemma 53.4. *Let P be a projective module over a local ring R. Then any element of P is contained in a free direct summand of P.*

Proof. Since P is projective, it is a direct summand of some free R-module, say $F = P \oplus Q$. Let $x \in P$ be the element we wish to show is contained in a free direct summand of P. Let B be a basis of F such that the number of basis elements needed in the expression of x is minimal, say

$$x = \sum_{i=1}^{n} a_i e_i$$

for some $e_i \in B$ and $a_i \in R$. Then no a_j can be expressed as a linear combination of the other a_i. Indeed, if

$$a_j = \sum_{i \neq j} a_i b_i$$

for some $b_i \in R$, then replacing e_i by $e_i + b_i e_j$ for $i \neq j$ and leaving unchanged the other elements of B, we get a new basis for F in terms of which

$$\begin{aligned} x &= \sum_{i=1}^{n} a_i e_i \\ &= \sum_{i \neq j} a_i e_i + a_j e_j \\ &= \sum_{i \neq j} a_i e_i + \left(\sum_{i \neq j} a_i b_i \right) e_j \\ &= \sum_{i \neq j} a_i (e_i + b_i e_j) \end{aligned}$$

has a shorter expression.

For each i we decompose e_i into its P and Q-components, say

$$e_i = y_i + z_i$$

where $y_i \in P$ and $z_i \in Q$. Write

$$y_i = \sum_{j=1}^{n} b_{ij} e_j + t_i \tag{175}$$

where t_i is a linear combination of elements in B other than $e_1, \ldots, e_n$. To finish the proof it suffices to show that the matrix (b_{ij}) is invertible. For then the map $F \to F$ sending $e_i \mapsto y_i$ for $i = 1, \ldots, n$ and fixing $B \backslash \{e_1, \ldots, e_n\}$ is an isomorphism, so that $y_1, \ldots, y_n$ together with $B \backslash \{e_1, \ldots, e_n\}$ form a basis for F. Then the submodule N spanned by $y_1, \ldots, y_n$ is a free submodule of P. Furthermore N is a direct summand of P since $N \subseteq P$ and both N and P are direct summands of F. Also $x \in N$ since $x \in P$ implies

$$\begin{aligned} x &= \sum_{i=1}^{n} a_i e_i \\ &= \sum_{i=1}^{n} a_i y_i \end{aligned}$$

So N is a free direct summand of P which contains x.

Now we prove that (b_{ij}) is invertible. Plugging (175) into

$$\sum_{i=1}^{n} a_i e_i = \sum_{i=1}^{n} a_i y_i$$

and equating coefficients gives us

$$a_j = \sum_{i=1}^{n} a_i b_{ij}.$$

But as noted above, our choice of B guarantees that no a_j can be written as a linear combination of the other a_i. Thus b_{ij} is a nonunit for $i \neq j$, and $1 - b_{ii}$ is a nonunit, so in particular b_{ii} is a unit for all i. But a matrix over a local ring having units along the diagonal and nonunits elsewhere is invertible, as its determinant is a unit. □

Theorem 53.5. *If P is a projective module over a local ring, then P is free.*

53.1.4 Local Conditions for being Projective

Proposition 53.4. *Let P be a finitely presented R-module. The following are equivalent.*

1. *P is a projective R-module.*
2. *$P_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module for all prime ideals $\mathfrak{p}$ in R.*
3. *$P_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$ in R.*

Furthermore, if R is Noetherian, then these statements are also equivalent to

1. *there is a finite set of elements $a_1, \ldots, a_n \in R$ that generate the unit ideal of R such that P_{a_i} is a free R_{a_i}-module for all i.*

Proof. We first show 1 implies 2. Suppose P is a projective R-module and let $\mathfrak{p}$ be a prime ideal of R. Since P is projective, it is a direct summand of a free R-module, say $F = P \oplus Q$. Since localization commutes with direct sums, this implies $F_{\mathfrak{p}} = P_{\mathfrak{p}} \oplus Q_{\mathfrak{p}}$. Thus $P_{\mathfrak{p}}$ is a direct summand of a free $R_{\mathfrak{p}}$-module. This implies $P_{\mathfrak{p}}$ is a projective $R_{\mathfrak{p}}$-module. Since projective modules over local rings are free, we see that $P_{\mathfrak{p}}$ is free.

That 2 implies 3 is clear, so we just need to show that 3 implies 1. Suppose $P_{\mathfrak{m}}$ is a free R-module for all maximal ideals $\mathfrak{m}$ in R. To show that P is projective, we need to show that for any surjective R-linear map $\varphi\colon M \to N$, then induced R-linear map

$$\mathrm{Hom}_R(P, \varphi)\colon \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$$

is also surjective, so let $\varphi\colon M \to N$ be a surjective R-linear map. Then observe that

$$\begin{aligned}
\mathrm{Hom}_R(P, \varphi) \text{ is surjective } &\iff \mathrm{Hom}_R(P, N)/\mathrm{Hom}_R(P, M) \cong 0 \\
&\iff (\mathrm{Hom}_R(P, N)/\mathrm{Hom}_R(P, M))_{\mathfrak{m}} \cong 0 \text{ for all maximal ideals } \mathfrak{m} \subseteq R \\
&\iff \mathrm{Hom}_R(P, N)_{\mathfrak{m}}/\mathrm{Hom}_R(P, M)_{\mathfrak{m}} \cong 0 \text{ for all maximal ideals } \mathfrak{m} \subseteq R \\
&\iff \mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, N_{\mathfrak{m}})/\mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, M_{\mathfrak{m}}) \cong 0 \text{ for all maximal ideals } \mathfrak{m} \subseteq R \\
&\iff \mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, \varphi_{\mathfrak{m}}) \text{ is surjective for all maximal ideals } \mathfrak{m} \subseteq R
\end{aligned}$$

where the last if and only if is true since $P_{\mathfrak{m}}$ is free (and hence projective) for all maximal ideals $\mathfrak{m} \subseteq R$.

Now we show 4 is equivalent to 1,2, and 3 when R is Noetherian. Suppose R is Noetherian. Then since P is finite and R is Noetherian, we see that $\operatorname{supp} P$ is finite, say

$$\operatorname{supp} P = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}.$$

In particular, statement 2 is equivalent to $P_{\mathfrak{p}_i}$ being a free $R_{\mathfrak{p}_i}$-module for all $1 \le i \le m$.

□

Proposition 53.5. *Let P and N be R-modules such that P is finitely generated and projective. Then we have a canonical isomorphism*

$$\Phi_{P,N}\colon P^* \otimes_R N \simeq \mathrm{Hom}_R(P, N),$$

given by mapping $\ell \otimes n \in P^* \otimes_R N$ to the map $\varphi_{\ell,n}\colon P \to N$ defined by $\varphi_{\ell,n}(p) = \ell(p)n$ for all $p \in P$.

Proof. Let $\mathfrak{p}$ be prime of R. We have the following commutative diagram:

$$\begin{tikzcd}
(P^* \otimes_R N)_{\mathfrak{p}} \arrow[r, "(\Phi_{P,N})_{\mathfrak{p}}"] \arrow[d, "\simeq"] & \mathrm{Hom}_R(P, N)_{\mathfrak{p}} \arrow[d, "\simeq"] \\
P^*_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}} \arrow[r, "\Phi_{P_{\mathfrak{p}}, N_{\mathfrak{p}}}"] & \mathrm{Hom}_{R_{\mathfrak{p}}}(P_{\mathfrak{p}}, N_{\mathfrak{p}})
\end{tikzcd}$$

where the vertical maps are isomorphisms since P is finitely presented, and where the bottom map is an isomorphism since $P_{\mathfrak{p}}$ is free. It follows that $(\Phi_{P,N})_{\mathfrak{p}}$ is an isomorphism. Since $\mathfrak{p}$ was arbitrary, it follows that $\Phi_{P,N}$ is an isomorphism. □

53.2 Projective Dimension

Definition 53.2. Let A be a ring and M a finitely generated A-module. A **free resolution** of M is an exact sequence

$$\cdots \longrightarrow F_{k+1} \xrightarrow{\varphi_{k+1}} F_k \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \tag{176}$$

with finitely generated free A-modules F_i for $i \ge 0$. We say that a free resolution has **length** n if $F_k = 0$ for all $k > n$ and n is minimal with this property.

If $(A, \mathfrak{m})$ is a local ring, then a free resolution as above is called **minimal** if $\varphi_k(F_k) \subset \mathfrak{m}F_{k-1}$ for $k \ge 1$, and then $b_k(M) := \mathrm{rank}(F_k)$, $k \ge 0$, is called the kth **Betti number** of M.

Remark 81. What does the condition $\varphi_k(F_k) \subset \mathfrak{m}F_{k-1}$ have to do with being minimal? Let $K_i := \operatorname{Ker}(\varphi_i)$. Then (63.8.3) breaks up into exact sequences of the form

$$F_k \xrightarrow{\varphi_k} F_{k-1} \longrightarrow K_{k-2} \longrightarrow 0 \tag{177}$$

Tensoring (177) with $A/\mathfrak{m}$ gives us

$$F_k/\mathfrak{m}F_k \xrightarrow{\bar{\varphi}_k} F_{k-1}/\mathfrak{m}F_{k-1} \longrightarrow K_{k-2}/\mathfrak{m}K_{k-2} \longrightarrow 0 \tag{178}$$

The condition $\varphi_k(F_k) \subset \mathfrak{m}F_{k-1}$ forces $\dim_{A/\mathfrak{m}}(F_{k-1}/\mathfrak{m}F_{k-1}) = \dim_{A/\mathfrak{m}}(K_{k-2}/\mathfrak{m}K_{k-2}) = b_{k-1}(M)$. Applying Nakayama's lemma shows that $b_{k-1}(M)$ is the minimal number of generators of K_{k-2}.

Theorem 53.6. *Let $(A, \mathfrak{m})$ be a local Noetherian ring and M a finitely generated A-module, then M has a minimal free resolution. The rank of F_k in a minimal free resolution is independent of the resolution. If M has a minimal resolution of finite length n,*

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \tag{179}$$

and if

$$0 \longrightarrow G_m \longrightarrow G_{m-1} \longrightarrow \cdots \longrightarrow G_0 \longrightarrow M \longrightarrow 0 \tag{180}$$

is any free resolution, then $m \geq n$.

Proof. Let $u_1, \ldots, u_{s_0}$ be a minimal set of generators of M and consider the surjective map $\varphi_0 \colon F_0 := R^{s_0} \to M$ defined by

$$\varphi_0(a_1, \ldots, a_{s_0}) = \sum_{i=1}^{s_0} a_i u_i$$

for all $(a_1, \ldots, a_{s_0}) \in F_0$. Because of Nakayama's Lemma, $u_1, \ldots, u_{s_0}$ induces a basis of the vector space $M/\mathfrak{m}M$, and hence φ_0 induces an isomorphism $\overline{\varphi}_0 : F_0/\mathfrak{m}F_0 \cong M/\mathfrak{m}M$. In particular, this implies $\ker \varphi_0 \subset \mathfrak{m}F_0$. Observe that $\ker \varphi_0$ is a submodule of a finitely generated module over a Noetherian ring, hence is finitely generated. As before, we can find a surjective map $\varphi_1 \colon F_1 := R^{s_1} \to K_1$, where s_1 is the minimal number of generators of K_1. Continuing in this manner, we obtain a minimal free resolution for M. To show the invariance of the Betti numbers, we consider two minimal resolutions of M:

$$\cdots \xrightarrow{\varphi_{n+1}} F_n \longrightarrow \cdots \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0 \tag{181}$$

and

$$\cdots \xrightarrow{\psi_{n+1}} G_n \longrightarrow \cdots \xrightarrow{\psi_1} G_0 \xrightarrow{\psi_0} M \longrightarrow 0 \tag{182}$$

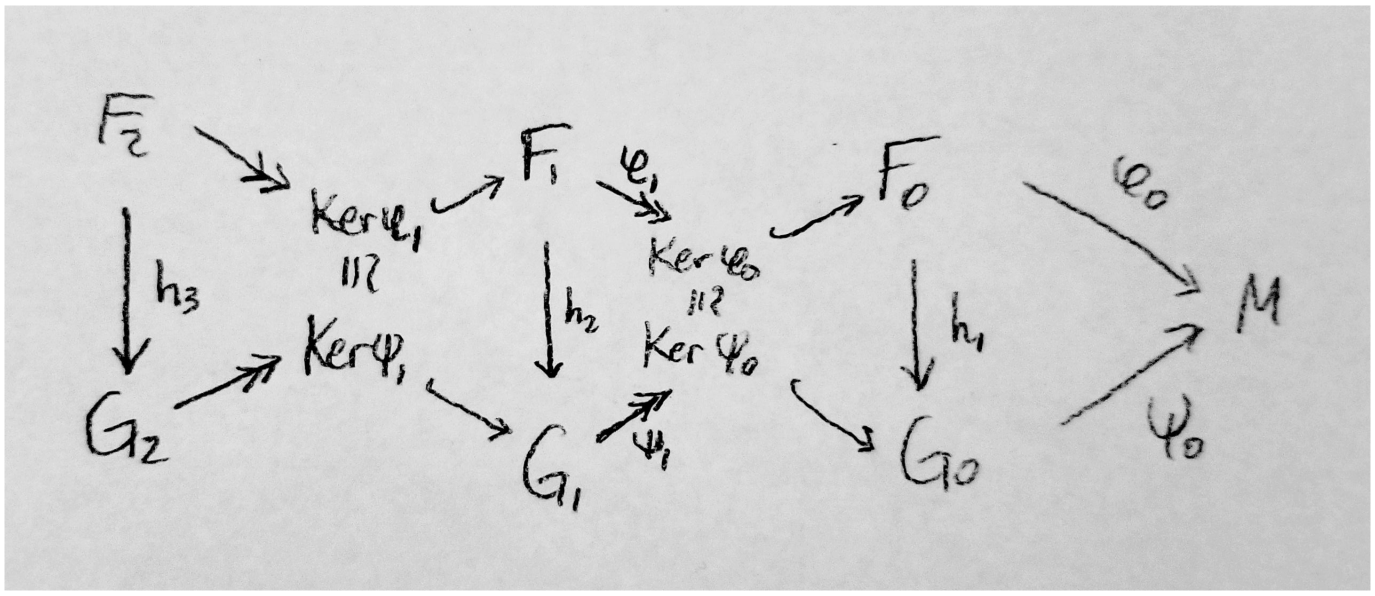
We have

$$F_0/\mathfrak{m}F_0 \cong M/\mathfrak{m}M \cong G_0/\mathfrak{m}G_0$$

and therefore $\operatorname{rank}(F_0) = \operatorname{rank}(G_0)$. Let $\{f_1, \ldots, f_{s_0}\}$, respectively $\{g_1, \ldots, g_{s_0}\}$ be bases of F_0, respectively G_0. As $\{\psi_0(g_i)\}$ generates M, we have

$$\varphi_0(f_i) = \sum_j a_{ij} \cdot \psi_0(g_j)$$

for some $a_{ij} \in R$. The matrix (a_{ij}) defines a map $\alpha_1 \colon F_0 \to G_0$ such that $\psi_0 \circ \alpha_1 = \varphi_0$. The induced map $\overline{\alpha}_1 : F_0/\mathfrak{m}F_0 \to G_0/\mathfrak{m}G_0$ is an isomorphism since it is a composition of isomorpisms: $\overline{\alpha}_1 = \overline{\psi}_0^{-1} \circ \overline{\varphi}_0$. In particular, we derive that $\det(a_{ij}) \neq 0 \bmod \mathfrak{m}$. This implies that $\det(a_{ij})$ is a unit in R (R is local ring) and α_1 is an isomorphism. Especially, α_1 induces an isomorphism $\ker \varphi_0 \to \ker \psi_0$. As φ_1 and ψ_1, considered as matrices, have entries in $\mathfrak{m}$, and since we have surjections $F_1 \to \ker \varphi_0$ and $G_1 \to \ker \varphi_0$, it follows, as before, that $\operatorname{rank}(F_1) = \operatorname{rank}(G_1)$. Now we can continue like this and obtain the invariance of the Betti numbers.



To prove the last statement, let

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \tag{183}$$

be a minimal free resolution with $F_n \neq \langle 0 \rangle$ and

$$0 \longrightarrow G_m \longrightarrow G_{m-1} \longrightarrow \cdots \longrightarrow G_0 \longrightarrow M \longrightarrow 0 \tag{184}$$

be any free resolution. We have to prove that $m \geq n$. This can be proved in a similar way to the previous step. With the same idea, one can prove that there are injections $h_i : F_i \to G_i$ for all $i \leq n$. $\square$

Definition 53.3. A **syzygy** between k elements $f_1, \ldots, f_k$ of an A-module M is a k-tuple $(g_1, \ldots, g_k) \in A^k$ satisfying

$$\sum_{i=1}^{k} g_i f_i = 0.$$

The set of syzygies between $f_1, \ldots, f_k$ is a submodule of A^k. Indeed, it is the kernel of the ring homomorphism

$$\varphi : F_1 := \bigoplus_{i=1}^{k} Ae_i \to M, \quad e_i \mapsto f_i,$$

where $\{e_1, \ldots, e_k\}$ denotes the canonical basis of A^k. The map φ surjects onto the A-module $I := \langle f_1, \ldots, f_k \rangle_A$ and

$$\operatorname{syz}(I) := \operatorname{syz}(f_1, \ldots, f_k) := \operatorname{Ker}(\varphi)$$

is called the **module of syzygies** of I with respect to the generators $f_1, \ldots, f_k$.

Example 53.1. Let $A = K[x, y, z, w]$ and let

$$f_1 = xz - y^2$$
$$f_2 = yw - z^2$$
$$f_3 = xw - yz.$$

There are three "trivial" syzygies of f_1, f_2 and f_3, which are given by the 3-tuples

$$m_1 = (f_2, -f_1, 0),$$
$$m_2 = (f_3, 0, -f_1),$$
$$m_3 = (0, f_3, -f_2),$$

but $\operatorname{syz}(f_1, f_2, f_3)$ is not generated by them. A generating set for $\operatorname{syz}(f_1, f_2, f_3)$ is given by the 3-tuples

$$n_1 = (w, y, -z)$$
$$n_2 = (z, x, -y),$$

Note that

$$f_1 = yn_1 - zn_2,$$
$$f_2 = xn_1 - yn_2,$$
$$f_3 = -zn_1 + wn_2.$$

Remark 82. Let A be a Noetherian local ring. If $I = \langle f_1, \dots, f_k \rangle = \langle g_1, \dots, g_s \rangle \subset A^r$, then it is not necessarily true that $\mathrm{syz}(f_1, \dots, f_k) \cong \mathrm{syz}(g_1, \dots, g_s)$. So why are we justified in writing $\mathrm{syz}(I)$. The reason is because the modules $\mathrm{syz}(f_1, \dots, f_k)$ and $\mathrm{syz}(g_1, \dots, g_s)$ are **projectively equivalent**. This means that $\mathrm{syz}(f_1, \dots, f_k) \oplus A^m \cong A^n \oplus \mathrm{syz}(g_1, \dots, g_s)$ for some free A-modules A^m and A^n. To prove this, we first need a lemma.

Lemma 53.7. *(Schanuel's Lemma) Let A be a Noetherian ring and M a finitely generated A-module. Moreover, assume that the following sequences are exact*

$$0 \longrightarrow K_1 \longrightarrow A^{n_1} \xrightarrow{\pi_1} M \longrightarrow 0$$

$$0 \longrightarrow K_2 \longrightarrow A^{n_2} \xrightarrow{\pi_2} M \longrightarrow 0$$

Then $K_1 \oplus A^{n_2} \cong K_2 \oplus A^{n_1}$.

Proof. Consider the A-module homomorphism $\pi \colon A^{n_1} \oplus A^{n_2} \to M$, given by $\pi(a, b) = \pi_1(a) + \pi_2(b)$. We will show that $\mathrm{Ker}(\pi) \cong A^{n_1} \oplus K_2$. A similar proof will show that $\mathrm{Ker}(\pi) \cong K_1 \oplus A^{n_2}$, and hence

$$A^{n_1} \oplus K_2 \cong \mathrm{Ker}(\pi) \cong K_1 \oplus A^{n_2}.$$

Let $e_1, \dots, e_{n_1}$ be a basis for A^{n_1} and let $f_1, \dots, f_{n_2}$ be a basis for A^{n_2}. Since π_2 is surjective, there exists $a_{ij} \in A$ such that

$$\pi_1(e_i) = \sum_{j=1}^{n_2} a_{ij} \pi_2(f_j).$$

for all $i = 1, \dots, n_1$. Choose such a_{ij} and let $\varphi \colon A^{n_1} \to A^{n_2}$ be the unique A-module homomorphism such that

$$\varphi(e_i) = \sum_{j=1}^{n_2} a_{ij} f_j$$

for all $i = 1, \dots, n_1$. Then $\pi_2 \circ \varphi = \pi_1$ and the set

$$F := \{(x, -\varphi(x)) \mid x \in A^{n_1}\}$$

is an A-module which is isomorphic to A^{n_1}. Viewing K_2 as

$$K_2 = \{(0, y) \mid y \in K_2\},$$

we see that $F \cap K_2 = \{(0, 0)\}$, so the sum $F + K_2$ is a direct sum $F \oplus K_2$. Now suppose $(x, y) \in \mathrm{Ker}(\pi)$. Then

$$\begin{aligned} 0 &= \pi_1(x) + \pi_2(y) \\ &= (\pi_2 \circ \varphi)(x) + \pi_2(y) \\ &= \pi_2(\varphi(x)) + \pi_2(y) \\ &= \pi_2(\varphi(x) + y), \end{aligned}$$

implies $\varphi(x) + y \in \mathrm{Ker}(\pi_2)$. Moreover, we can write

$$(x, y) = (x, -\varphi(x)) + (0, \varphi(x) + y) \in F \oplus K_2 \cong A^{n_1} \oplus K_2.$$

Therefore $\mathrm{Ker}(\pi) \subseteq M \oplus K_2 \cong A^{n_1} \oplus K_2$. Conversely, suppose $(x, -\varphi(x)) + (0, y) \in M \oplus K_2$. Applying π to $(x, -\varphi(x)) + (0, y)$, we have

$$\begin{aligned} \pi((x, -\varphi(x)) + (0, y)) &= \pi((x, y - \varphi(x)) \\ &= \pi_1(x) + \pi_2(y) - \pi_2(\varphi(x)) \\ &= \pi_1(x) - \pi_1(x) \\ &= 0. \end{aligned}$$

Therefore, $A^{n_1} \oplus K_2 \cong M \oplus K_2 \subseteq \mathrm{Ker}(\pi)$. We conclude that $\mathrm{Ker}(\pi) \cong A^{n_1} \oplus K_2$. $\square$

Corollary 55. *Let A be a Noetherian ring and $M = \langle f_1, \dots, f_k \rangle = \langle g_1, \dots, g_s \rangle \subset A^r$. Then $syz(f_1, \dots, f_k) \oplus A^s \cong A^r \oplus syz(g_1, \dots, g_s)$.*

53.2.1 Schanuel's Lemma

Lemma 53.8. *(Schanuel's Lemma) Let*

$$0 \longrightarrow K \xrightarrow{\iota} P \xrightarrow{\pi} M \longrightarrow 0$$

and

$$0 \longrightarrow K' \xrightarrow{\iota'} P' \xrightarrow{\pi'} M \longrightarrow 0$$

be two short exact sequences of R-modules where P and P′ are projective R-modules. Then there is an isomorphism

$$K \oplus P' \cong K' \oplus P.$$

Proof. Consider the diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r, "\iota"] \arrow[d, dashed, "\alpha"] & P \arrow[r, "\pi"] \arrow[d, dashed, "\beta"] & M \arrow[r] \arrow[d, "1_M"] & 0 \\ 0 \arrow[r] & K' \arrow[r, "\iota'"] & P' \arrow[r, "\pi'"] & M \arrow[r] & 0 \end{tikzcd}$$

Since P is projective, there is a map $\beta \colon P \to P'$ with $\pi'\beta = \pi$; that is, the right square in the diagram above commutes. A diagram chase shows that there is a map $\alpha \colon K \to K'$ making the other square commute. This commutative diagram with exact rows gives an exact sequence

$$0 \to K \xrightarrow{\theta} P \oplus K' \xrightarrow{\psi} P' \to 0$$

where $\theta \colon x \mapsto (\iota x, \alpha x)$ and $\psi \colon (u, x') \mapsto \beta u - \iota' x'$ for $x \in K$, $u \in P$, and $x' \in K'$. Exactness of this sequence is a straightforward calculation. This sequence splits because P' is projective. □

54 Associated Primes and Primary Decomposition

54.1 Radicals and Colon Ideals

54.1.1 Radical of an Ideal

Definition 54.1. Let A be a ring and let $\mathfrak{a}$ be an ideal in A. The **radical of** $\mathfrak{a}$, denoted $\sqrt{\mathfrak{a}}$, is defined to be the ideal

$$\sqrt{\mathfrak{a}} := \{a \in A \mid a^n \in I \text{ for some } n \in \mathbb{N}\}.$$

We call $\sqrt{\langle 0 \rangle}$ the **nilradical of** A.

Proposition 54.1. *Let A be a ring and let $\mathfrak{a}$ be an ideal in A. Then*

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p} \supset \mathfrak{a} \\ \textit{prime}}} \mathfrak{p}.$$

Proof. We claim that $\mathfrak{p} \supset \mathfrak{a}$ implies $\mathfrak{p} \supset \sqrt{\mathfrak{a}}$. Indeed, if $x \in \sqrt{\mathfrak{a}}$, then $x^n \in \mathfrak{a} \subset \mathfrak{p}$. But this implies $x \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Thus, we have

$$\sqrt{\mathfrak{a}} \subset \bigcap_{\substack{\mathfrak{p} \supset \mathfrak{a} \\ \text{prime}}} \mathfrak{p}.$$

For the reverse inclusion, we may assume that $\mathfrak{a} = 0$ by passing to the quotient $A/\mathfrak{a}$. Suppose that $x \in \bigcap_{\text{prime}} \mathfrak{p}$ but $x^n \neq 0$ for all $n \geq 0$. Then $A[x^{-1}]$ is nonzero and hence contains a prime ideal $\mathfrak{q}$. The preimage of $\mathfrak{q}$ in A under the natural inclusion $A \to A[x^{-1}]$ is a prime ideal which doesn't contain x. This is a contradiction. □

Proposition 54.2. *Let A be a ring and let I, J be ideals in A. Then*

1. *$\sqrt{I}$ is an ideal.*
2. *If $I \subset J$, then $\sqrt{I} \subset \sqrt{J}$.*
3. *$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*
4. *$\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.*

Proof.

1. Suppose $a \in A$ and $x, y \in \sqrt{I}$, so $x^n, y^m \in I$ for some $n, m \in \mathbb{N}$. Then
$$(ax + y)^{n+m} = \sum_{i=0}^{n+m} (ax)^{n+m-i} y^i. \tag{185}$$
Each term in (185) belongs to I, so $(ax + y)^{n+m}$ belongs to I. Therefore $ax + y$ belongs to $\sqrt{I}$.

2. Suppose $a \in \sqrt{I}$, then for some $n \in \mathbb{N}$, we have $a^n \in I \subset J$, thus $a \in \sqrt{J}$.

3. Suppose $a \in \sqrt{I \cap J}$, so $a^n \in I \cap J$ for some $n \in \mathbb{N}$. Since $a^n \in I \cap J \subset I$ and $a^n \in I \cap J \subset J$, we have $a \in \sqrt{I}$ and $a \in \sqrt{J}$. Therefore $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$. For the reverse inclusion, suppose $a \in \sqrt{I} \cap \sqrt{J}$, so $a^n \in I$ and $a^m \in J$ for some $n, m \in \mathbb{N}$. Then $a^{\max(m,n)} \in I \cap J$ implies $a \in \sqrt{I \cap J}$. Therefore $\sqrt{I \cap J} \supset \sqrt{I} \cap \sqrt{J}$.

4. The inclusion $\sqrt{I + J} \subset \sqrt{\sqrt{I} + \sqrt{J}}$ follows from the fact that $I + J \subset \sqrt{I} + \sqrt{J}$. For the reverse inclusion, suppose $a \in \sqrt{\sqrt{I} + \sqrt{J}}$. Then $a^n = b + c$, where $b^m \in I$ and $c^k \in J$ for some $n, m, k \in \mathbb{N}$. Then $(a^n)^{(m+k)} \in I + J$, and it follows that $a \in \sqrt{I + J}$. Thus $\sqrt{I + J} \supset \sqrt{\sqrt{I} + \sqrt{J}}$.

□

Remark 83. Note that we do not necessarily have $\sqrt{\bigcap_{\lambda \in \Lambda} I_\lambda} = \bigcap_{\lambda \in \Lambda} \sqrt{I_\lambda}$. Indeed, consider $I_n = \langle T^n \rangle$ in $K[T]$. Then

$$\begin{aligned} \sqrt{\bigcap_{n=1}^{\infty} \langle T^n \rangle} &= \sqrt{0} \\ &= 0 \\ &\neq \langle T \rangle. \\ &= \bigcap_{n=1}^{\infty} \langle T \rangle \\ &= \bigcap_{n=1}^{\infty} \sqrt{\langle T^n \rangle}. \end{aligned}$$

54.1.2 Colon Ideal

Definition 54.2. Let A be a ring and let I, J be ideals in A. The **colon ideal** $I : J$ is defined as:

$$I : J = \{a \in A \mid aJ \subseteq I\}$$

Remark 84. Given $a \in A$, we use the shorthand notation $I : a$ for $I : \langle a \rangle$.

Proposition 54.3. *Let A be a ring, $a, b \in A$, d be a nonzerodivisor in A, and let I, J be ideals in A. Then*

1. $(I \cap J) : a = (I : a) \cap (J : a)$,
2. $I : \langle a, b \rangle = (I : a) \cap (I : b)$,
3. $I : d = \frac{1}{d}(I \cap \langle d \rangle)$.

Proof.

1. Suppose $x \in (I \cap J) : a$, so $ax \in I \cap J$. Since $I \cap J \subset I$ and $I \cap J \subset J$, this implies $x \in I : a$ and $x \in J : a$. Therefore $(I \cap J) : f \subset (I : f) \cap (J : f)$. Now suppose $x \in (I : a) \cap (J : a)$, then $ax \in I$ and $ax \in J$, so $x \in (I \cap J) : a$, which means $(I \cap J) : f \supset (I : f) \cap (J : f)$.

2. If $x \in A$, then $x\langle a, b \rangle \subset I$ if and only if $xa \in I$ and $xb \in I$.

3. Omitted.

□

Lemma 54.1. *Let A be a ring and I_1, I_2, I_3 be ideals in A.*

1. $(I_1 \cap I_2) : I_3 = (I_1 : I_3) \cap (I_2 : I_3)$*, in particular* $I_1 : I_3 = (I_1 \cap I_2) : I_3$ *if* $I_3 \subset I_2$.
2. $(I_1 : I_2) : I_3 = I_1 : (I_2 I_3)$.
3. *If* I_1 *is prime and* $I_2 \not\subset I_1$*, then* $I_1 : I_2^j = I_1$ *for* $j \geq 1$.
4. *If* $I_1 = \bigcap_{i=1}^r \mathfrak{p}_i$ *with* $\mathfrak{p}_i$ *prime, then* $I_1 : I_2^\infty = I_1 : I_2 = \bigcap_{I_2 \not\subset \mathfrak{p}_i} \mathfrak{p}_i$.

Proof.

1. Is an easy exercise
2. $I_1 \subset I_1 : I_2^j$ is clear. Let $gI_2^j \subset I_1$. Since $I_2 \not\subset I_1$ and I_1 is radical, $I_2^j \not\subset I_1$ and we can find an $h \in I_2^j$ such that $h \notin I_1$ and $gh \in I_1$. Since I_1 is prime, we have $g \in I_1$.

□

54.2 Primary Ideals

Definition 54.3. Let A be a ring and let $Q \subset A$ be an ideal. We say Q is a **primary ideal** if for all $a, b \in A$, we have

$$ab \in Q \text{ and } a \notin Q \text{ implies } b^n \in Q \text{ for some } n \in \mathbb{N}.$$

Proposition 54.4. *Let A be a ring and let $Q \subset A$ be a primary ideal. Then $\sqrt{Q}$ is a prime ideal. Moreover, $\sqrt{Q}$ is the smallest prime ideal containing Q.*

Proof. Suppose $ab \in \sqrt{Q}$ and $a \notin \sqrt{Q}$. Then $(ab)^m = a^m b^m \in Q$ for some $m \in \mathbb{N}$. Since $a^m \notin Q$ and Q is primary, $(b^m)^n = b^{mn} \in Q$ for some $n \in \mathbb{N}$. This implies $b \in \sqrt{Q}$. This shows that $\sqrt{Q}$ is a prime ideal. To see that it is the smallest prime ideal, suppose $\mathfrak{p} \subset A$ is a prime ideal such that $Q \subset \mathfrak{p}$ and suppose $a \in \sqrt{Q}$. Then $a^n \in Q \subset \mathfrak{p}$ for some $n \in \mathbb{N}$. Since $\mathfrak{p}$ is a prime ideal, this implies $a \in \mathfrak{p}$. Therefore $\sqrt{Q} \subset \mathfrak{p}$. □

Example 54.1. The converse to Proposition (54.4) is false, that is, if $\mathfrak{a} \subset A$ is an ideal such that $\sqrt{\mathfrak{a}}$ is prime, then $\mathfrak{a}$ is not necessarily primary. Indeed, let $A = K[x, y]$ and $\mathfrak{a} = \langle x^2, xy \rangle$. Then $\sqrt{\mathfrak{a}} = \langle x \rangle$ is prime, but $\mathfrak{a}$ is not primary. We have $xy \in \mathfrak{a}$ and $x \notin \mathfrak{a}$, but no power of y belongs to $\mathfrak{a}$.

Definition 54.4. Let A be a ring and let $Q \subset A$ be a primary ideal. We denote $\mathfrak{p} := \sqrt{Q}$ and say Q is $\mathfrak{p}$**-primary**.

54.2.1 Intersection of $\mathfrak{p}$-Primary Ideals is Primary

Proposition 54.5. *Let A be a ring and let $Q_1, Q_2 \subset A$ be $\mathfrak{p}$-primary ideals. The $Q_1 \cap Q_2$ is a $\mathfrak{p}$-primary ideal.*

Proof. Suppose $ab \in Q_1 \cap Q_2$ and $a \notin Q_1 \cap Q_2$. Then either $a \notin Q_1$ or $a \notin Q_2$. Without loss of generality, assume $a \notin Q_2$. Then $b^n \in Q_2$ for some $n \in \mathbb{N}$. Since $\sqrt{Q_2} = \mathfrak{p}$, we have $b \in P$. But since $\mathfrak{p} = \sqrt{Q_1}$, we also have $b^m \in Q_1$ for some $m \in \mathbb{N}$. So $b^{\gcd(m,n)} \in Q_1 \cap Q_2$. □

Remark 85. Notice that we used the fact that these are $\mathfrak{p}$-primary ideals. If Q_1 is $\mathfrak{p}_1$-primary and Q_2 is $\mathfrak{p}_2$-primary, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are different primes, then

$$\sqrt{Q_1 \cap Q_2} = \sqrt{Q_1} \cap \sqrt{Q_2} = \mathfrak{p}_1 \cap \mathfrak{p}_2,$$

which is not a prime ideal. Hence $Q_1 \cap Q_2$ is not primary.

54.2.2 $\mathfrak{p}$-primary ideals and colon properties

Proposition 54.6. *Let R be a ring, let $\mathfrak{p}$ be a prime ideal of R, let Q be a $\mathfrak{p}$-primary ideal of R, and let $x \in R$. Then*

1. *If* $x \notin Q$*, then* $Q : x$ *is* $\mathfrak{p}$*-primary.*
2. *If* $x \notin \mathfrak{p}$*, then* $Q : x = Q$
3. *If* $x \in Q$*, then* $Q : x = R$.

Proof. 1. Suppose $x \notin Q$ and let $a, b \in R$ such that $ab \in Q : x$ and $a \notin Q : x$. We need to show that a power of b belongs to $Q : x$. Since $ab \in Q : x$, we have $abx \in Q$, and since $a \notin Q : x$, we have $ax \notin Q$. Thus $abx \in Q$ and $ax \notin Q$. This implies a power of b belongs to Q since Q is primary, but $Q \subseteq Q : x$; hence a power of b belongs to $Q : x$.

2. Suppose $x \notin \mathfrak{p}$. We want to show $Q : x = Q$. Clearly $Q : x \supseteq Q$, so it suffices to show the reverse inclusion. Let $a \in Q : x$. Then $ax \in Q$. Since $\mathfrak{p}$ is prime and $x \notin \mathfrak{p}$, we see that $x^n \notin \mathfrak{p}$ for all $n \geq 1$. This implies $a \in Q$ since Q is primary; hence $Q \subseteq Q : x$.

3. Suppose $x \in R$. If $a \in R$, then $ax \in Q$ since $x \in Q$ and Q is an ideal. Thus $R \subseteq Q : x$. The reverse inclusion is obvious. $\square$

54.2.3 *n*th Symbolic Power

Definition 54.5. Let A be a ring and let $\mathfrak{q}$ be a prime ideal in A. The ***n*th symbolic power of** $\mathfrak{q}$, denoted $\mathfrak{q}^{(n)}$, is defined to be the ideal

$$\mathfrak{q}^{(n)} = \mathfrak{q}^n A_{\mathfrak{q}} \cap A = \{a \in A \mid as \in \mathfrak{q}^n \text{ for some } s \in A \backslash \mathfrak{q}\}.$$

Proposition 54.7. *Let A be a ring and let $\mathfrak{q}$ be a prime ideal in A. Then $\mathfrak{q}^{(n)}$ is the smallest $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$.*

Proof. It is clear that $\mathfrak{q}^n \subset \mathfrak{q}^{(n)}$. Let us show that $\mathfrak{q}^{(n)}$ is a $\mathfrak{q}$-primary ideal. Suppose $ab \in \mathfrak{q}^{(n)}$ and $a \notin \mathfrak{q}^{(n)}$. Choose $s \in A\backslash\mathfrak{q}$ such that $abs \in \mathfrak{q}^n$. Since $a \in \mathfrak{q}^{(n)}$, we must not have $bs \in A\backslash\mathfrak{q}$. In particular, this implies $b \in \mathfrak{q}$ since $A\backslash\mathfrak{q}$ is multiplicatively closed. But then $b^n \in \mathfrak{q}^n \subset \mathfrak{q}^{(n)}$. Thus $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary.

Now we will show that it is the smallest $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$. Let Q be any $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$ and let $a \in \mathfrak{q}^{(n)}$. Choose $s \in A\backslash\mathfrak{q}$ such that $as \in \mathfrak{q}^n \subset Q$. Since $A\backslash\mathfrak{q}$ is multiplicatively closed and since $Q \cap A\backslash\mathfrak{q} = \emptyset$, we must have $s^m \notin Q$ for all $m \in \mathbb{N}$. This implies $a \in Q$ since Q is primary. Thus $\mathfrak{q}^{(n)} \subset Q$. $\square$

54.3 Primary Decomposition

In a Noetherian ring, any ideal can be written as a finite intersection of primary ideals (called the **primary decomposition**). Before we go over the proof, we need a definition and a lemma.

Definition 54.6. Let A be a ring and let $I \subset A$ be an ideal. We say I is **irreducible** if given two ideals $I_1, I_2 \subset A$ such that $I = I_1 \cap I_2$, then either $I = I_1$ or $I = I_2$.

Lemma 54.2. *Let A be a Noetherian ring and let $I \subset A$ be an irreducible ideal. Then I is primary.*

Proof. Suppose $ab \in I$ with $a \notin I$. There is a chain of ideals:

$$I \subset I : b \subset I : b^2 \subset \cdots$$

By the Noetherian condition we must have $I : b^n = I : b^{n+1}$ for some $n \in \mathbb{N}$. Assume $b^n \notin I$. We will show $\langle I, b^n \rangle \cap \langle I, a \rangle = I$, which is a contradiction since $b^n, a \notin I$. To show this, we only need to show $\langle b^n \rangle \cap \langle a \rangle \subset I$. Suppose $x \in \langle b^n \rangle \cap \langle a \rangle$. Then $x \in \langle a \rangle$ implies $x = ay$ and $x \in \langle b^n \rangle$ implies $x = b^n z$. Then

$$bx = b^{n+1} z = bay \in I$$

implies $z \in I : b^{n+1} = I : b^n$. Therefore $x = zb^n \in I$. $\square$

Theorem 54.3. *Let A be a Noetherian ring and let $I \subset A$ be an ideal. Then I can be expressed as a finite intersection of primary ideals.*

Proof. First, we show that I can be expressed as a finite intersection of irreducible ideals. Assume, on the contrary, that I cannot be expressed as a finite intersection of irreducible ideals. Let S be the set of all ideals which cannot be expressed as a finite intersection of irreducible ideals. Then S is nonempty since $I \in S$. Since A is noetherian, S has a maximal element J. Since $J \in S$, it must be reducible, so we can write $J = J_1 \cap J_2$ with $J \subsetneq J_1$ and $J \subsetneq J_2$. Since J is maximal, we can express J_1 and J_2 as a finite intersection of irreducible ideals, and hence we can express J as a finite intersection of irreducible ideals, which is a contradiction. Now apply Lemma 54.2. $\square$

Remark 86. It is interesting to compare this proof with the proof given in my Algebraic Number Theory notes on why every ideal in $\mathcal{O}_K$ contains a product of primes. In both cases, we needed a maximal element; one based on the index of an ideal in the ring of integers, and one based containment.

Definition 54.7. A primary decomposition $I = \bigcap\limits_{i=1}^{n} Q_i$ is **irredundant** if for each $j \in \{1, \dots, n\}$

$$\bigcap_{i \neq j} Q_i \neq I.$$

Remark 87. So there are no "extraneous" factors".

Given an irredundant primary decomposition $I = \bigcap\limits_{i=1}^{n} Q_i$, if $i \neq j$ then $\mathfrak{p}_i \neq \mathfrak{p}_j$. The reason is because if $\mathfrak{p}_i = \mathfrak{p}_j$, then by Proposition 54.5, $Q = Q_i \cap Q_j$ is a smaller primary ideal which contains I, and hence the primary decomposition for I can be replaced by removing Q_i and Q_j and replacing them with Q, which means $I = \bigcap\limits_{i=1}^{n} Q_i$ is not irredundant. So we get a picture that looks like this:

Definition 54.8. The set of **associated primes** of I, denoted by $Ass(I)$, is defined as

$$Ass(I) = \{P \subset R \mid P \text{ prime}, P = I : f \text{ for some } f \in R\}$$

Given an irredundant primary decomposition $I = \bigcap\limits_{i=1}^{n} Q_i$, we claim $P_i \in Ass(I)$: For any j, we can find $f_j \notin Q_j$ but which is in all the other Q_i for $i \neq j$. Then

$$I : f_j = \left(\bigcap_{i=1}^{n} Q_i \right) : f_j = \bigcap_{i=1}^{n} (Q_i : f_j) = Q_j : f_j$$

Thus, $I : f_j$ is P_j-primary. In particular $\sqrt{I : f_j} = \sqrt{Q_j : f_j} = P_j$. Also, if $P = I : f$ for some $f \in R$, then

$$P \supset Q_1 \cap Q_2 \cap \cdots \cap Q_n$$

Since P is a prime ideal, $P \supset Q_k$ for some $1 \leq k \leq n$. Then $P \supset P_k$ since P_k is the smallest prime ideal which contains Q_k.

Definition 54.9. An associated prime P_i which does not properly contain any other associated prime P_j is called a **minimal** associated prime. The non-minimal associated primes are called **embedded** associated primes.

Example 54.2. Let $I = \langle x^2, xy \rangle$. Clearly $I = \langle x^2, y \rangle \cap \langle x \rangle$.

$\langle x^2, xy \rangle$ $\qquad$ $\langle x^2 - x, xy \rangle$

Lemma 54.4. *(Splitting tool) Let A be a ring, $I \subset A$ an ideal, and let $I : a = I : a^2$ for some $a \in A$. Then $I = (I : a) \cap \langle I, a \rangle$.*

Proof. Since both $I : a$ and $\langle I, a \rangle$ contain I, we have $I \subset (I : a) \cap \langle I, a \rangle$. For the reverse inclusion, let $f \in (I : a) \cap \langle I, a \rangle$ and let $f = g + xa$ for some $g \in I$. Then $af = ag + xa^2 \in I$ and, therefore, $xa^2 \in I$. That is, $x \in I : a^2 = I : a$ which implies $xa \in I$ and, consequently, $f \in I$. $\square$

Example 54.3. Let $I = \langle xy^2, y^3 \rangle$. Then $I : x = \langle y^2 \rangle = I : x^2$. Therefore, $I = \langle y^2 \rangle \cap \langle x, y^3 \rangle$.

Example 54.4. Let $I = \langle wx, wy, wz, vx, vy, vz, ux, uy, uz, y^3 - x^2 \rangle$. Then $I : w = \langle x, y, z \rangle = I : w^2$. Therefore $I = \langle x, y, z \rangle \cap I_1$ where $I_1 = \langle w, vx, vy, vz, ux, uy, uz, y^3 - x^2 \rangle$. Then $I_1 : v = \langle w, x, y, z \rangle = I_1 : v^2$, and so $I_1 = \langle w, x, y, z \rangle \cap I_2$ where $I_2 = \langle w, v, ux, uy, uz, y^3 - x^2 \rangle$. Finally, $I_2 : u = \langle w, v, x, y, z \rangle = I_2 : u^2$, and so $I_2 = \langle w, v, x, y, z \rangle \cap \langle w, v, u, y^3 - x^2 \rangle$. So $I = \langle x, y, z \rangle \cap \langle w, x, y, z \rangle \cap \langle w, v, x, y, z \rangle \cap \langle w, v, u, y^3 - x^2 \rangle = \langle x, y, z \rangle \cap \langle w, v, u, y^3 - x^2 \rangle$.

Example 54.5. Let $A = K[x, y, z, w]$. The twisted cubic is the set-theoretic intersection of $xz - y^2$ and $z(yw - z^2) - w(xw - yz)$, but it is not a sheme-theoretic or ideal-theoretic complete intersection. To get a sense of why this is, we compute a primary decomposition of $I = \langle xz - y^2, z(yw - z^2) - w(xw - yz) \rangle$. Using Singular, we see that I is $\mathfrak{p}$-primary where $\mathfrak{p} = \langle xz - y^2, yw - z^2, xw - yz \rangle$, and thus $\sqrt{I} = \mathfrak{p}$. Therefore $\mathbf{V}(I) = \mathbf{V}(\mathfrak{p})$. On the other hand, $I \subsetneq \mathfrak{p}$.

Definition 54.10. Let A be a Noetherian ring and let I be an ideal in A.

1. The set of **associated primes** of I, denoted by $\mathrm{Ass}(I)$, is defined as

$$\mathrm{Ass}(I) = \{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ is prime and } \mathfrak{p} = I : a \text{ for some } a \in A\}.$$

   Elements of $\mathrm{Ass}(\langle 0 \rangle)$ are also called **associated primes** of A.

2. Let $\mathfrak{p}, \mathfrak{q} \in \mathrm{Ass}(I)$ and $\mathfrak{q} \subset \mathfrak{p}$. Then $\mathfrak{p}$ is called an **embedded prime ideal** of I. We define $\mathrm{Ass}(I, \mathfrak{p}) := \{\mathfrak{q} \mid \mathfrak{q} \in \mathrm{Ass}(I) \text{ and } \mathfrak{q} \subset \mathfrak{p}\}$.

3. I is called **equidimensional** or **pure dimensional** if all associated primes of I have the same dimension.

4. I is a **primary ideal** if, for any $a, b \in A$, $ab \in I$, and $a \notin I$, then $b \in \sqrt{I}$. Let $\mathfrak{p}$ be a prime ideal. Then a primary ideal I is called $\mathfrak{p}$-primary if $\mathfrak{p} = \sqrt{I}$.

5. A **primary decomposition** of I, that is, a decomposition $I = Q_1 \cap \cdots \cap Q_s$ with Q_i primary ideals, is called **irredundant** if no Q_i can be omitted in the decomposition and if $\sqrt{Q_i} \neq \sqrt{Q_j}$ for all $i \neq j$.

54.4 Examples

Example 54.6. Let $A = K[x, y]$ and $I = \langle x^2, xy \rangle$. Then a primary decomposition of I is given by $I = I_1 \cap I_2$, where

$$I_1 = \langle x^2, y \rangle \qquad \sqrt{I_1} = \langle x, y \rangle$$
$$I_2 = \langle x \rangle \qquad \sqrt{I_2} = \langle x \rangle$$

Example 54.7. Let $A = K[x, y, u, v]$ and $I = \langle xu, xv, yu, yv \rangle$. Then a primary decomposition of I is given by $I = I_1 \cap I_2$, where

$$I_1 = \langle x, y \rangle \qquad \sqrt{I_1} = \langle x, y \rangle$$
$$I_2 = \langle u, v \rangle \qquad \sqrt{I_2} = \langle u, v \rangle$$

Example 54.8. Let $A = K[x, y, u, v]$ and $I = \langle xu, yv, xv + yu \rangle$. Then a primary decomposition of I is given by $I = I_1 \cap I_2 \cap I_3$, where

$$I_1 = \langle x, y \rangle \qquad \sqrt{I_1} = \langle x, y \rangle$$
$$I_2 = \langle u, v \rangle \qquad \sqrt{I_2} = \langle u, v \rangle$$
$$I_3 = \langle x^2, xy, xu, yu + xv, y^2, yv, u^2, uv, v^2 \rangle \qquad \sqrt{I_3} = \langle x, y, u, v \rangle$$

Example 54.9. Let $A = K[x, y, u, v]$ and $I = \langle xu + yv, xv + yu \rangle$. Then a primary decomposition of I is given by $I = I_1 \cap I_2 \cap I_3 \cap I_4$, where=

$$I_1 = \langle x, y \rangle \qquad \sqrt{I_1} = \langle x, y \rangle$$
$$I_2 = \langle u, v \rangle \qquad \sqrt{I_2} = \langle u, v \rangle$$
$$I_3 = \langle x + y, u - v \rangle \qquad \sqrt{I_3} = \langle x + y, u - v \rangle$$
$$I_4 = \langle x - y, u + v \rangle \qquad \sqrt{I_4} = \langle x - y, u + v \rangle$$

Example 54.10. Let $R = K[x, y]$ and let $I = \langle x^2 - xy, xy^2 - xy \rangle$. Using Singular, we calculate

Ring	$R = K[x, y]$
Ideal	$I = \langle x^2 - xy, xy^2 - xy \rangle$
Minimal Associated Primes	$\operatorname{MinAss} I = \{\langle x \rangle, \langle x-1, y-1 \rangle\}$
Associated Primes	$\operatorname{Ass} I = \{\langle x \rangle, \langle x, y \rangle, \langle x-1, y-1 \rangle\}$
Primary Decomposition	$I = \langle x \rangle \cap \langle x^2, y \rangle \cap \langle x-1, y-1 \rangle$

Now observe that $\dim I = 1$ and $y-1$ belongs to a minimal associated prime of I, yet $\dim(\langle I, y-1 \rangle) = 0$. On the other hand, x also belongs to a minimal associated prime of I, and $\dim(\langle I, x \rangle) = 1$. The difference between $y-1$ and x here is that $y-1$ belongs to the minimal associated prime $\langle x-1, y-1 \rangle$ whereas x belongs to the minimal associated prime $\langle x \rangle$.

Now if we localize at the maximal ideal $\mathfrak{m} = \langle x, y \rangle$, then the table above transforms as follows:

Ring	$R_{\mathfrak{m}} = K[x, y]_{\langle x, y \rangle}$
Ideal	$I_{\mathfrak{m}} = \langle x^2, xy \rangle$
Minimal Associated Primes	$\operatorname{MinAss} I = \{\langle x \rangle\}$
Associated Primes	$\operatorname{Ass} I = \{\langle x \rangle, \langle x, y \rangle\}$
Primary Decomposition	$I = \langle x \rangle \cap \langle x^2, y \rangle$

What happened here is that we now have $\langle x-1, y-1 \rangle_{\mathfrak{m}} = R_{\mathfrak{m}}$, since both $x-1$ and $y-1$ are units. Thus it is becomes an irrelevant factor.

54.5 Associated Primes

Definition 54.11. Let $\mathfrak{p}$ be a prime ideal of R and let M be an R-module.

1. We say $\mathfrak{p}$ is **weakly associated** to M if there exists an element $m \in M$ such that $\mathfrak{p}$ is minimal among the prime ideals containing the annihilator $0 : m = \{r \in R \mid rm = 0\}$. The set of all such primes is denoted $\operatorname{WeakAss} M$.

2. We say $\mathfrak{p}$ is **associated** to M if there exists an element $m \in M$ such that $\mathfrak{p}$ is equal to the annihilator $0 : m$. The set of all such primes is denoted $\operatorname{Ass} M$.

It turns out that the union of all weakly associated primes of R is precisely the set of all zerodivisors of R.

Proposition 54.8. *Let R be a commutative ring with identity. Then the set of all zerodivisors of R is given by the set*

$$\bigcup_{\mathfrak{p} \in \operatorname{WeakAss} R} \mathfrak{p}.$$

Proof. Suppose $x \in R$ is a zerodivisor. Choose $y \neq 0$ such that $xy = 0$. Then $0 : y$ is a proper ideal of R. Choose a minimal prime $\mathfrak{p}$ over $0 : y$. Then $\mathfrak{p}$ is a weakly associated prime to R and $x \in \mathfrak{p}$ implies

$$\{\text{set of zerodivisors of } R\} \subseteq \bigcup_{\mathfrak{p} \in \operatorname{WeakAss} R} \mathfrak{p}.$$

Conversely, suppose $x \in \bigcup_{\mathfrak{p} \in \operatorname{WeakAss} R} \mathfrak{p}$. Then $x \in \mathfrak{p}$ for some prime $\mathfrak{p}$ which is weakly associated to R. Since $\mathfrak{p}$ is weakly associated to R, there exists a $y \in R$ such that $\mathfrak{p}$ is a minimal prime over $0 : y$. Since localization is exact, we see that $\mathfrak{p}_{\mathfrak{p}}$ is a weakly associated prime to $R_{\mathfrak{p}}$, with $\mathfrak{p}_{\mathfrak{p}}$ being minimal over $0 : (y/1)$. Since $R_{\mathfrak{p}}$ is local and $\mathfrak{p}_{\mathfrak{p}}$ is minimal over the annihilator $0 : (y/1)$, we have $\operatorname{rad}(0 : (y/1)) = \mathfrak{p}_{\mathfrak{p}}$. In particular, there exists $n \in \mathbb{N}$ and a $z \in R \backslash \mathfrak{p}$ such that $x^n z \in 0 : y$, or in other words, such that $x^n yz = 0$. Note that $yz \neq 0$ as $z \notin \mathfrak{p}$, so if $n = 1$, then $xyz = 0$ implies x is a zerodivisor. Assume $n > 1$. Choose $m \in \mathbb{N}$ such that $m \leq n$ and $x^m yz = 0$ and $x^{m-1} yz \neq 0$. Then $x(x^{m-1} yz) = x^m yz = 0$ implies x is a zerodivisor. Thus

$$\{\text{set of zerodivisors of } R\} \supseteq \bigcup_{\mathfrak{p} \in \operatorname{WeakAss} R} \mathfrak{p}.$$

$\square$

Corollary 56. *Assume that R is a zero-dimensional ring. Then any nonunit of R is a zerodivisor.*

Proof. We have

$$\begin{aligned}\{\text{set of zerodivisors of } R\} &= \bigcup_{\mathfrak{p}\in \operatorname{WeakAss} R} \mathfrak{p} \\ &= \bigcup_{\mathfrak{p}\in \operatorname{Spec} R} \mathfrak{p} \\ &= \{\text{nonunits of } R\},\end{aligned}$$

where we obtained the second line from the first line from the fact that R is 0-dimensional. Indeed, clearly we have

$$\bigcup_{\mathfrak{p}\in \operatorname{WeakAss} R} \mathfrak{p} \subseteq \bigcup_{\mathfrak{p}\in \operatorname{Spec} R} \mathfrak{p}.$$

Conversely, suppose $\mathfrak{p}$ is a prime ideal of R and choose $x \notin \mathfrak{p}$. Then since $x \in \mathfrak{p}$ and $\mathfrak{p}$ is prime we have $\mathfrak{p} \supseteq 0 : x$ and since R is 0-dimensional we see that $\mathfrak{p}$ is minimal over $0 : x$. Thus $\mathfrak{p}$ is a weakly associated prime to R. It follows that

$$\bigcup_{\mathfrak{p}\in \operatorname{WeakAss} R} \mathfrak{p} \supseteq \bigcup_{\mathfrak{p}\in \operatorname{Spec} R} \mathfrak{p}.$$

□

Clearly, every associated prime of R is a weakly associated prime of R. If R is Noetherian, then the converse holds as well:

Proposition 54.9. *Assume R is Noetherian. Let M be a finitely generated R-module and let $\mathfrak{p}$ be a weakly associated prime of M. Then $\mathfrak{p}$ is an associated prime of M.*

Proof. Choose $u \in M$ such that $\mathfrak{p}$ is minimal over $0 : u$. Since R is Noetherian, we can express $0 : u$ in terms of an irredundant primary decomposition, say

$$0 : u = Q_1 \cap Q_2 \cap \cdots \cap Q_r.$$

The prime $\mathfrak{p}$ must me minimal over one of the Q_i's, say $\mathfrak{p}$ is minimal over Q_1. Since the decomposition of $0 : u$ is irredundant, we can choose $x \in R$ such that $x \notin Q_1$ and $x \in Q_j$ for $j = 2, \dots, r$. Now observe that=

$$\begin{aligned}0 : xu &= (0 : u) : x \\ &= (Q_1 \cap Q_2 \cap \cdots \cap Q_r) : x \\ &= (Q_1 : x) \cap (Q_2 : x) \cap \cdots \cap (Q_r : x) \\ &= Q \cap R \cap \cdots \cap R \\ &= Q,\end{aligned}$$

where we set $Q = Q_1 : x$. Note that Q is $\mathfrak{p}$-primary ideal, and in particular we have $\sqrt{Q} = \mathfrak{p}$. If $Q \neq \mathfrak{p}$, then we choose $x_1 \in \mathfrak{p}\backslash Q$ and $n_1 \geq 2$ minimal such that $x_1^{n_1} \in Q$. Then observe that

$$Q \subset Q : x_1 \subseteq \mathfrak{p}$$

where the inclusion on the left is strict since $x_1^{n_1-1} \in Q : x_1$ but $x_1^{n_1-1} \notin Q$. If $Q : x_1 \neq \mathfrak{p}$, then we choose $x_2 \in \mathfrak{p}\backslash(Q : x_1)$ and $n_2 \geq 2$ minimal such that $x_2^{n_2} \in Q : x_1$. Then observe that

$$Q \subset Q : x_1 \subset Q : x_1x_2 \subseteq \mathfrak{p}$$

where we are using the fact that $(Q : x_1) : x_2 = Q : x_1x_2$. Continuing in this manner, we obtain an ascending sequence of ideals

$$Q \subset Q : x_1 \subset Q : x_1x_2 \subset \cdots \subset Q : x_1x_2\cdots x_i \subset \cdots \mathfrak{p}.$$

This sequence must terminate since R is Noetherian, say at $Q : x_1x_2\cdots x_n$. In particular, we must have $\mathfrak{p} = Q : x_1x_2\cdots x_n$. In particular, we have

$$\begin{aligned}0 : xx_1x_2\cdots x_nu &= (0 : xu) : x_1x_2\cdots x_n \\ &= Q : x_1x_2\cdots x_n \\ &= \mathfrak{p}.\end{aligned}$$

It follows that $\mathfrak{p}$ is an associated prime of M. □

Theorem 54.5. *Let A be a Noetherian ring and let M be a finitely generated A-module.*

1. $\operatorname{Ass}(M)$ *is a finite, nonempty set of primes, each containing $Ann(M)$. The set $Ass(M)$ includes all primes minimal among primes containing $Ann(M)$.*

2. *The union of associated primes of M consists of 0 and the set of zerodivisors on M.*

3. *The formation of the set $Ass(M)$ commutes with localization at an arbitrary multiplicately closed set, in the sense that*
$$Ass_{S^{-1}A}(S^{-1}M) = \{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in Ass(M) \text{ and } \mathfrak{p} \cap S = \emptyset\}.$$

Lemma 54.6. *(Prime Avoidance) If $I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, with $\mathfrak{p}_i$ prime, then $I \subseteq \mathfrak{p}_i$ for some i.*

Proof. We prove the contrapositive: $I \not\subseteq \mathfrak{p}_i$ for all i implies $I \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Induct on n, the base case is trivial. We now suppose that $I \not\subseteq \mathfrak{p}_i$ for all i and $I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, and arrive at a contradiction. From our inductive hypothesis, for each i, $I \not\subseteq \bigcup_{j\neq i} \mathfrak{p}_j$. In particular, for each i there is an x_i which is in I but is not in $\bigcup_{j\neq i} \mathfrak{p}_j$. Notice that if $x_i \notin \mathfrak{p}_i$ then $x_i \notin \bigcup_{j=1}^n \mathfrak{p}_j$, and we have an immediate contradiction. So suppose for every i that $x_i \in \mathfrak{p}_i$. Consider the element
$$x = \sum_{i=1}^n x_1 \cdots \hat{x}_i \cdots x_n.$$
By construction, $x \in I$. We claim that $x \notin \bigcup_{i=1}^n \mathfrak{p}_i$. To see this, observe that $x_1 \cdots \hat{x}_i \cdots x_n \notin \mathfrak{p}_i$, because for each index $k \neq i$, x_k is not in $\bigcup_{j\neq k} \mathfrak{p}_j$, so in particular is not in $\mathfrak{p}_i$. Since $\mathfrak{p}_i$ is prime, this proves that $x_1 \cdots \hat{x}_i \cdots x_n \notin \mathfrak{p}_i$. But every other monomial of x is in $\mathfrak{p}_i$, since every other monomial contains x_i. This shows that $x \notin \mathfrak{p}_i$ for any i, hence $x \notin \bigcup_{j=1}^n \mathfrak{p}_j$, a contradiction. □

Finitely generated modules over Noetherian rings are distinguished for two reasons:

1. Every zerodivisor of M is contained in an associated prime ideal: Let x be a nonzerodivisor of M. This means there is a nonzero $m \in M$ such that $xm = 0$. Then x belongs to the ideal $0 : m = \{a \in A \mid am = 0\}$. In a Noetherian ring, we have primary decomposition. So
$$x \in 0 : m = Q_1 \cap Q_2 \cap \cdots \cap Q_k \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_k$$
where each $\mathfrak{p}_i = (0 : m) : d_i = 0 : d_i m$ for some $d_i \in A$. That is, each $\mathfrak{p}_i$ is an associated prime ideal of M.

2. The number of associated prime ideals of M is finite. So if I is an ideal which consists of zero-divisors of M, then
$$I \subseteq \bigcup_{\mathfrak{p}\in \operatorname{Ass}(M)} \mathfrak{p}.$$
and by the Lemma (55.1), we must have $I \subseteq \mathfrak{p}_i$ for some i. Writing $\mathfrak{p}_i = 0 : m_i$, the assignment $1 \mapsto m_i$ induces a non-zero homomorphism $\varphi : A/I \to M$.

Example 54.11. Let $R = \Bbbk[x,y]$ and let $M = \Bbbk[x,y]/\langle xy\rangle$. Then $\operatorname{Ass} M = \{\langle x\rangle, \langle y\rangle\}$ and $\operatorname{Supp} M = \operatorname{V}(xy)$. Clearly $\operatorname{Supp} M$ is much bigger than $\operatorname{Ass} M$. For example, $\langle x-a, y\rangle \in \operatorname{Supp} M$ but $\langle x-a, y\rangle \notin \operatorname{Ass} M$ for all $a \in \Bbbk$. Now consider the filtration
$$M = M_0 \supset M_1 \supset M_2 \supset M_3 = 0,$$
where $M_1 = \langle x,y\rangle/\langle xy\rangle$ and where $M_2 = \langle x\rangle/\langle xy\rangle$. The cyclic factors of this filtration are
$$\begin{aligned} M/M_1 &\cong \Bbbk[x,y]/\langle x,y\rangle, \\ M_1/M_2 &\cong \Bbbk[x,y]/\langle x\rangle, \\ M_2/M_3 &\cong \Bbbk[x,y]/\langle y\rangle. \end{aligned}$$
Note we could consider the smaller filtration instead:
$$M = M_0 \supset M_2 \supset M_3 = 0.$$
In this case, the cyclic factors would be
$$\begin{aligned} M/M_2 &\cong \Bbbk[x,y]/\langle x\rangle \\ M_2/M_3 &\cong \Bbbk[x,y]/\langle y\rangle. \end{aligned}$$

Example 54.12. Let R be a noetherian ring and let I be an ideal of R. What does a filtration of R/I look like? Choose a sequence $r_1, \dots, r_n \in R$ and let

$$I_k = I_{k-1}, r_k \quad \text{and} \quad \mathfrak{p}_k = I_{k-1} : r_k$$

for each $1 \leq k \leq n$. By replacing $r_1, \dots, r_n$ with another sequence if necessary, we may choose the r_k such that $I_k \supset I_{k-1}$ and $\mathfrak{p}_k$ is prime. If I_n is prime, then

$$R/I \supset I_n/I \supset \cdots \supset I_1/I \supset I_0/I = 0,$$

is a filtration of R/I whose factors are $R/\mathfrak{p}_1, \dots, R/\mathfrak{p}_n, R/I_n$. Furthermore, every filtration of R/I arises this way. In particular, associated primes of R/I are of the form $I : r$ for some $r \in R$, whereas as primes which occur in a filtration of R/I are of the form $I, r_1, \dots, r_k \colon r_{k+1}$ for some $r_1, \dots, r_k, r_{k+1} \in R$.

Example 54.13. Let R be a noetherian ring and let M be a nonzero finitely generated R-module. We give a procedure on constructing a filtration of M as follows: we begin with an associated prime $\mathfrak{p}_1$ of M. Thus we have a short exact sequence

$$0 \longrightarrow R/\mathfrak{p}_1 \rightarrowtail M \twoheadrightarrow N_1 \longrightarrow 0 \tag{186}$$

and we set $M_1 = \ker(M \to N_1) \cong R/\mathfrak{p}_1$. If $N_1 = 0$, then we are done, otherwise let $\mathfrak{p}_2$ be an associated prime of N_1. Thus we have a short exact sequence

$$0 \longrightarrow R/\mathfrak{p}_2 \rightarrowtail N_1 \twoheadrightarrow N_2 \longrightarrow 0 \tag{187}$$

and we set $M_2 = \ker(M \twoheadrightarrow N_1 \twoheadrightarrow N_2)$. Note that

$$\begin{aligned} M_2/M_1 &= \ker(M \twoheadrightarrow N_1 \twoheadrightarrow N_2)/\ker(M \twoheadrightarrow N_1) \\ &= \ker(N_1 \twoheadrightarrow N_2) \\ &\cong R/\mathfrak{p}_2. \end{aligned}$$

If $N_2 = 0$ then we are done, otherwise we proceed inductively. At the kth step, we let $\mathfrak{p}_k$ be an associated prime of N_{k-1}, so that we have a short exact sequence

$$0 \longrightarrow R/\mathfrak{p}_k \rightarrowtail N_{k-1} \twoheadrightarrow N_k \longrightarrow 0 \tag{188}$$

and we set $M_k = \ker(M \twoheadrightarrow N_{k-1} \twoheadrightarrow N_k)$ and note that

$$\begin{aligned} M_k/M_{k-1} &= \ker(M \twoheadrightarrow N_{k-1} \twoheadrightarrow N_k)/\ker(M \twoheadrightarrow N_{k-1}) \\ &= \ker(N_{k-1} \twoheadrightarrow N_k) \\ &\cong R/\mathfrak{p}_k. \end{aligned}$$

This procedure will eventually terminate into finite filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_{k-1} \subset M_k \subset \cdots \subset M_{m-1} \subset M_m = M,$$

where $M_k/M_{k-1} \cong R/\mathfrak{p}_k$.

Definition 54.12. Let M be a finitely generated R-module. We say M is **clean** if it admits a filtration such that the primes which occur in that filtration are precisely the associated primes of M.

Example 54.14. Let $R = \Bbbk[x_1, x_2, x_3, x_4, x_5, x_6] = \Bbbk[\boldsymbol{x}]$ and let $I = \langle x_1^2, x_1x_2, x_2x_3, x_3x_4, x_4x_5, x_5x_6, x_6^2 \rangle$. An irredundant primary decomposition of I is given by $I = Q_1 \cap Q_2 \cap Q_3 \cap Q_4 \cap Q_5$ where

$$\begin{array}{lll} Q_1 = \langle x_1, x_3, x_4, x_6 \rangle & \mathfrak{p}_1 = \langle x_1, x_3, x_4, x_6 \rangle & r_1 = x_2x_5 \\ Q_2 = \langle x_1^2, x_2, x_4, x_6 \rangle & \mathfrak{p}_2 = \langle x_1, x_2, x_4, x_6 \rangle & r_2 = x_1x_3x_5 \\ Q_3 = \langle x_1, x_3, x_5, x_6^2 \rangle & \mathfrak{p}_3 = \langle x_1, x_3, x_5, x_6 \rangle & r_3 = x_2x_4x_6 \\ Q_4 = \langle x_1^2, x_2, x_4, x_5, x_6 \rangle & \mathfrak{p}_4 = \langle x_1, x_2, x_4, x_5, x_6 \rangle & r_5 = x_1x_3x_6 \\ Q_5 = \langle x_1^2, x_2, x_3, x_5, x_6^2 \rangle & \mathfrak{p}_5 = \langle x_1, x_2, x_3, x_5, x_6 \rangle & r_5 = x_1x_4x_6 \end{array}$$

where $\mathfrak{p}_i = I : r_i$ for all i.

Example 54.15. Let $R = \Bbbk[x,y,z,w]$ and let $I = \langle x^2, w^2, zw, xy, yz\rangle$. An irredundant primary decomposition of I is given by $I = Q_1 \cap Q_2 \cap Q_3$ where

$$\begin{aligned} Q_1 &= \langle x, z, w^2\rangle & \mathfrak{p}_1 &= \langle x,z,w\rangle & r_1 &= yw \\ Q_2 &= \langle x^2, y, w\rangle & \mathfrak{p}_2 &= \langle x,y,w\rangle & r_2 &= xz \\ Q_3 &= \langle x^2, y, z, w^2\rangle & \mathfrak{p}_3 &= \langle x,y,z,w\rangle & r_3 &= xw \end{aligned}$$

where $\mathfrak{p}_i = I : r_i$ for all i. We set $I_0 = I$ and for $1 \leq k \leq 3$ we set $I_k = \langle I_{k-1}, r_k\rangle$. In particular, note that

Proposition 54.10. *Let*

$$0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then

$$\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$$

Proof. We first show $\mathrm{Ass}(M') \subset \mathrm{Ass}(M)$. Let $\mathfrak{p} \in \mathrm{Ass}(M')$. Choose $u' \in M'$ such that $\mathfrak{p} = 0 : u'$. We claim that $\mathfrak{p} = 0 : \varphi(u')$. Indeed, if $a \in \mathfrak{p}$, then

$$\begin{aligned} a\varphi(u') &= \varphi(au') \\ &= \varphi(0) \\ &= 0 \end{aligned}$$

implies $a \in 0 : \varphi(u')$ and hence $\mathfrak{p} \subset 0 : \varphi(u')$. Conversely, if $a \in 0 : \varphi(u')$, then

$$\begin{aligned} 0 &= a\varphi(u') \\ &= \varphi(au') \end{aligned}$$

implies $au' = 0$ since φ is injective, which implies $a \in \mathfrak{p}$ since $\mathfrak{p} = 0 : u'$. Therefore $\mathfrak{p} \supset 0 : \varphi(u')$, and so $\mathfrak{p} \in \mathrm{Ass}(M)$. This implies $\mathrm{Ass}(M') \subset \mathrm{Ass}(M)$.

We now show $\mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$. Let $\mathfrak{p} \in \mathrm{Ass}(M)$. Choose $u \in M$ such that $\mathfrak{p} = 0 : u$.

Case 1: Assume that $Ru \cap M' \neq 0$. Choose an a nonzero element in $Ru \cap M'$, say au for some $a \in R$. Since $au \neq 0$, we must have $a \notin \mathfrak{p}$ since $0 : u = \mathfrak{p}$. Thus

$$\begin{aligned} 0 : au &= (0 : u) : a \\ &= \mathfrak{p} : a \\ &= \mathfrak{p}, \end{aligned}$$

which implies $\mathfrak{p} \in \mathrm{Ass}(M')$, hence $\mathrm{Ass}(M) \subset \mathrm{Ass}(M')$.

Case 2: Assume that $Ru \cap M' = 0$. We claim that $\mathfrak{p} = 0 : \psi(u)$. First note that $\mathfrak{p} \subset 0 : \psi(u)$ follows from the argument above, so it suffices to show $\mathfrak{p} \supset 0 : \psi(u)$. Let $a \in 0 : \psi(u)$. Then

$$\begin{aligned} 0 &= a\psi(u) \\ &= \psi(au) \end{aligned}$$

implies $au \in \ker\psi = M'$. Since $Ru \cap M' = 0$, this implies $au = 0$, and consequently $a \in \mathfrak{p}$. It follows that $\mathfrak{p} \supset 0 : \psi(u)$. □

Proposition 54.11. *Let R be a Noetherian ring and let M be a finitely-generated R-module. Then there exists a finite filtration*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_k = M$$

such that the successive quotients M_{i+1}/M_i are isomorphic to various $R/\mathfrak{p}_i$ with the $\mathfrak{p}_i \subset R$ prime.

Proof. Let $M' \subset M$ be maximal among submodules for which such a filtration (ending with M') exists. We would like to show that $M' = M$. Now M' is well-defined since 0 has such a filtration and M is Noetherian.

There is a filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_l = M' \subset M$$

where the successive quotients, *except* possibly the last M/M', are of the form $R/\mathfrak{p}_i$ for $\mathfrak{p}_i$ prime. If $M' = M$, we are done. Otherwise, consider the quotient $M/M' \neq 0$. There is an associated prime of M/M'. So there is a prime $\mathfrak{p}$ which is the annihilator of $x \in M/M'$. This means that there is an injection

$$R/\mathfrak{p} \hookrightarrow M/M'.$$

Now, take M_{l+1} as the inverse image in M of $R/\mathfrak{p} \subset M/M'$. Then we can consider the finite filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_{l+1},$$

all of whose successive quotients are of the form $R/\mathfrak{p}_i$; this is because $M_{l+1}/M_l = M_{l+1}/M'$ is of this form by construction. We have thus extended this filtration one step further, a contradiction since M' was assumed to be maximal. $\square$

Proposition 54.12. *Let R be a noetherian domain and let M be a finitely generated R-module. Then $\operatorname{Ann} M = 0$ if and only if there exists an injective R-linear map $R \rightarrowtail M$.*

Proof. Clearly if there exists an injective R-linear map $R \rightarrowtail M$ then $\operatorname{Ann} M = 0$. Conversely, assume that $\operatorname{Ann} M = 0$. Since M is finitely generated, we have $\operatorname{Supp} M = \mathrm{V}(\operatorname{Ann} M) = \mathrm{V}(0)$. In particular, $M_{\langle 0\rangle} \neq 0$, that is $\langle 0\rangle \in \operatorname{Supp} M$. Since $\operatorname{Supp} M$ and $\operatorname{Ass} M$ have the same minimal elements, it follows that $\langle 0\rangle \in \operatorname{Ass} M$. This is equivalent to saying there exists an injective R-linear map $R \rightarrowtail M$. $\square$

54.5.1 Clean Modules

Definition 54.13. Let M be a finitely generated R-module. We say M is **clean** if it admits a filtration such that the primes which occur in that filtration are precisely the associated primes of M.

Our goal in this subsubsection is to give a characterization of clean cyclic modules in a noetherian ring. To this end, let R be a noetherian ring, let I be an ideal of R, and let $I = Q_1 \cap \cdots \cap Q_m$ be an irredundant primary decomposition of I and set $\mathfrak{p}_i := \sqrt{Q_i}$. Choose $s_i \in R$ such that $s_i \notin Q_i$ and $s_i \in \bigcap_{j\neq i} Q_j$. Then

$$\begin{aligned} I : s_i &= (Q_1 \cap \cdots \cap Q_i \cdots \cap Q_m) : s_i \\ &= (Q_1 : s_i) \cap \cdots \cap (Q_i : s_i) \cap \cdots \cap (Q_m : s_i) \\ &= R \cap \cdots \cap Q_i' \cap \cdots \cap R \\ &= Q_i', \end{aligned}$$

where $Q_i' := Q_i : s_i$ is $\mathfrak{p}_i$-primary. If $Q_i' = \mathfrak{p}_i$, then we set $r_i = s_i$, otherwise Q_i' is a proper subset of $\mathfrak{p}_i$ and there exists $a_i \in \mathfrak{p}_i \backslash Q_i'$ such that $I : s_i a_i = \mathfrak{p}_i$, and we set $r_i = s_i a_i$ in this case. Now let $I_1 := \langle I, r_1\rangle$. We claim that $I_1 : r_i = \mathfrak{p}_i$ for all $i \neq 1$. Indeed, first observe that

$$\begin{aligned} I_1 : s_i &\subseteq (Q_2 \cap \cdots \cap Q_i \cap \cdots \cap Q_m) : s_i \\ &= (Q_2 : s_i) \cap \cdots \cap (Q_i : s_i) \cap \cdots \cap (Q_m : s_i) \\ &= R \cap \cdots \cap Q_i' \cap \cdots \cap R \\ &= Q_i'. \end{aligned}$$

Therefore we have

$$\begin{aligned} \mathfrak{p}_i &= I : r_i \\ &\subseteq I_1 : r_i \\ &= (I_1 : s_i) : a_i \\ &\subseteq Q_2' : a_i \\ &= \mathfrak{p}_i, \end{aligned}$$

which implies $\mathfrak{p}_i = I_1 : r_i$. An inductive argument shows that if we set $I_k = \langle I_{k-1}, r_k\rangle$ for $2 \leq k < m$, then $\mathfrak{p}_k = I_k : r_{k+1}$. Now consider the sequence:

$$R/I \supset I_m/I \supset \cdots \supset I_1/I \supset I_0/I = 0. \tag{189}$$

The factors of (189) are $R/\mathfrak{p}_1, \ldots, R/\mathfrak{p}_n, R/I_m$. In particular, (189) is the start of a filtration of R/I.

Proposition 54.13. *Let R be a noetherian ring and let I be an ideal of R. Let $I = Q_1 \cap \cdots \cap Q_m$ be an irredundant primary decomposition of I and set $\mathfrak{p}_i := \sqrt{Q_i}$. For each i choose $s_i \in R$ such that $s_i \in \bigcap_{j\neq i} Q_j$ and $s_i \notin Q_i$. If $I : s_i = \mathfrak{p}_i$, then we set $r_i := s_i$, otherwise there exists an $a_i \in \mathfrak{p}_i \backslash (I : s_i)$ such that $I : a_i s_i = \mathfrak{p}_i$, and wet set $r_i := a_i s_i$ in this case. Finally, set $I_0 = I$ and for each $1 \leq k \leq m$ set $I_k = \langle I_{k-1}, r_k\rangle$. Then R/I is a clean R-module if and only if $I_m = \mathfrak{p}_m$.*

Proof. Suppose R/I is a clean R-module. Let $J = Q_2 \cap \cdots \cap Q_{m-1}$. Let

$$R/I = M_m \supset M_{m-1} \supset \cdots \supset M_1 \supset M_0 := 0$$

be a filtration of R/I such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for all $1 \leq i \leq m$. $\square$

Lemma 54.7. *We have $I_1 : r_i = \mathfrak{p}_i$ for all $i \neq 1$ and $I_1 : s_1 = \mathfrak{p}_1$.*

Proof. It remains to show $I_1 : s_1 = \mathfrak{p}_1$. □

Lemma 54.8. *Let R be a noetherian ring, let I be an ideal of R, let $I = Q_1 \cap \cdots \cap Q_m$ be an irredundant primary decomposition of I, and let $\sqrt{Q_i} = \mathfrak{p}_i = I : r_i$.*

1. *$r_i \in Q_j$ for all j such that $\mathfrak{p}_j \not\supseteq \mathfrak{p}_i$.*
2. *$Q_i \neq \mathfrak{p}_i$ if and only if $r_i \in \mathfrak{p}_i$.*

Proof. Recall that for each j we have

$$Q_j : r_i = \begin{cases} R & \text{if } r_i \in Q_j \\ Q_j' & \text{if } r_i \in \mathfrak{p}_j \backslash Q_j \\ Q_j & \text{if } r_i \notin \mathfrak{p}_j \end{cases}$$

where $Q_j' = Q_j : r_i$ is another $\mathfrak{p}_j$-primary ideal which contains Q_j. Order the primary ideals such that $r_i \notin Q_1, \dots, Q_l$ and $r_i \in Q_{l+1}, \dots, Q_m$. Then

$$\begin{aligned} \mathfrak{p}_i &= \sqrt{\mathfrak{p}_i} \\ &= \sqrt{I : r_i} \\ &= \sqrt{(Q_1 : r_i) \cap \cdots \cap (Q_l : r_i) \cap (Q_{l+1} : r_i) \cap \cdots \cap (Q_m : r_i)} \\ &= \sqrt{(Q_1 : r_i) \cap \cdots \cap (Q_l : r_i) \cap R \cap \cdots \cap R} \\ &= \sqrt{(Q_1 : r_i) \cap \cdots \cap (Q_l : r_i)} \\ &= \sqrt{Q_1 : r_i} \cap \cdots \cap \sqrt{Q_l : r_i} \\ &= \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_l. \end{aligned}$$

It follows that, say without loss of generality, $\mathfrak{p}_i = \mathfrak{p}_1$ and $\mathfrak{p}_1 \subseteq \mathfrak{p}_j$ for all $1 \leq j \leq l$. Thus we conclude that $r_1 \in Q_j$ for each j such that $\mathfrak{p}_j \not\supseteq \mathfrak{p}_1$. □

Example 54.16. Let $R = \Bbbk[x, y, z]$ and let $I = \langle x^{10}, x^6y^3, x^2y^5, x^2y^3z^3 \rangle$. An irredundant primary decomposition of I is given by $I = Q_1 \cap Q_2 \cap Q_3$ where

$$\begin{aligned} &Q_1 = \langle x^2 \rangle && \mathfrak{p}_1 = \langle x \rangle && r_1 = xy^3z^3 \\ &Q_2 = \langle x^{10}, y^3 \rangle && \mathfrak{p}_2 = \langle x, y \rangle && r_2 = x^9y^2 \\ &Q_3 = \langle x^{10}, x^6y^3, y^5, z^3 \rangle && \mathfrak{p}_3 = \langle x, y, z \rangle && r_3 = x^5y^4z^2 \end{aligned}$$

where $\mathfrak{p}_i = \sqrt{Q_i} = I : r_i$ for $i = 1, 2, 3$. Note that $r_2 \notin Q_3$. On the other hand, if we set $r_2' = x^9y^2z^3$, then $r_2' \in Q_3$ and $I : r_2' = \mathfrak{p}_2$.

Theorem 54.9. *Let $(R, \mathfrak{m})$ be a local noetherian ring, let I be an ideal of R, and let $I = Q_1 \cap \cdots \cap Q_m$ be an irredundant primary decomposition of I such that Q_1 is $\mathfrak{m}$-primary. Then*

$$I^{\text{sat}} := \bigcup_{n=1}^{\infty} I : \mathfrak{m}^n = Q_2 \cap \cdots \cap Q_m.$$

Proof. The idea of the proof is very simple. Observe that

$$\begin{aligned} I : \mathfrak{m}^n &= (Q_1 \cap Q_2 \cap \cdots \cdots \cap Q_m) : \mathfrak{m}^n \\ &= (Q_1 : \mathfrak{m}^n) \cap (Q_2 : \mathfrak{m}^n) \cap \cdots \cap (Q_m : \mathfrak{m}^n) \\ &\subseteq R \cap Q_2 \cap \cdots \cap Q_m \\ &= Q_2 \cap \cdots \cap Q_m. \end{aligned}$$

for all $n \geq 1$. In particular, it follows that $I^{\text{sat}} \subseteq Q_2 \cap \cdots \cap Q_m$. In fact, we can get quality: choose $N \geq 1$ such that $Q_1 \supseteq \mathfrak{m}^N$ (we can do this since Q_1 is $\mathfrak{m}$-primary). Then note that $Q_1 : \mathfrak{m}^N = R$ implies $I : \mathfrak{m}^N = Q_2 \cap \cdots \cap Q_m$. Therefore we have $I^{\text{sat}} \supseteq Q_2 \cap \cdots \cap Q_m$ as well. □

55 Depth

55.0.1 Prime Avoidance

Lemma 55.1. *(Prime Avoidance) If $I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, with $\mathfrak{p}_i$ prime, then $I \subseteq \mathfrak{p}_i$ for some i.*

Proof. We prove the contrapositive: $I \nsubseteq \mathfrak{p}_i$ for all i implies $I \nsubseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Induct on n, the base case is trivial. We now suppose that $I \nsubseteq \mathfrak{p}_i$ for all i and $I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, and arrive at a contradiction. From our inductive hypothesis, for each i, $I \nsubseteq \bigcup_{j \neq i} \mathfrak{p}_j$. In particular, for each i there is an x_i which is in I but is not in $\bigcup_{j \neq i} \mathfrak{p}_j$. Notice that if $x_i \notin \mathfrak{p}_i$ then $x_i \notin \bigcup_{j=1}^n \mathfrak{p}_j$, and we have an immediate contradiction. So suppose for every i that $x_i \in \mathfrak{p}_i$. Consider the element

$$x = \sum_{i=1}^n x_1 \cdots \hat{x}_i \cdots x_n.$$

By construction, $x \in I$. We claim that $x \notin \bigcup_{i=1}^n \mathfrak{p}_i$. To see this, observe that $x_1 \cdots \hat{x}_i \cdots x_n \notin \mathfrak{p}_i$, because for each index $k \neq i$, x_k is not in $\bigcup_{j \neq k} \mathfrak{p}_j$, so in particular is not in $\mathfrak{p}_i$. Since $\mathfrak{p}_i$ is prime, this proves that $x_1 \cdots \hat{x}_i \cdots x_n \notin \mathfrak{p}_i$. But every other monomial of x is in $\mathfrak{p}_i$, since every other monomial contains x_i. This shows that $x \notin \mathfrak{p}_i$ for any i, hence $x \notin \bigcup_{j=1}^n \mathfrak{p}_j$, a contradiction. $\square$

55.0.2 Support

Definition 55.1. Let M be an R-module. The **support** of M is the set

$$\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} R \mid M_{\mathfrak{p}} \neq 0\}$$

Lemma 55.2. *Let M be an R-module. Then we have*

$$\operatorname{Supp} M \subseteq \mathrm{V}(\operatorname{Ann} M).$$

If moreover, M is finitely-generated, then

$$\operatorname{Supp} M \supseteq \mathrm{V}(\operatorname{Ann} M).$$

Proof. Let $\mathfrak{p} \in \operatorname{Supp} M$ and assume for a contradiciton that $\mathfrak{p} \notin \mathrm{V}(\operatorname{Ann} M)$, so $\mathfrak{p} \nsupseteq \operatorname{Ann} M$. Choose $s \in \operatorname{Ann} M$ such that $x \notin \mathfrak{p}$. Then $M_{\mathfrak{p}} = 0$ since given any $u/t \in M_{\mathfrak{p}}$, we have

$$\begin{aligned} \frac{u}{t} &= \frac{su}{st} \\ &= \frac{0}{st} \\ &= 0. \end{aligned}$$

This is a contradiction as $\mathfrak{p} \in \operatorname{Supp} M$ which means $M_{\mathfrak{p}} \neq 0$. Thus $\mathfrak{p} \in \mathrm{V}(\operatorname{Ann} M)$ and since $\mathfrak{p}$ is arbitrary, this implies

$$\operatorname{Supp} M \subseteq \mathrm{V}(\operatorname{Ann} M).$$

Now we prove the second part of the lemma: suppose M is finitely-generated, say by $u_1, \dots, u_n \in M$, and let $\mathfrak{p} \in \mathrm{V}(\operatorname{Ann} M)$, so $\mathfrak{p} \supseteq \operatorname{Ann} M$. Assume for a contradiction that $\mathfrak{p} \notin \operatorname{Supp} M$, so $M_{\mathfrak{p}} = 0$. Choose $s_i \in R \backslash \mathfrak{p}$ such that $s_i u_i = 0$ for all $1 \leq i \leq n$ and denote $s = s_1 s_2 \cdots s_n$. Then $s \in R \backslash \mathfrak{p}$ and $s \in \operatorname{Ann} M$ since

$$\begin{aligned} s u_i &= s_1 s_2 \cdots s_n u_i \\ &= s_1 \cdots s_{i-1} s_{i+1} \cdots s_n (s_i u_i) \\ &= s_1 \cdots s_{i-1} s_{i+1} \cdots s_n \cdot 0 \\ &= 0 \end{aligned}$$

for all $1 \leq i \leq n$. This contradicts the fact that $\mathfrak{p} \supseteq \operatorname{Ann} M$. Thus $\mathfrak{p} \in \operatorname{Supp} M$ and since $\mathfrak{p}$ is arbitary, this implies

$$\operatorname{Supp} M \supseteq \mathrm{V}(\operatorname{Ann} M).$$

$\square$

Lemma 55.3. *Let M be a finitely generated R-module and let I be an ideal of R. Then*

$$\sqrt{\operatorname{Ann}(M/IM)} = \sqrt{\langle I, \operatorname{Ann} M \rangle}.$$

Proof. To prove the equality on radicals, it suffices to show that a prime $\mathfrak{p}$ of R contains $\operatorname{Ann}(M/IM)$ if and only if it contains $\langle I, \operatorname{Ann} M \rangle$. Note by Proposition (55.2), we have $\mathfrak{p} \supseteq \operatorname{Ann}(M/IM)$ if and only if $M_{\mathfrak{p}}/I_{\mathfrak{p}} M_{\mathfrak{p}} = (M/IM)_{\mathfrak{p}} \neq 0$. By Nakayama's lemma, we have $M_{\mathfrak{p}}/I_{\mathfrak{p}} M_{\mathfrak{p}} \neq 0$ if and only if $M_{\mathfrak{p}} \neq 0$ and $I_{\mathfrak{p}} \subseteq \mathfrak{p}_{\mathfrak{p}}$. These conditions are satisfied if and only if $\mathfrak{p} \supseteq \langle I, \operatorname{Ann} M \rangle$. $\square$

55.1 Depth

Finite modules over Noetherian rings are distinguished for two reasons: First, every zerodivisor of M is contained in an associated prime ideal. Indeed, let x be a zerodivisor of M. This means there is a nonzero $u \in M$ such that $xu = 0$. Then x belongs to the ideal

$$0 :_R u = \{a \in R \mid au = 0\}.$$

In a Noetherian ring, we have primary decomposition. So

$$\begin{aligned} x \in 0 :_R u \\ &= Q_1 \cap \cdots \cap Q_m \\ &\subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m, \end{aligned}$$

where

$$\begin{aligned} \mathfrak{p}_i &= (0 :_R u) : d_i \\ &= 0 :_R d_i u. \end{aligned}$$

for some $d_i \in R$. That is, each $\mathfrak{p}_i$ is an associated prime ideal of M.

Secondly, the number of associated prime ideals of M is finite. So if I is an ideal which consists of zerodivisors of M, then

$$I \subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}.$$

and by the Lemma (55.1), we must have $I \subseteq \mathfrak{p}_i$ for some i. Writing $\mathfrak{p}_i = 0 :_R u_i$, the assignment $1 \mapsto u_i$ induces a nonzero homomorphism $\varphi \colon R/I \to M$.

Proposition 55.1. *Let M and N be R-modules.*

1. *If* $\mathrm{Ann}\, M$ *contains an N-regular element, then* $\mathrm{Hom}_R(M, N) = 0$.
2. *Conversely, if R is Noetherian, and M, N are finite, then* $\mathrm{Hom}_R(M, N) = 0$ *implies that* $\mathrm{Ann}\, M$ *contains an N-regular element.*

Proof. 1. Suppose $\mathrm{Ann}\, M$ contains an N-regular element. Choose $x \in \mathrm{Ann}\, M$ to be such an element and let $\varphi \in \mathrm{Hom}_R(M, N)$. Then

$$\begin{aligned} x\varphi(u) &= \varphi(xu) \\ &= \varphi(0) \\ &= 0 \end{aligned}$$

implies $\varphi(u) = 0$ for all $u \in M$. Therefore $\varphi = 0$.

2. Suppose R is Noetherian, M, N are finite, and $\mathrm{Hom}_R(M, N) = 0$. Assume for a contradiction that $\mathrm{Ann}\, M$ consists of zerodivisors of N. Then by the remarks above, $\mathrm{Ann}\, M \subset \mathfrak{p}$ for some associated prime ideal $\mathfrak{p}$ of N. By Lemma (55.2), $\mathfrak{p} \in \mathrm{Supp}\, M$; so $M_\mathfrak{p} \neq 0$. In fact, Nakayama's Lemma tells us that $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \neq 0$. Since $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ is just a direct sum of copies of $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, one has an epimorphism

$$M_\mathfrak{p} \to M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \to R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}.$$

Now observe that $\mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}\, N_\mathfrak{p}$, and thus we can compose this epimorphism with a nonzero homomorphism to obtain a nonzero homomorphism,

$$M_\mathfrak{p} \to R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \to N_\mathfrak{p}.$$

Thus

$$\begin{aligned} 0 &\neq \mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \\ &= \mathrm{Hom}_R(M, N)_\mathfrak{p}, \end{aligned}$$

which is a contradiction. □

Example 55.1. Let $A = \mathbb{Q}[x,y]$, $N = \mathbb{Q}[x,y]/\langle x \rangle$, and $M = \mathbb{Q}[x,y]/\langle x^2, yx \rangle$. Clearly there exists a nonzero morphism from N to M. For example, $N \xrightarrow{\cdot x} M$ is a homomorphism from N to M. However, we want to construct a homomorphism from N to M using the techniques of Proposition (55.1). Set $I := \mathrm{Ann}(N) = \langle x \rangle$. There are two associated primes of M, namely $\mathfrak{p} := \langle x, y \rangle$ and $\mathfrak{q} := \langle x \rangle$, both contain I, and $0 : \overline{x} = \mathfrak{p}$ and $0 : \overline{y} = \mathfrak{q}$. We have $N_\mathfrak{q} \cong \mathbb{Q}(y)$, $N_\mathfrak{p} \cong \mathbb{Q}[y]_{\langle y \rangle}$, $A_\mathfrak{q}/\mathfrak{q}A_\mathfrak{q} \cong \mathbb{Q}(y)$, and $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong \mathbb{Q}$. The morphism $N_\mathfrak{p} \to M_\mathfrak{p}$ is given by $f/g \mapsto xf/g$ where $f, g \in \mathbb{Q}[y]$ and $g(0) \neq 0$. The morphism $N_\mathfrak{q} \to M_\mathfrak{q}$ is given by $f/g \mapsto yf/g$ where $f, g \in \mathbb{Q}(y)$ and $g \neq 0$.

Lemma 55.4. *Let M and N be R-modules and let $\mathbf{x} = x_1, \ldots, x_n$ be a weak N-sequence contained in* $\operatorname{Ann} M$. *Then*

$$\operatorname{Hom}_R(M, N/\mathbf{x}N) \cong \operatorname{Ext}_R^n(M, N).$$

Proof. We use induction on n, starting form the vacuous case $n = 0$. Let $n \geq 1$, and set $\mathbf{x}' = x_1, \ldots, x_{n-1}$. Then the induction hypothesis implies that

$$\operatorname{Ext}_R^{n-1}(M, N) \cong \operatorname{Hom}_R(M, N/\mathbf{x}'N).$$

As x_n is $(N/\mathbf{x}'N)$-regular, we must have $\operatorname{Ext}_R^{n-1}(M, N/\mathbf{x}'N) = 0$ by Prop (55.1). Therefore the exact sequence

$$0 \longrightarrow N/\mathbf{x}'N \xrightarrow{\cdot x_n} N/\mathbf{x}'N \longrightarrow N/\mathbf{x}N \longrightarrow 0$$

yields an exact sequence

$$0 \longrightarrow \operatorname{Ext}_R^{n-1}(M, N/\mathbf{x}N) \longrightarrow \operatorname{Ext}_R^n(M, N/\mathbf{x}'N) \xrightarrow{\overline{x}_n} \operatorname{Ext}_R^n(M, N/\mathbf{x}'N)$$

The map φ is multiplication by x_n inherited from $M/\mathbf{x}'M$: That is, after choosing an injective resolution of $M/\mathbf{x}'M$ with modules labeled I_i and morphisms labeled $\varphi_i : I_i \to I_{i+1}$, then an element in $\operatorname{Ext}_A^n(N, M/\mathbf{x}'M)$ is represented by a map $\psi_n : N \to I_n$ such that $\varphi_n \circ \psi_n = 0$. Then the map φ sends the representative ψ_n in $\operatorname{Ext}_A^n(N, M/\mathbf{x}'M)$ to the representative $x_n\psi_n$ in $\operatorname{Ext}_A^n(N, M/\mathbf{x}'M)$, but

$$\begin{aligned}
(x_n\psi_n)(n) &= x_n\psi_n(n) \\
&= \psi_n(x_n n) \\
&= \psi_n(0) \\
&= 0,
\end{aligned}$$

for all $n \in N$. Therefore φ is the zero map. Hence ψ is an isomorphism. It's now easy to show that we get the sequence of isomorphism:

$$\operatorname{Hom}_A(N, M/\mathbf{x}M) \cong \operatorname{Ext}_A^0(N, M/\mathbf{x}M) \cong \operatorname{Ext}_A^1(N, M/\mathbf{x}'M) \cong \cdots \cong \operatorname{Ext}_A^n(N, M)$$

□

Let A be a Noetherian ring, I an ideal, M a finite A-module with $M \neq IM$, and $\mathbf{x} = x_1, \ldots, x_n$ a maximal M-sequence in I. From Prop (55.1) and Lemma (55.4), we have, since I contains an $M/\langle x_1, \ldots, x_{i-1}\rangle M$-regular element for $i = 1, \ldots, n$,

$$\operatorname{Ext}_A^{i-1}(A/I, M) \cong \operatorname{Hom}_A(A/I, M/\langle x_1, \ldots, x_{i-1}\rangle M) \neq 0.$$

We have therefore proved

Theorem 55.5. *(Rees). Let A be a Noetherian ring, M be a finite A-module, and I an ideal such that $IM \neq M$. Then all maximal M-sequences in I have the same length n given by*

$$n = min\{i \mid Ext_A^i(A/I, M) \neq 0\}.$$

Definition 55.2. Let A be a ring, $I \subset A$ and ideal and M an A-module. If $M \neq IM$, then the maximal length n of an M-sequence $a_1, \ldots, a_n \in I$ is called the I-**depth** of M and denoted by $\operatorname{depth}(I, M)$. If $M = IM$ then the I-depth of M is by convention ∞. If $(A, \mathfrak{m})$ is a local ring, then the $\mathfrak{m}$-depth of M is simply called the **depth** of M, that is, $\operatorname{depth}(M) := \operatorname{depth}(\mathfrak{m}, M)$.

Example 55.2.

1. Let K be a field and $K[x_1, \ldots, x_n]$ the polynomial ring. Then

$$\operatorname{depth}(\langle x_1, \ldots, x_n\rangle, K[x_1, \ldots, x_n]) \geq n,$$

since $x_1, \ldots, x_n$ is an $\langle x_1, \ldots, x_n\rangle$-sequence (and we shall see later that it is $= n$).

2. Let A be a ring, $I \subset A$ an ideal and M an A-module. Then the I-depth of M is 0 if and only if every element of I is a zerodivisor for M. Hence, $\operatorname{depth}(I, M) = 0$ if and only if I is contained in some associated prime ideal of M. In particular, for a local ring $(A, \mathfrak{m})$, we have $\operatorname{depth}(\mathfrak{m}, A/\mathfrak{m}) = 0$.

Recall that if $M = IM$, then we set the I-depth of M to be ∞. This is consistent with Theorem (55.5) because $\operatorname{depth}(I, M) = \infty$ if and only if $\operatorname{Ext}_A^i(A/I, M) = 0$ for all i. For if $IM = M$, then $\operatorname{supp}(M) \cap \operatorname{supp}(A/I) = \{\mathfrak{p} \mid \mathfrak{p} \supset I \text{ and } M_{\mathfrak{p}} \neq 0\} = \emptyset$, by Nakayama's lemma, hence

$$\operatorname{supp}(\operatorname{Ext}_A^i(A/I, M) \subset \operatorname{supp}(M) \cap \operatorname{supp}(A/I) = \emptyset;$$

conversely, if $\operatorname{Ext}_A^i(A/I, M) = 0$ for all i, then Theorem (55.5) gives $IM = M$.

Proposition 55.2. *Let A be a Noetherian ring, I and ideal in A, and*

$$0 \longrightarrow U \longrightarrow M \longrightarrow N \longrightarrow 0$$

an exact sequence of finite A-modules. Then

1. *$\operatorname{depth}(I, M) \geq \min\{\operatorname{depth}(I, U), \operatorname{depth}(I, N)\}$.*
2. *$\operatorname{depth}(I, U) \geq \min\{\operatorname{depth}(I, M), \operatorname{depth}(I, N) + 1\}$.*
3. *$\operatorname{depth}(I, N) \geq \min\{\operatorname{depth}(I, U) - 1, \operatorname{depth}(I, M)\}$.*

Proof. Let $k = \operatorname{depth}(I, U)$, $m = \operatorname{depth}(I, M)$, and $n = \operatorname{depth}(I, N)$. The given exact sequence induces a long exact sequence

$$\begin{tikzcd}
& \cdots \arrow[r] & \mathrm{Ext}_A^{i-1}(A/I,N) \arrow[dll, rounded corners] \\
\mathrm{Ext}_A^{i}(A/I,U) \arrow[r] & \mathrm{Ext}_A^{i}(A/I,M) \arrow[r] & \mathrm{Ext}_A^{i}(A/I,N) \arrow[dll, rounded corners] \\
\mathrm{Ext}_A^{i+1}(A/I,U) \arrow[r] & \cdots &
\end{tikzcd}$$

From the long exact sequence above, we deduce the following:

- If $k < n$, then $\operatorname{Ext}_A^i(A/I, M) \cong \operatorname{Ext}_A^i(A/I, N)$ for all $i > k$. This implies $m = n$.
- If $k > n + 1$, then $\operatorname{Ext}_A^i(A/I, M) \cong \operatorname{Ext}_A^i(A/I, U)$ for all $i > n + 1$. This implies $m = k$.
- If $k = n + 1$, then $\operatorname{Ext}_A^i(A/I, M) \cong \operatorname{Ext}_A^i(A/I, U)$ for all $i > n + 1$. This implies $m \leq n$.
- If $k = n$, then $\operatorname{Ext}_A^i(A/I, M) \cong 0$ for all $i > n$. Moreover, $\operatorname{Ext}_A^n(A/I, M) \not\cong 0$, since $\operatorname{Ext}_A^n(A/I, N) \not\cong 0$ and $\operatorname{Ext}_A^n(A/I, U) \cong 0$. This implies $m = n = k$.

∎

Proposition 55.3. *Let A be a Noetherian ring, I, J ideals of A, and M a finite A-module. Then*

1. *$\operatorname{grade}(I, M) = \inf\{\operatorname{depth} M_{\mathfrak{p}} \mid \mathfrak{p} \supset I\}$.*
2. *$\operatorname{grade}(I, M) = \operatorname{grade}(\sqrt{I}, M)$,*
3. *$\operatorname{grade}(I \cap J, M) = \min\{\operatorname{grade}(I, M), \operatorname{grade}(J, M)\}$*
4. *If $\mathbf{x} = x_1, \ldots, x_n$ is an M-sequence in I, then $\operatorname{grade}(I/\langle \mathbf{x} \rangle, M/\mathbf{x}M) = \operatorname{grade}(I, M/\mathbf{x}M) = \operatorname{grade}(I, M) - n$.*
5. *If N is a finite A-module with $\operatorname{supp} N = V(I)$, then $\operatorname{grade}(I, M) = \inf\{i \mid \operatorname{Ext}_A^i(N, M) \neq 0\}$.*

Proof.

1. It is evident from the definition that $\operatorname{grade}(I, M) \leq \operatorname{grade}(\mathfrak{p}, M) \leq \operatorname{depth} M_{\mathfrak{p}}$ for $\mathfrak{p} \supset I$. Suppose $IM \neq M$ and choose a maximal M-sequence $\mathbf{x}$ in I. Since I consists of zero-divisors of $M/\mathbf{x}M$, there exists $\mathfrak{p} \in \operatorname{Ass}(M/\mathbf{x}M)$ with $\mathfrak{p} \supset I$. Since $\mathfrak{p}A_{\mathfrak{p}} \in \operatorname{Ass}(M/\mathbf{x}M)_{\mathfrak{p}}$ and $(M/\mathbf{x}M)_{\mathfrak{p}} \cong M_{\mathfrak{p}}/\mathbf{x}M_{\mathfrak{p}}$, the ideal $\mathfrak{p}A_{\mathfrak{p}}$ consists of zero-divisors of $M_{\mathfrak{p}}/\mathbf{x}M_{\mathfrak{p}}$, and $\mathbf{x}$ (as a sequence in $A_{\mathfrak{p}}$) is a maximal $M_{\mathfrak{p}}$-sequence.
2. Factor I into its primary decomposition $I = Q_1 \cap Q_2 \cap \cdots \cap Q_k$. Then $\sqrt{I} = \sqrt{Q_1} \cap \sqrt{Q_2} \cap \cdots \cap \sqrt{Q_k}$. Any prime $\mathfrak{p}$ which contains I, must contain one of the $\sqrt{Q_i}$, and therefore must contain $\sqrt{I}$.

3. Factor I and J into their primary decompositions $I = Q_1 \cap Q_2 \cap \cdots \cap Q_k$ and $J = P_1 \cap P_2 \cap \cdots \cap P_\ell$ with corresponding primes $\mathfrak{q}_1, \mathfrak{q}_2 \ldots, \mathfrak{q}_k$ and $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_\ell$ respectively. For similar reasons as above, we must have $\operatorname{grade}(I \cap J, M) = \operatorname{depth} M_\mathfrak{p}$ for some $\mathfrak{p} \in \{\mathfrak{q}_1, \mathfrak{q}_2 \ldots, \mathfrak{q}_k, \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_\ell\}$.

4. Set $\overline{A} = A/\langle \mathbf{x} \rangle$, $\overline{I} = I/\langle \mathbf{x} \rangle$, and $\overline{M} = M/\mathbf{x}M$. First observe that $IM = M \iff I\overline{M} = \overline{M} \iff \overline{IM} = \overline{M}$. Furthermore, $y_1, \ldots, y_n \in I$ form an $\overline{M}$-sequence if and only if $\overline{y}_1, \ldots, \overline{y}_n \in \overline{I}$ form such a sequence. This shows that $\operatorname{grade}(I/\langle \mathbf{x} \rangle, M/\mathbf{x}M) = \operatorname{grade}(I, M/\mathbf{x}M)$.

□

Let $(A, \mathfrak{m})$ be Noetherian local and M a finite A-module. All the minimal elements of $\operatorname{Supp} M$ belong to $\operatorname{Ass} M$. Therefore if $x \in \mathfrak{m}$ is an M-regular element, then $x \notin \mathfrak{p}$ for all minimal elements of $\operatorname{Supp} M$: Suppose $x \in \mathfrak{p}$ where $\mathfrak{p} = 0 : m$ for some nonzero $m \in M$. Then $x \in \mathfrak{p}$ implies $xm = 0$, which is a contradiction since x is M-regular. Therefore $\dim M/xM \leq \dim M - 1$: A longest chain containing $\operatorname{Ann} M$ must start with a minimal prime of $\operatorname{Supp} M$, but a longest chain containing $\operatorname{Ann} M \cup \langle x \rangle$ does not start with a minimal prime of $\operatorname{Supp} M$.

Proposition 55.4. *Let $(A, \mathfrak{m})$ be Noetherian local and $M \neq 0$ a finite A-module. Then $\operatorname{depth} M \leq \dim A/\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Ass} M$.*

Lemma 55.6. *Let A be a Noetherian ring, M a finitely generated A-module, and $I \subset A$ an ideal with $IM \neq M$. Then the following are equivalent:*

1. *$\operatorname{Ext}^i_A(N, M) = 0$ for all $i < n$ and all finitely generated A-modules N with $\operatorname{supp}(N) \subset V(I)$.*

2. *$\operatorname{Ext}^i_A(A/I, M) = 0$ for all $i < n$.*

3. *$\operatorname{Ext}^i_A(N, M) = 0$ for all $i < n$ and some finitely generated A-module N with $\operatorname{supp}(N) = V(I)$.*

4. *I contains an M-sequence of length n.*

Proof. (1) implies (2) is obvious since $\operatorname{supp}(A/I) = V(I)$. Also, (2) implies (3) is obvious since A/I is some finitely generated A-module with $\operatorname{supp}(A/I) = V(I)$. To prove (3) implies (4), let $n > 0$ and assume first that I contains only zero divisors of M, that is, I is contained in an associated prime ideal $\mathfrak{p} = 0 : m$, where m is some nonzero element in M. Then the map $A/\mathfrak{p} \to M$, defined by $1 \mapsto m$, is injective. Localizing a $\mathfrak{p}$, we obtain that $\operatorname{Hom}_{A_\mathfrak{p}}(k, M_\mathfrak{p}) \neq 0$, where $k = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Now $\mathfrak{p} \in V(I) = \operatorname{supp}(N)$, that is, $N_\mathfrak{p} \neq 0$, and hence, $N_\mathfrak{p}/\mathfrak{p}N_\mathfrak{p} = N \otimes_A k \neq 0$ (Lemma of Nakayama). This implies that $\operatorname{Hom}_k(N \otimes_A k, k) \neq 0$ and, therefore, we have a non-trivial $A_\mathfrak{p}$-linear map

$$N_\mathfrak{p} \to N \otimes_A k \to k \to M_\mathfrak{p},$$

that is, $\operatorname{Hom}(N_\mathfrak{p}, M_\mathfrak{p}) \neq 0$. This implies that $\operatorname{Hom}_A(N, M) \neq 0$, which contradicts (3) for $i = 0$. So we proved that I contains an M-regular element f. By assumption, $M/IM \neq 0$, hence if $n = 1$ we are done. If $n > 1$, then we obtain from the exact sequence

$$0 \longrightarrow M \xrightarrow{f} M \longrightarrow M/fM \longrightarrow 0$$

that $\operatorname{Ext}^i_A(N, M/fM) = 0$ for $i < n - 1$. Using induction, this implies that I contains an (M/fM)-regular sequence $f_2, \ldots, f_n$.

To prove (4) implies (1), let $f_1, \ldots, f_n \in I$ be an M-sequence and consider again the exact sequence

$$0 \longrightarrow M \xrightarrow{f_1} M \longrightarrow M/f_1M \longrightarrow 0$$

Applying the function $\operatorname{Ext}^i_A(N, -)$ to this sequence gives the exact sequence

$$\cdots \longrightarrow \operatorname{Ext}^i_A(N, M) \xrightarrow{f_1} \operatorname{Ext}^i_A(N, M) \longrightarrow \operatorname{Ext}^i_A(N, M/f_1M) \longrightarrow \cdots$$

If $n = 1$, then we consider the first part of this sequence

$$0 \longrightarrow \operatorname{Hom}_A(N, M) \xrightarrow{f_1} \operatorname{Hom}_A(N, M)$$

If $n > 1$, then we use induction to obtain $\operatorname{Ext}^i_A(N, M/f_1M) = 0$ for $i < n - 1$. This implies

$$0 \longrightarrow \operatorname{Ext}^i_A(N, M) \xrightarrow{f_1} \operatorname{Ext}^i_A(N, M)$$

is exact for $i < n$. Now $\mathrm{Ext}^i_A(N, M)$ is annihilated by elements of $\mathrm{Ann}(N)$. On the other hand, by assumption, we have

$$\mathrm{supp}(N) = V(\mathrm{Ann}(N)) \subset V(I).$$

This implies that $I \subset \sqrt{\mathrm{Ann}(N)}$. Therefore, a sufficiently large power of f_1 annihilates $\mathrm{Ext}^i_A(N, M)$. But we already saw that f_1 is a nonzerodivisor for $\mathrm{Ext}^i_A(N, M)$ and, consequently, $\mathrm{Ext}^i_A(N, M) = 0$ for $i < n$. □

55.2 Regular Sequences

Definition 55.3. Let M be an R-module and let $x \in R$. We say x is M**-regular** if x is a not a zerodivisor for M. In other words, x is M-regular if the map $M \xrightarrow{x} M$ is injective. A sequence of elements $\boldsymbol{x} = x_1, \dots, x_n$ in R is called an M**-sequence** if x_1 is M-regular and x_i is $(M/\langle x_1, \dots, x_{i-1} \rangle M)$-regular for all $2 \leq i \leq n$. In other words, $\boldsymbol{x}$ is an M-sequence if the the sequences of maps

$$\begin{aligned} M &\xrightarrow{\cdot x_1} M \\ M/x_1 M &\xrightarrow{\cdot x_2} M/x_1 M \\ &\vdots \\ M/(x_1, \dots, x_{n-1})M &\xrightarrow{\cdot x_n} M/(x_1, \dots, x_{n-1})M \end{aligned}$$

are all injective. In this case, the sequence $\boldsymbol{x}$ is said to have **length** n. Now let I be any ideal of R. We define the I**-depth** of M, denoted $\mathrm{depth}(I, M)$, to be supremum of the lengths of M-sequences. In the case where $(R, \mathfrak{m})$ is a local ring and $I = \mathfrak{m}$, then the $\mathfrak{m}$-depth of M is simply called the **depth** of M and is denoted $\mathrm{depth}\, M$.

Example 55.3. Let R be an integral domain. Suppose that $\boldsymbol{g} = g_1, g_2$ is an R-sequence. We claim that there are no nontrival ways of writing g_1/g_2: they are all of the form $(hg_1)/(hg_2)$ for some $h \in R$. Indeed, let f_1 and f_2 be two elements in R such that $g_1/g_2 = f_1/f_2$. Then this implies that $f_1 g_2 = f_2 g_1$. Since the map

$$R/g_1 \xrightarrow{g_2} R/g_1$$

is injective, we must have $f_1 = hg_1$ for some $h \in R$. Hence,

$$\begin{aligned} 0 &= f_1 g_2 - f_2 g_1 \\ &= hg_1 g_2 - f_2 g_1 \\ &= g_1(hg_2 - f_2), \end{aligned}$$

which implies $f_2 = hg_2$ since R is an integral domain (in particular g_1 is not a zerodivisor). Therefore

$$\frac{f_1}{f_2} = \frac{hg_1}{hg_2}.$$

On the other hand, we can show that if $\boldsymbol{g}$ fails to form an R-sequence, then there exists nontrivial ways of writing g_1/g_2. When does $\boldsymbol{g}$ fail to form an R-sequence? Well, R is an integral domain, so the map from R to R given by multiplication by g_1 is injective if and only if $g_1 \neq 0$. Then assuming $g_1 \neq 0$, we see that $\boldsymbol{g}$ is an R-sequence if and only if the map from R/g_1 to R/g_1 given by multiplication by g_2 is not injective. This happens if and only if there exists f_1, f_2 in S such that $f_1 g_2 = f_2 g_1$ and f_1 is not of the form hg_1 for some $h \in R$, which means f_1/f_2 is a nontrivial way of writing g_1/g_2. So we see that $\boldsymbol{g}$ is an R-sequence if and only if there are no nontrivial ways of writing g_1/g_2.

For instance, suppose $R = \mathbb{Z}[\sqrt{-5}]$. The sequence $2, 1 + \sqrt{-5}$ does not form an R-sequence. Indeed, we have

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

and neither 2 divides $1 - \sqrt{-5}$ nor $1 + \sqrt{-5}$ divides 3.

Example 55.4. Let $R = \Bbbk[x, y, z]$, let $\boldsymbol{a} = a_1, a_2, a_3$, and let $\widehat{\boldsymbol{a}} = a_1, a_3, a_2$, where

$$\begin{aligned} a_1 &= x(y-1) \\ a_2 &= y \\ a_3 &= z(y-1). \end{aligned}$$

It can be shown that $\boldsymbol{a}$ is an R-sequence, but that $\widehat{\boldsymbol{a}}$ is not an R-sequence.

Remark 88. We shall see that, for local rings, the permutation of a regular sequence is again a regular sequence.

55.3 Koszul Complex and Depth

Let R be a noetherian ring, let I be an ideal of R such that $I = \sqrt{\langle x_1, \dots, x_n \rangle} = \sqrt{\langle \boldsymbol{x} \rangle}$ where $x_1, \dots, x_n \in I$, and let M a finitely-generated R-module such that $M \neq IM$. Choose $k \in \mathbb{N}$ such that $I^k \subseteq \langle \boldsymbol{x} \rangle \subseteq I$. Then since $\mathrm{H}_n(\boldsymbol{x}, M) = 0 :_M \boldsymbol{x}$ and $\mathrm{H}_0(\boldsymbol{x}, M) = M/\boldsymbol{x}M$, we have

$$0 :_M I \subseteq \mathrm{H}_n(\boldsymbol{x}, M) \subseteq 0 :_M I^k \quad \text{and} \quad M/IM \subseteq \mathrm{H}_0(\boldsymbol{x}, M) \subseteq M/I^k M$$

In particular, the condition $M \neq IM$ implies $\mathrm{H}_0(\boldsymbol{x}, M) \neq 0$. Thus the set $\{i \in \mathbb{Z} \mid \mathrm{H}_i(\boldsymbol{x}, M) \neq 0\}$ is nonempty and bounded above (since $\mathcal{K}_i(\boldsymbol{x}, M) = 0$ for all $i > n$). Therefore it makes sense to define the supremum of that set:

$$\delta_M = \delta = \sup\{i \mid \mathrm{H}_i(\boldsymbol{x}, M) \neq 0\}.$$

We will use this fact in the proof of the following theorem:

Theorem 55.7. *With the notation as above, all maximal M-sequences in I have length $n - \delta$. In particular,*

$$\operatorname{depth}(I, M) = n - \sup\{i \mid \mathrm{H}_i(\boldsymbol{x}, M) \neq 0\} = \operatorname{depth}(\langle \boldsymbol{x} \rangle, M).$$

*In other words, the I-**depth** of M is equal to the $\langle \boldsymbol{x} \rangle$-**depth** of M.*

Proof. First suppose that every element in I is a zerodivisor for M (this is equivalent to saying every maximal M-sequence in I has length 0). This means that for each $y \in I$ there exists a nonzero $u_y \in M$ such that $yu_y = 0$. In fact, we can do much better: since R is noetherian, we can actually find a single nonzero $u \in M$ such that $yu = 0$ for all $y \in I$. Indeed, if I consists of zerodivisors for M, then it is contained in an associated prime of M, say $\mathfrak{p}$ where $\mathfrak{p} = 0 : u$ for some nonzero $u \in M$ (again we are using the fact that R is noetherian here). In particular, we have $Iu = 0$ as claimed. Thus we have $u \in 0 :_M I$. It follows that $0 :_M I \neq 0$ which implies $\mathrm{H}_n(\boldsymbol{x}, M) \neq 0$ which implies $\delta = n$. Conversely, if $\delta = n$, then $\mathrm{H}_n(\boldsymbol{x}, M) \neq 0$ which implies $0 :_M I^k \neq 0$. Thus there exists a nonzero $u \in M$ such that $I^k u = 0$. This is equivalent to saying $0 : u \supseteq I^k$. By replacing u by an R-multiple of itself if necessary, we may assume $0 : u = \mathfrak{p}$ is an associated prime of M. Then we must have $\mathfrak{p} \supseteq I$ since $\mathfrak{p}$ is prime. This implies every element in I is a zerodivisor for M.

Now suppose that $\boldsymbol{y} = y_1, \dots, y_\varepsilon$ is a maximal M-sequence in I. Then $\boldsymbol{z} = z_1, \dots, z_\varepsilon$ is a maximal M-sequence in $\langle \boldsymbol{x} \rangle$ where $z_i = y_i^k$ for each $1 \leq i \leq \varepsilon$. We shall prove $\delta = n - \varepsilon$ by induction on ε. The base case $\varepsilon = 0$ was shown above, so assume that $\varepsilon > 0$. Consider the short exact sequence of R-modules

$$0 \longrightarrow M \xrightarrow{z_1} M \longrightarrow M/z_1 M \longrightarrow 0 \tag{190}$$

This short exact sequence of R-modules induces a short exact sequence of R-complexes

$$0 \longrightarrow \mathcal{K}(\boldsymbol{x}, M) \xrightarrow{z_1} \mathcal{K}(\boldsymbol{x}, M) \longrightarrow \mathcal{K}(\boldsymbol{x}, M/z_1 M) \longrightarrow 0 \tag{191}$$

Taking the long exact sequence in homology and using the fact that z_1 kills $\mathrm{H}(\boldsymbol{x}, M)$ (as $z_1 \in \langle \boldsymbol{x} \rangle$!), we obtain following short exact sequence of R-modules

$$0 \longrightarrow \mathrm{H}_i(\boldsymbol{x}, M) \longrightarrow \mathrm{H}_i(\boldsymbol{x}, M/z_1 M) \longrightarrow \mathrm{H}_{i-1}(\boldsymbol{x}, M) \longrightarrow 0 \tag{192}$$

for all $i \in \mathbb{Z}$. Note that $y_2, \dots, y_\varepsilon$ is a maximal $M/z_1 M$-sequence in I of length $\varepsilon - 1$ and that $I(M/z_1 M) \neq M/z_1 M$ since $z_1 \in I$ and $M \neq IM$. Thus by induction, we have $\mathrm{H}_i(\boldsymbol{x}, M/z_1 M) = 0$ for all $i > n - (\varepsilon - 1) = n - \varepsilon + 1$ and $\mathrm{H}_{n-\varepsilon+1}(\boldsymbol{x}, M/z_1 M) \neq 0$. Using this together with the short exact sequence (192) gives us $\mathrm{H}_i(\boldsymbol{x}, M) = 0$ for all $i > n - \varepsilon$ and $\mathrm{H}_{n-\varepsilon}(\boldsymbol{x}, M) \neq 0$. In other words, $\delta = n - \varepsilon$. □

Remark 89. It's worth pointing out that we obtain something extra from the proof above that wasn't stated in the theorem; namely from (192) we obtain $\mathrm{H}_\delta(\boldsymbol{x}, M) \simeq \mathrm{H}_{\delta+1}(\boldsymbol{x}, M/z_1 M)$. We think of this as an **antishift property** of Koszul homologies in the sense that δ increases by one when we replace it by $\delta + 1$ whereas the $\langle \boldsymbol{x} \rangle$-depth (and hence I-depth) decreases by one when we replace $M/z_1 M$ with M (slogan: homological degree goes up, depth goes down). More generally, an inductive argument gives us

$$\begin{aligned} \mathrm{H}_\delta(\boldsymbol{x}, M) &\simeq \mathrm{H}_n(\boldsymbol{x}, M/\boldsymbol{z}M) \\ &= 0 :_{M/\boldsymbol{z}M} \boldsymbol{x} \\ &= \operatorname{Hom}_R(R/\boldsymbol{x}, M/\boldsymbol{z}M) \\ &= \operatorname{Ext}_R^0(R/\boldsymbol{x}, M/\boldsymbol{z}M) \\ &\simeq \operatorname{Ext}_R^\varepsilon(R/\boldsymbol{x}, M). \end{aligned}$$

The last isomorphism $\operatorname{Ext}_R^\varepsilon(R/\boldsymbol{x}, M) \simeq \operatorname{Ext}_R^0(R/\boldsymbol{x}, M/\boldsymbol{z}M)$ will be explained in the next section. We think of this as a **shift property** of Ext in the second component (slogan: homological degree goes down, depth goes down).

Theorem 55.8. *Let M be a nonzero R-module and let $\boldsymbol{x} = x_1, \dots, x_n$ be a sequence in R.*

1. *If $\boldsymbol{x}$ is an M-sequence, then $\mathrm{H}_i(\boldsymbol{x}, M) = 0$ for all $i > 0$. In particular, $\mathcal{K}(\boldsymbol{x}, M)$ is a free resolution of $M/\boldsymbol{x}M$ over R.*
2. *Suppose $(R, \mathfrak{m})$ is local with $\boldsymbol{x} \in \mathfrak{m}$. If M is finitely generated and $\mathrm{H}_1(\boldsymbol{x}, M) = 0$, then $\boldsymbol{x}$ is an M-sequence, and consequently $\mathcal{K}(\boldsymbol{x}, M)$ is a free resolution of $M/\boldsymbol{x}M$ over R.*

Proof. 1. We prove this by induction on n. For the base case, suppose $n = 1$. Then since $\mathrm{H}_1(x_1, M) = 0 :_M x_1$, we see that $\mathrm{H}_1(x_1, M) = 0$ if and only if x_1 is M-regular. This establishes the base case. For the induction step, assume $n > 1$ and assume that we've shown the theorem to be true for all M-sequences of length $m < n$. Let $\boldsymbol{x} = x_1, \dots, x_n$ be an M-sequence of length n and let $\boldsymbol{x}' = x_1, \dots, x_{n-1}$ be the M-sequence of length $n-1$ obtained by removing x_n from $\boldsymbol{x}$. The multiplication by x_n map from $\mathcal{K}(\boldsymbol{x}', M)$ to itself induces a short exact sequence of R-complexes

$$0 \to \mathcal{K}(\boldsymbol{x}', M) \to \mathrm{C}(x_n) \to \Sigma\mathcal{K}(\boldsymbol{x}', M) \to 0, \tag{193}$$

where $\mathrm{C}(x_n)$ is the mapping cone with respect to the multiplication by x_n map. Since $\mathrm{C}(x_n) \cong \mathcal{K}(\boldsymbol{x}, M)$ and since the connecting map induced by (193) is just multiplication by x_n, we obtain a long exact sequence in homology

$$\begin{tikzcd} & \cdots \arrow[r] & \mathrm{H}_i(\boldsymbol{x}', M) \arrow[dll, rounded corners, "x_n"'] \\ \mathrm{H}_i(\boldsymbol{x}', M) \arrow[r] & \mathrm{H}_i(\boldsymbol{x}, M) \arrow[r] & \mathrm{H}_{i-1}(\boldsymbol{x}', M) \arrow[dll, rounded corners, "x_n"'] \\ \mathrm{H}_{i-1}(\boldsymbol{x}', M) \arrow[r] & \cdots & \end{tikzcd} \tag{194}$$

Since $\boldsymbol{x}'$ is an M-sequence of length $n-1$, we have by induction $\mathrm{H}_i(\boldsymbol{x}', M) = 0$ for all $i > 0$. This together with the long exact sequence in homology (194) implies $\mathrm{H}_i(\boldsymbol{x}, M) = 0$ for all $i > 1$. The vanishing of $\mathrm{H}_1(\boldsymbol{x}, M)$ follows from taking $i = 1$ in (194) together with the fact that $\mathrm{H}_0(\boldsymbol{x}', M) \cong M/\boldsymbol{x}'M$ and x_n is $(M/\boldsymbol{x}'M)$-regular.

2. We prove this by induction on n. The base case $n = 1$ is proved similarly as in the base case in 1. For the induction step, suppose that we've shown the theorem to be true for all sequences in $\mathfrak{m}$ of length $m < n$ for some $n > 1$. Let $\boldsymbol{x} = x_1, \dots, x_n$ be a sequence in $\mathfrak{m}$ of length n and suppose that $\mathrm{H}_1(\boldsymbol{x}, M) = 0$. As in 1, let $\boldsymbol{x}' = x_1, \dots, x_{n-1}$ be the sequence in $\mathfrak{m}$ of length $n-1$ obtained by removing x_n from $\boldsymbol{x}$. By the same argument as in 1, we obtain a long exact sequence in homology (194). In particular, since $\mathrm{H}_1(\boldsymbol{x}, M) = 0$, we have a surjective map $\mathrm{H}_1(\boldsymbol{x}', M) \xrightarrow{x_n} \mathrm{H}_1(\boldsymbol{x}', M)$. By Nakayama's lemma, this implies $\mathrm{H}_1(\boldsymbol{x}', M) = 0$. Using induction, we obtain that $\boldsymbol{x}'$ is an M-sequence. Finally, using the fact that $\mathrm{H}_1(\boldsymbol{x}, M) = 0$ together with the long exact sequence in homology (194) we see that $\mathrm{H}_0(\boldsymbol{x}', M) \xrightarrow{x_n} \mathrm{H}_0(\boldsymbol{x}', M)$ is injective. Since $\mathrm{H}_0(\boldsymbol{x}', M) \cong M/\boldsymbol{x}'M$, it follows that $\boldsymbol{x}$ is an M-sequence. □

Corollary 57. *Let $(R, \mathfrak{m})$ be a local ring, let $I = \langle x_1, \dots, x_n \rangle = \langle \boldsymbol{x} \rangle$ be a proper ideal of R, and let M be a nonzero finitely-generated R-module. Suppose $\boldsymbol{y} = y_1, \dots, y_n$ is an M-sequence of length n contained in I. Then $\boldsymbol{x}$ is an M-sequence.*

Proof. Since $\boldsymbol{y}$ is an M-sequence of length n contained in the ideal I which is generated by n elements, we must have $\mathrm{depth}(I, M) = n$. In particular, this implies $\mathrm{H}_1(\boldsymbol{x}, M) = 0$. Therefore $\boldsymbol{x}$ must be an M-sequence, by Theorem (55.8).

□

Corollary 58. *Let P be a projective resolution of M over R. Suppose $\boldsymbol{x} = x_1, \dots, x_m$ is an R-sequence and an M-sequence. Then $P/\boldsymbol{x}P$ is a projective resolution of $M/\boldsymbol{x}M$ over $R/\boldsymbol{x}R$.*

Proof. First we observe that $P/\boldsymbol{x}P$ is a projective $R/\boldsymbol{x}$ module. Indeed, this follows from one of the base change arguments (which follows from tensor-hom adjointness). Next we observe that since $\boldsymbol{x}$ is an R-sequence, we have

$$\begin{aligned} \mathrm{H}(P/\boldsymbol{x}P) &= \mathrm{H}(P \otimes_R R/\boldsymbol{x}) \\ &= \mathrm{H}(M \otimes_R \mathbb{K}(\boldsymbol{x})) \\ &= \mathrm{H}(\mathbb{K}(\boldsymbol{x}, M)) \\ &= \mathrm{H}(\boldsymbol{x}, M), \end{aligned}$$

and since $\boldsymbol{x}$ is an M-sequence, we have

$$\mathrm{H}_i(P/\boldsymbol{x}P) = \mathrm{H}(\boldsymbol{x}, M) = \begin{cases} M/\boldsymbol{x}M & \text{if } i = 0 \\ 0 & \text{else} \end{cases}$$

It follows that $P/\boldsymbol{x}P$ is a projective resolution of $M/\boldsymbol{x}M$ over $R/\boldsymbol{x}$. □

Remark 90. Let $S = R/\boldsymbol{x}R$, let $N = M/\boldsymbol{x}M$, and let $Q = P/\boldsymbol{x}P$. Suppose Q is a projective resolution of N over S. Then since $\boldsymbol{x}$ is an R-sequence, we have

$$\begin{aligned} N &= \mathrm{H}(Q) \\ &= \mathrm{H}(P \otimes_R R/\boldsymbol{x}) \\ &= \mathrm{H}(P \otimes_R \mathcal{K}(\boldsymbol{x})) \end{aligned}$$

Lemma 55.9. *Let $S = \mathbb{k}[t, x_1, \ldots, x_n] = \mathbb{k}[t, \boldsymbol{x}]$, let $R = \mathbb{k}[\boldsymbol{x}] = S/(t-1)$, let J be a graded ideal of S, and let $I = J/(t-1)$. Then $t-1$ is both an S-regular and (S/J)-regular element. In particular, if G is the minimal graded free resolution of S/J over S, then $F = G/(t-1)$ is a free resolution of R/I over R (though it need not be minimal).*

Proof. Clearly $t-1$ is S-regular. To see why $t-1$ is (S/J)-regular, first observe that if $f \in S$ is homogeneous such that $(t-1)f \in J$, then we must have $f \in J$ since f is a homogeneous component of $(t-1)f = tf - f$ and each homogeneous component of $(t-1)f$ must belong to J. More generally, if $f = f_1 + \cdots + f_k$ with f_1 being the component of f in smallest degree, then $(t-1)f \in J$ implies $f_1 \in J$ since f_1 is the component of $(t-1)f$ in smallest degree. Arguing by induction on the number of components of f, we can show that $(t-1)f \in J$ implies $f \in J$. Therefore $t-1$ is (S/J)-regular as claimed. □

Remark 91. The same argument shows that $t - \tau$ is S and (S/J)-regular for all nonzero $\tau \in \mathbb{k}$.

Example 55.5. Let $R = \mathbb{k}[x, y, z, w]$, let $I^\tau = \langle x + \tau z, y + \tau w, z^2, zw, w^2 \rangle$, and let F^τ be the minimal free graded resolution of R/I^τ over R for each $\tau \in \mathbb{k}$. We claim that each F^τ has the same "shape", namely $\boldsymbol{\beta} = (1, 5, 9, 7, 2)$. In other words, we claim that the function $\tau \to \beta_i(R/I^\tau)$ is constant for all i. To show this, let $S = \mathbb{k}[x, y, z, w, t]$, let $J = \langle x + tz, y + tw, z^2, zw, w^2 \rangle$, and let G be the minimal free graded resolution of S/J over S. Setting $N = S/J$, it is easy to check that $t - \tau$ is both S-regular and N-regular. Thus $G/\langle t - \tau \rangle G$ is the minimal free resolution of $N/\langle t - \tau \rangle N \simeq R/I^\tau$ over $S/\langle t - \tau \rangle \simeq R$. In particular we must have $G/\langle t - \tau \rangle G \simeq F^\tau$ for all τ. Next set $\mathfrak{p} = \langle x, y, z, w \rangle$ and consider $A = S_{\mathfrak{p}} = \mathbb{k}(t)[x, y, z, w]$ and $Q = J_{\mathfrak{p}} = \langle x + tz, y + tw, z^2, zw, w^2 \rangle$. Let H be the minimal free resolution of A/Q over A. One can show that H has the same $(1, 5, 9, 7, 2)$.

Proposition 55.5. *Let $R = K[x_1, \ldots, x_n] = K[\boldsymbol{x}]$, let $\boldsymbol{m} = m_1, \ldots, m_t$ where each m_r is a squarefree monomial and $m_r \nmid m_s$ whenever $r \neq s$ for all $1 \leq r, s \leq t$. Let $i, j \in \{1, \ldots, n\}$ such that $i < j$. Then $x_j - x_i$ is a $R/\boldsymbol{m}$-regular if and only if either x_i is $R/\boldsymbol{m}$-regular or x_j is $R/\boldsymbol{m}$-regular.*

Suppose $f \in R$ such that $(x_j - x_i)f \in \langle \boldsymbol{m} \rangle$. We claim that $x_i x^{\boldsymbol{\alpha}} \in \langle \boldsymbol{m} \rangle$ for all monomials $x^{\boldsymbol{\alpha}}$ of f. Indeed, let $x^{\boldsymbol{\alpha}}$ be a monomial of f. If $x^{\boldsymbol{\alpha}} \in \langle \boldsymbol{m} \rangle$, then clearly $x_i x^{\boldsymbol{\alpha}} \in \langle \boldsymbol{m} \rangle$, so assume $x^{\boldsymbol{\alpha}} \notin \langle \boldsymbol{m} \rangle$. Assume for a contradiction that $x_i x^{\boldsymbol{\alpha}} \notin \langle \boldsymbol{m} \rangle$. Then $x_i x^{\boldsymbol{\alpha}}$ cannot be a monomial of $(x_j - x_i)f \in \langle \boldsymbol{m} \rangle$ (cancellation must occur), thus we must have $x_i x^{\boldsymbol{\alpha}} = x_j x^{\boldsymbol{\alpha} - e_j + e_i}$ where $x^{\boldsymbol{\alpha} - e_j + e_i}$ is another monomial of f. Then since $\langle \boldsymbol{m} \rangle$ is squarefree, we see that $x_i x^{\boldsymbol{\alpha} - e_j + e_i} \notin \langle \boldsymbol{m} \rangle$. Thus we must have $x_i x^{\boldsymbol{\alpha} - e_j + e_i} = x_j x^{\boldsymbol{\alpha} - 2e_j + e_i}$ where $x^{\boldsymbol{\alpha} - 2e_j + e_i}$ is another monomial of f. We cannot continue this process forever, so we have a contradiction. A similar argument shows that $x_j x^{\boldsymbol{\alpha}} \in \langle \boldsymbol{m} \rangle$ for all monomials $x^{\boldsymbol{\alpha}}$ of f. Thus

$$(x_j - x_i)f \in \langle \boldsymbol{m} \rangle \iff x_i f \in \langle \boldsymbol{m} \rangle \text{ and } x_j f \in \langle \boldsymbol{m} \rangle$$

Now let m be a monomial such that $(x_j - x_i)m \in \langle \boldsymbol{m} \rangle$. Then there exists m_r, m_s such that

$$\begin{aligned} m_r m_r' &= x_i m \\ m_s m_s' &= x_j m \end{aligned}$$

Example 55.6. Let $R = \mathbb{k}[x, y, z]$ and let $\boldsymbol{f} = f_1, f_2$ where $f_1 = xz$ and $f_2 = yz$. Then one has

$$\begin{aligned} \mathrm{H}_0(\boldsymbol{f}, R) &= R/\langle xz, yz \rangle \\ \mathrm{H}_1(\boldsymbol{f}, R) &= R/\langle z \rangle \\ \mathrm{H}_2(\boldsymbol{f}, R) &= 0. \end{aligned}$$

In particular, the koszul complex $E = \mathcal{K}(\boldsymbol{f})$ is not a resolution of $R/\langle xz, yz \rangle$ over R since $\mathrm{H}_1(E) \neq 0$. On the other hand, note that if we localize at the prime $\mathfrak{p} = \langle x, y \rangle$, then we have

$$\mathrm{H}_1(\boldsymbol{f}, R_{\mathfrak{p}}) = \mathrm{H}_1(\boldsymbol{f}, R)_{\mathfrak{p}} = 0,$$

so $E_{\mathfrak{p}}$ is a resolution of $R_{\mathfrak{p}}/\langle xz, yz \rangle_{\mathfrak{p}} \cong \mathbb{k}(z)$ over $R_{\mathfrak{p}}$.

55.3.1 Perfect ideals

Definition 55.4. Let $(R, \mathfrak{m})$ be a local noetherian ring and let $I \subseteq \mathfrak{m}$ be an ideal of R. The **grade** of I is defined to be the I-depth of R:

$$g_I := \operatorname{depth}(I, R).$$

In other words, g_I is the maximal length of a regular sequence in I. We say I is **perfect** if

$$g_I = \rho_{R/I} := \operatorname{projdim} R/I$$

where $\rho_{R/I}$ is the projective dimension of R/I over R. If the projective dimension is finite, then by the Auslander Buchsbaum formula, this is equivalent to saying $g_I = \delta_R - \delta_{R/I}$ where

$$\delta_R := \operatorname{depth} R \quad \text{and} \quad \delta_{R/I} := \operatorname{depth} R/I.$$

Suppose I is perfect of grade g. The **type** of I is the dimension of the $\Bbbk$-vector space $\operatorname{Ext}_R^{\delta-g}(\Bbbk, R/I)$. An ideal of grade g is a **complete intersection** if it can be generated by g elements (such an ideal is automatically perfect of type 1). More generally we say that a perfect ideal is **Gorensten** if it has type 1. A perfect ideal of graded g is an **almost complete intersection** if it can be generated by $g+1$ elements.

Proposition 55.6. *Let $(R, \mathfrak{m})$ be a local noetherian ring and let $I = \langle \boldsymbol{t} \rangle = \langle t_1, \dots, t_m \rangle \subseteq \mathfrak{m}$ be a perfect ideal of grade g. Suppose that*

$$\operatorname{depth} R/I = \operatorname{depth} R - m.$$

Then $m = g$ and $\boldsymbol{t}$ is a regular R-sequence.

Proof. Set $\delta = \operatorname{depth} R$ and $\delta' = \operatorname{depth} R/I$. Since I is perfect, we have

$$\begin{aligned} g &= \delta - \delta' \\ &= \delta - \delta + m \\ &= m. \end{aligned}$$

This further implies $\boldsymbol{t}$ is a regular sequence by Corollary (57). □

Remark 92. If I is not perfect, then this need not hold. For instance, consider $R = \Bbbk[x, y]_{\mathfrak{m}}$ where $\mathfrak{m} = \langle x, y \rangle$ and let $I = \langle \boldsymbol{t} \rangle = \langle x^2, xy \rangle$. Then

$$\operatorname{depth}(R/I) = 0 = \operatorname{depth} R - 2,$$

however $\boldsymbol{t}$ is not a regular sequence

55.4 Ext and Depth

Proposition 55.7. *Let R be a noetherian local ring, let N be a finitely-generated R-module, and let I be an ideal of R such that $IN \neq N$, and let n be a positive integer. Then the following are equivalent:*

1. $\operatorname{Ext}_R^i(M, N) = 0$ *for all $i < n$ and all finitely-generated R-modules M with* $\operatorname{Supp} M \subseteq \mathrm{V}(I)$.
2. $\operatorname{Ext}_R^i(R/I, N) = 0$ *for all $i < n$.*
3. $\operatorname{Ext}_R^i(M, N) = 0$ *for all $i < n$ for some finitely-generated R-module M with* $\operatorname{Supp} M = \mathrm{V}(I)$.
4. *I contains an N-sequence of length n.*

Remark 93. Note that if M is a finitely-generated R-module, then $\operatorname{Supp} M = \mathrm{V}(\operatorname{Ann} M)$. Thus we have several equivalent statements:

$$\begin{aligned} M_{\mathfrak{p}} \neq 0 \text{ implies } \mathfrak{p} \supseteq I &\iff \operatorname{Supp} M \subseteq \mathrm{V}(I) \\ &\iff \mathrm{V}(\operatorname{Ann} M) \subseteq \mathrm{V}(I) \\ &\iff \sqrt{\operatorname{Ann} M} \supseteq \sqrt{I} \\ &\iff \sqrt{\operatorname{Ann} M} \supseteq I \\ &\iff \text{if } x \in I \text{ then } x^k M = 0 \text{ for some } k \in \mathbb{N} \\ &\iff I^k M = 0 \text{ for some } k \in \mathbb{N}, \end{aligned}$$

where the last if and only if follows from the fact that R is noetherian.

Proof. That 1 implies 2 implies 3 is clear. Let us prove 3 implies 4. Assume for a contradiction that I consists of zero divisors of N. We will show $\mathrm{Hom}_R(M,N) \neq 0$ which will contradict 3 by taking $i = 0$. Since I consists of zero divisors of N, we see that

$$I \subseteq \bigcup_{\mathfrak{p} \in \operatorname{Ass} N} \mathfrak{p}.$$

It follows from the fact that $\operatorname{Ass} N$ is finite and prime avoidance that I be contained in some associated prime of N, say $I \subseteq \mathfrak{p}$. It follows that there is an injective R-linear map $R/\mathfrak{p} \rightarrowtail N$. By localizing at $\mathfrak{p}$ we obtain an injective $R_\mathfrak{p}$-linear map $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \rightarrowtail N_\mathfrak{p}$. Also $M_\mathfrak{p} \neq 0$ since $\mathfrak{p} \in \mathrm{V}(I) = \operatorname{Supp} M$, and by Nakayama's lemma, we must also have $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \neq 0$. Note that $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ is just an $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$-vector space, thus we can certainly find a surjective $(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p})$-linear map $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \twoheadrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, and hence an $R_\mathfrak{p}$-linear map when viewing these as $R_\mathfrak{p}$-modules. Altogether we obtain a sequence of $R_\mathfrak{p}$-linear maps

$$M_\mathfrak{p} \twoheadrightarrow M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \twoheadrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \rightarrowtail N_\mathfrak{p}.$$

In particular, we see that

$$\begin{aligned} 0 &\neq \mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \\ &= \mathrm{Hom}_R(M,N)_\mathfrak{p}, \end{aligned}$$

which is a contradiction.

Thus I must contain an N-regular element, say $x_1 \in I$. By assumption, $N/IN \neq 0$, hence if $n = 1$, then we are done. Otherwise, assume $n > 1$. From the exact sequence

$$0 \to N \xrightarrow{x_1} N \to N/x_1N \to 0$$

we obtain a long exact sequence in Ext

$$\cdots \to \mathrm{Ext}_R^i(M,N) \to \mathrm{Ext}_R^i(M, N/x_1N) \to \mathrm{Ext}_R^{i+1}(M,N) \to \cdots,$$

which implies $\mathrm{Ext}_R^i(M, N/x_1N) = 0$ for all $i < n-1$. Using induction, this implies that I contains an (N/x_1N)-sequence of length $n-1$, say $x_2, \dots, x_n$. In particular, we see that $x_1, x_2, \dots, x_n$ is an N-sequence of length n.

Now we prove 4 implies 1. Suppose M is a finitely-generated R-module with $\operatorname{Supp} M \subseteq \mathrm{V}(I)$. We will prove by induction on n that for any finitely-generated R-module N, if I contains an N-sequence of length n, then $\mathrm{Ext}_R^i(M,N) = 0$ for all $i < n$. For the base case $n = 1$, suppose $x \in I$ is an N-regular element. In this case, we just need to show that $\mathrm{Hom}_R(M,N) = 0$. Note that since M is finitely-generated, we have $\operatorname{Supp} M = \mathrm{V}(\operatorname{Ann} M)$. Thus we we see that $\mathrm{V}(\operatorname{Ann} M) = \operatorname{Supp} M \subseteq \mathrm{V}(I)$, and this implies $\sqrt{\operatorname{Ann} M} \supseteq I$. In particular, some power of x kills M, say $x^k M = 0$. Thus if $\varphi \in \mathrm{Hom}_R(M,N)$, then for all $u \in M$, we have

$$\begin{aligned} x^k \varphi(u) &= \varphi(x^k u) \\ &= \varphi(0) \\ &= 0, \end{aligned}$$

which implies $\varphi(u) = 0$ since x is N-regular. Thus $\varphi = 0$ and hence $\mathrm{Hom}_R(M,N) = 0$.

For the induction step, suppose $n > 1$ and suppose that for any finitely-generated R-module N' such that I contains an N'-sequence of length $n-1$, we have $\mathrm{Ext}_R^i(M,N') = 0$ for all $i < n-1$. Let N be an R-module such that I contains an N-sequence of length n, say $x_1, \dots, x_n \in I$. Again, since $\sqrt{\operatorname{Ann} M} \supseteq I$, some power of x_1 kills M, say $x_1^k M = 0$. From the exact sequence

$$0 \to N \xrightarrow{x_1^k} N \to N/x_1^k N \to 0$$

we obtain a long exact sequence in Ext

$$\cdots \to \mathrm{Ext}_R^{i-1}(M, N/x_1^k N) \to \mathrm{Ext}_R^i(M,N) \xrightarrow{\cdot x_1^k} \mathrm{Ext}_R^i(M,N) \to \mathrm{Ext}_R^i(M, N/x_1^k N) \to \cdots. \tag{195}$$

Note that x_1^k kills $\mathrm{Ext}_R(M,N)$. To see this, let (E, d) be an injective resolution of N over R. Then for any $\varphi \in \mathrm{Hom}_R^\star(M,E)$, we have $x_1^k \varphi = 0$ by the same argument as in the base case. It follows that x_1^k kills $\mathrm{Hom}_R^\star(M,E)$. In particular, we have

$$\begin{aligned} x_1^k \mathrm{Ext}_R(M,N) &= x_1^k \mathrm{H}(\mathrm{Hom}_R^\star(M,E)) \\ &\rightarrowtail \mathrm{H}(x_1^k \mathrm{Hom}_R^\star(M,E)) \\ &= \mathrm{H}(0) \\ &= 0. \end{aligned}$$

Thus x_1^k kills $\mathrm{Ext}_R(M,N)$ as claimed. It follows that the long exact sequence in homology (195) breaks up into short exact sequences of R-modules

$$0 \to \mathrm{Ext}_R^i(M,N) \to \mathrm{Ext}_R^i(M,N/x_1^kN) \to \mathrm{Ext}_R^{i+1}(M,N) \to 0 \tag{196}$$

for all $i \in \mathbb{Z}$. Now recall that if $x_1, x_2, \dots, x_n$ is an N-sequence, then $x_1^k, x_2, \dots, x_n$ is also an N-sequence. In particular, I contains an (N/x_1^kN)-sequence of length $n-1$. Thus, using induction (with $N' = N/x_1^kN$), we have $\mathrm{Ext}_R^{i+1}(M,N/x_1^kN) = 0$ for all $i+1 < n$. Using this together with the short exact sequence (196) gives us $\mathrm{Ext}_R^i(M,N) = 0$ for all $i < n$. □

Keep the same notation as in Proposition (55.7). Then the proposition above tells us that

$$\mathrm{depth}(I,N) = \inf\{i \mid \mathrm{Ext}_R^i(R/I,N) \neq 0\}.$$

Indeed, denote $q = \mathrm{depth}(I,N)$. Then I contains an N-sequence of length q which implies $\mathrm{Ext}_R^i(R/I,N) = 0$ for all $i < q$. On the other hand, any maximal N-sequence contained in I must also have length q, so we must have $\mathrm{Ext}_R^q(R/I,N) \neq 0$ (otherwise there would be an N-sequence in I of length $q+1$). In fact, we get more than just this from Proposition (55.7). Indeed, if $\sqrt{I}N \neq N$, then Proposition (55.7) also implies

$$\begin{aligned} \mathrm{depth}(I,N) &= \inf\{i \mid \mathrm{Ext}_R^i(R/\sqrt{I},N) \neq 0\}. \\ &= \mathrm{depth}(\sqrt{I},N). \end{aligned}$$

More generally, if J is any ideal of R such that $\sqrt{J} = \sqrt{I}$, then $\mathrm{depth}(I,N) = \mathrm{depth}(J,N)$.

Note also that just as in the Koszul case, we obtain more than what's stated in the theorem above. In particular, denote $y = x_1^k$ in (196) and let $q = \mathrm{depth}(I,N)$. Then (196) gives us an isomorphism

$$\mathrm{Ext}_R^q(M,N) \cong \mathrm{Ext}_R^{q-1}(M,N/yN).$$

This explains Remark (89) in the last section.

Example 55.7. Let $R = K[x,y,z,w]$, let $I = \langle x^2, w^2, zw, xy, y^2z^2\rangle$, and let $\boldsymbol{t} = t_1, t_2, t_3, t_4$ where $\boldsymbol{t}$

$$\begin{aligned} t_1 &= x^2 + w^2 \\ t_2 &= w^2 + zw \\ t_3 &= zw + xy \\ t_4 &= x^3 + w^3. \end{aligned}$$

Now when we apply $\mathrm{Hom}_R(-,R)$ to the following short exact sequence of R-modules

$$0 \longrightarrow I/\langle \boldsymbol{t}\rangle \longrightarrow R/\langle \boldsymbol{t}\rangle \longrightarrow R/I \longrightarrow 0 \tag{197}$$

we obtain an induced map in Ext:

$$\cdots \longrightarrow \mathrm{Ext}^3(I/\langle \boldsymbol{t}\rangle, R) \longrightarrow \mathrm{Ext}^4(R/I,R) \longrightarrow \mathrm{Ext}^4(R/\langle \boldsymbol{t}\rangle, R) \longrightarrow \cdots \tag{198}$$

Note that $\boldsymbol{t}$ is an R-sequence contained in $\langle \boldsymbol{t}\rangle \subseteq I$ of length 4. It follows that $\mathrm{Ext}_R^3(I/\langle \boldsymbol{t}\rangle, R) = 0$ and $\mathrm{Ext}_R^4(R/I,R) = \mathrm{Hom}_R(R/I, R/\langle \boldsymbol{t}\rangle) \neq 0$ and $\mathrm{Ex}_R^4(R/\langle \boldsymbol{t}\rangle, R) = \mathrm{Hom}_R(R/\langle \boldsymbol{t}\rangle, R/\langle \boldsymbol{t}\rangle) \neq 0$.

56 Cohen-Macaulay Modules

Let $(R, \mathfrak{m}, \Bbbk)$ be a local noetherian ring and let M be a nonzero finitely generated R-module. Recall that the **depth** of M is the supremum of the lengths of all M-regular sequences and we denote it by $\delta_M = \mathrm{depth}\, M$. We saw earlier that this can be measured in terms of homological algebra in at least a few ways:

1. We can calculate the depth using Koszul homology. In particular, suppose $\dim R = d$ and let $\boldsymbol{x} = x_1, \dots, x_d \in \mathfrak{m}$ be a system of parameters for R; thus $\sqrt{\langle \boldsymbol{x}\rangle} = \mathfrak{m}$. The assumption that $M \neq 0$ implies $\mathrm{H}_0(\boldsymbol{x}, M) = M/\boldsymbol{x}M \neq 0$ by Nakayama's lemma, therefore supremum $\tau = \sup\{i \mid \mathrm{H}_i(\boldsymbol{x}, M) \neq 0\}$ makes sense (since $\{i \mid \mathrm{H}_i(\boldsymbol{x}, M) \neq 0\}$ is bounded above also). In this case, we have

$$\delta_M = d - \tau.$$

In particular, we have $\mathrm{H}_d(\boldsymbol{x}, M) = 0 :_M \boldsymbol{x} \neq 0$ if and only if $\mathfrak{m}$ consists of zerodivisors on M if and only if $\delta_M = 0$. Note that we can also replace $\boldsymbol{x}$ with another sequence $\boldsymbol{y} = y_1, \dots, y_n$ such that $\sqrt{\langle \boldsymbol{y}\rangle} = \mathfrak{m}$ (so necessarily we must have $n \geq d$) and calculate the depth using the supremum of $\{i \mid \mathrm{H}_i(\boldsymbol{y}, M) \neq 0\}$:

$$\delta_M = n - \sup\{i \mid \mathrm{H}_i(\boldsymbol{y}, M) \neq 0\}.$$

2. We can calculate the depth using Ext. In particular, set $\sigma = \inf\{i \mid \mathrm{Ext}^i_R(\Bbbk, M) \neq 0\}$ (this makes sense because $M \neq 0$ is finitely generated and R is noetherian). Then we have

$$\delta_M = \sigma.$$

In particular, we have $\mathrm{Ext}^0_R(\Bbbk, M) = \mathrm{Hom}_R(\Bbbk, M) \neq 0$ if and only if $\mathfrak{m}$ consists of zerodivisors on M if and only if $\delta_M = 0$. Note that we can replace $\Bbbk$ by an finitely generated R-module L such that $\sqrt{\mathrm{Ann}\, L} = \mathfrak{m}$ and calculate depth using the infimum of $\{i \mid \mathrm{Ext}^i_R(L, M) \neq 0\}$:

$$\delta_M = \inf\{i \mid \mathrm{Ext}^i_R(L, M) \neq 0\}.$$

3. If M happens to have finite projective dimension, then the famous Auslander-Buchsbaum formula (which we prove later) says

$$\delta_M = \delta_R - \rho_M,$$

where $\rho_M = \mathrm{pd}_R M$ is the projective dimension of M and $\delta_R = \operatorname{depth} R$ is the depth of R. In particular, if M is free, then $\delta_M = \delta_R$.

4. Finally, we can calculate the depth of M by finding a maximal M-sequence $\boldsymbol{z} = z_1, \dots, z_\delta$ contained in $\mathfrak{m}$. How does one go about doing this? The idea is to *avoid* associated primes: we have $\delta_M = 0$ if and only if $\mathfrak{m}$ consists of zerodivisors on M, so there's nothing to consider here; assume $\delta_M > 0$. Note that if $z \in \mathfrak{m}$, then z is a zerodivisor on M if and only if z is contained in an associated prime of M. Said differently, z is a nonzerodivisor on M if and only if $z \notin \bigcup_{\mathfrak{p} \in \mathrm{Ass} M} \mathfrak{p}$. Thus to get the M-sequence started, we choose $z_1 \in \mathfrak{m} \backslash \bigcup_{\mathfrak{p} \in \mathrm{Ass} M} \mathfrak{p}$. Now before preceding further, we wish to make the following important remark: denote $I = \mathrm{Ann}\, M$. We have

$$\bigcup_{\mathfrak{q} \in \mathrm{Ass}\, R/I} \mathfrak{q} \subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}\, M} \mathfrak{p}.$$

Indeed, this follows from the fact that there is an injective map $R/I \rightarrowtail M^n$ given by $\overline{1} \mapsto (u_1, \dots, u_n)$ where M is generated by $u_1, \dots, u_n$, and thus every associated prime of R/I is an associated prime of M. With this remark understood, notice that since if z_1 is a nonzerodivisor on M, we have

$$\delta_{M/z_1} = \delta_M - 1,$$

and since z_1 avoids all associated primes of R/I, we have

$$\begin{aligned}
\dim(M/z_1 M) &:= \dim(R/\mathrm{Ann}(M/z_1 M)) \\
&= \dim(R/\langle I, z_1\rangle) \\
&= \dim(R/I) - 1 \\
&= \dim M - 1.
\end{aligned}$$

Thus going from $M_0 := M$ to $M_1 := M/z_1 M$ decreases depth and dimension by one. Now if $\delta_{M_1} = 0$, then we are done: z_1 is a maximal M-sequence of length one. On the other hand, if $\delta_{M_1} > 0$, we repeat the same process as before: choose $z_2 \in \mathfrak{m} \backslash \bigcup_{\mathfrak{p} \in \mathrm{Ass} M_1} \mathfrak{p}$ and set $M_2 := M/\langle z_1, z_2\rangle M$. Then we have $\delta_{M_2} = \delta_M - 2$ and $\dim M_2 = \dim M - 2$. We continue this process until we construct a maximal M-sequence $\boldsymbol{z} = z_1 \dots, z_\varepsilon$ where $M_\delta := M/\langle \boldsymbol{z}\rangle M$ satisfies $\operatorname{depth} M_\delta = 0$ and $\dim M_\delta = \dim M - \delta_M$.

By the remark 4 above, it is clear that we always have $\dim M \geq \operatorname{depth} M$. When the converse happens, we give M a special name:

Definition 56.1. We say M is a **Cohen-Macaulay module** (or **CM module** for short) if $\operatorname{depth} M = \dim M$. If $\operatorname{depth} M = \dim R$, then M is called **maximal Cohen-Macaulay**. We say R is a **Cohen-Macaulay ring** if it is a Cohen-Macaulay R-module.

Now suppose R is CM and suppose M is maximal CM. Let $d = \dim R$ and let $\boldsymbol{x} = x_1, \dots, x_d \in \mathfrak{m}$ be a system of parameters for R. Since $\operatorname{depth} R = d$ we know by 1 above that $\mathrm{H}_0(\boldsymbol{x}, M) = M/\boldsymbol{x}M \neq 0$ and $\mathrm{H}_i(\boldsymbol{x}, M) = 0$ for all $i > 0$. It follows from Theorem (55.8) that $\boldsymbol{x}$ is already an M-sequence!

Lemma 56.1. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M and N be nonzero finitely-generated R-modules. Then $\mathrm{Ext}^i_R(M, N) \cong 0$ for all $i < \operatorname{depth} N - \dim M$.*

Proof. Denote $q = \operatorname{depth} N$ and $d = \dim M$. We prove the lemma by induction on d. If $d = 0$, then $\sqrt{\mathrm{Ann}\, M} = \mathfrak{m}$. Therefore $\mathrm{Ext}^i_R(M, N) \cong 0$ for all $i < q$ by Lemma (56.2). Now assume that $d > 0$. Choose a filtration of M, say

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = \langle 0 \rangle$$

wher $M_j/M_{j+1} \cong R/\mathfrak{p}_j$ for suitable prime ideals $\mathfrak{p}_j$. Now it is sufficient to prove $\mathrm{Ext}^i_R(M_j/M_{j+1}, N) \cong 0$ for all j and $i < q - d$ because this implies $\mathrm{Ext}^i_R(M, N) \cong 0$. Since $\dim(M_j/M_{j+1}) \le \dim M$ for all j, we may as well assume that $M = R/\mathfrak{p}$ for a prime ideal $\mathfrak{p}$. Since $\dim(R/\mathfrak{p}) > 0$, we must have $\mathfrak{m} \supset \mathfrak{p}$ where the inclusion containment is proper. Therefore we can choose an $x \in \mathfrak{m}$ which is not in $\mathfrak{p}$. Consider the short exact sequence

$$0 \to R/\mathfrak{p} \xrightarrow{x} R/\mathfrak{p} \to R/\langle \mathfrak{p}, x\rangle \to 0. \tag{199}$$

This short exact sequence (199) gives rise to the following long exact sequence in Ext

$$\cdots \to \mathrm{Ext}^i_R(R/\langle \mathfrak{p}, x\rangle, N) \to \mathrm{Ext}^i_R(R/\mathfrak{p}, N) \xrightarrow{x} \mathrm{Ext}^i_R(R/\mathfrak{p}, N) \to \mathrm{Ext}^{i+1}_R(R/\langle \mathfrak{p}, x\rangle, N) \to \cdots \tag{200}$$

Since $\dim(R/\langle \mathfrak{p}, x\rangle) < d$, we obtain by induction on d that $\mathrm{Ext}^i_R(R/\langle \mathfrak{p}, x\rangle, N) \cong 0$ for all $i < q - d + 1$. Using this together with the long exact sequence (200), we find find that the map

$$\mathrm{Ext}^i_R(R/\mathfrak{p}, N) \xrightarrow{x} \mathrm{Ext}^i_R(R/\mathfrak{p}, N)$$

is surjective for all $i < q - d$ which implies $\mathrm{Ext}^i_R(R/\mathfrak{p}, N) \cong 0$ for all $i < q - d$ by Nakayama's lemma. □

Lemma 56.2. *Let $(A, \mathfrak{m})$ be a local Cohen-Macaulay ring of dimension d, M be a maximal Cohen-Macaulay module of finite injective dimension, and N a finitely generated module of depth e. Then*

$$Ext^i_A(N, M) = 0 \text{ for } i > depth(M) - depth(N) = d - e.$$

Proof. We do induction on e. □

Proposition 56.1. *Let R be a local Cohen-Macaulay ring of dimension d, and let N be a maximal Cohen-Macaulay module of finite injective dimension.*

1. *If M is a finitely generated R-module of depth q, then $\mathrm{Ext}^i_R(M, N) \cong 0$ for $i > d - q$.*
2. *If x is a nonzerodivisor on M, then x is a nonzerodivisor on $Hom_A(N, M)$. If N is also a maximal Cohen-Macaulay module, then*

   $$Hom_A(N, M)/xHom_A(N, M) \cong Hom_{A/x}(N/xN, M/xM)$$

   by the homomorphism taking the class of a map $\varphi : N \to M$ to the map $N/xN \to M/xM$ induced by φ.

Proof. We do induction on q. By Proposition (57.8), the injective dimension of N is d, so that $\mathrm{Ext}^i_R(M, N) \cong 0$ for any M if $i > d$. This gives the case $e = 0$. Now suppose $e > 0$, and let x be a nonzerodivisor on N that lies in the maximal ideal of A. From the short exact sequence

$$0 \longrightarrow N \xrightarrow{\cdot x} N \longrightarrow N/xN \longrightarrow 0$$

we get a long exact sequence

$$\cdots \longrightarrow \mathrm{Ext}^j_A(N, M) \xrightarrow{\cdot x} \mathrm{Ext}^j_A(N, M) \longrightarrow \mathrm{Ext}^{j+1}_A(N/xN, M) \longrightarrow \cdots$$

The module N/xN has depth $e - 1$, so by induction $\mathrm{Ext}^{j+1}_A(N/xN, M)$ vanishes if $j + 1 > d - (e - 1)$, that is, if $j > d - e$. By Nakayama's lemma, $\mathrm{Ext}^j_A(N, M)$ vanishes if $j > d - e$.

1. We do induction on e. By Proposition (57.8), the injective dimension of M is d, so that $\mathrm{Ext}^j_A(N, M) = 0$ for any N if $j > d$. This gives the case $e = 0$. Now suppose $e > 0$, and let x be a nonzerodivisor on N that lies in the maximal ideal of A. From the short exact sequence

   $$0 \longrightarrow N \xrightarrow{\cdot x} N \longrightarrow N/xN \longrightarrow 0$$

   we get a long exact sequence

   $$\cdots \longrightarrow \mathrm{Ext}^j_A(N, M) \xrightarrow{\cdot x} \mathrm{Ext}^j_A(N, M) \longrightarrow \mathrm{Ext}^{j+1}_A(N/xN, M) \longrightarrow \cdots$$

   The module N/xN has depth $e - 1$, so by induction $\mathrm{Ext}^{j+1}_A(N/xN, M)$ vanishes if $j + 1 > d - (e - 1)$, that is, if $j > d - e$. By Nakayama's lemma, $\mathrm{Ext}^j_A(N, M)$ vanishes if $j > d - e$.
2. From the short exact sequence

$$0 \longrightarrow M \xrightarrow{\cdot x} M \longrightarrow M/xM \longrightarrow 0$$

we derive a long exact sequence beginning

$$0 \longrightarrow \operatorname{Hom}_A(N, M) \xrightarrow{\cdot x} \operatorname{Hom}_A(N, M) \longrightarrow \operatorname{Hom}_A(N, M/xM) \longrightarrow \operatorname{Ext}^1_A(N, M) \longrightarrow \cdots$$

Thus x is a nonzerodivisor on $\operatorname{Hom}_A(N, M)$. If N is a maximal Cohen-Macaulay module then $\operatorname{depth}(N) = d$, so $\operatorname{Ext}^1_A(N, M) = 0$ by part 1. Every homomorphism $N \to M/xM$ factors uniquely through N/xN, so $\operatorname{Hom}_A(N, M/xM) = \operatorname{Hom}_A(N/xN, M/xM)$. The short exact sequence above thus becomes

$$0 \longrightarrow \operatorname{Hom}_A(N, M) \xrightarrow{\cdot x} \operatorname{Hom}_A(N, M) \longrightarrow \operatorname{Hom}_A(N/xN, M/xM) \longrightarrow 0$$

Since $\operatorname{Hom}_A(M/xM, N/xN) = \operatorname{Hom}_{A/x}(N/xN, M/xM)$, this proves part 2.

□

Proposition 56.2. *Let $(A, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated A-module. Then $\dim(A/\mathfrak{p}) \geq \operatorname{depth}(M)$ for all $\mathfrak{p} \in \operatorname{Ass}(M)$.*

Proof. Let $\mathfrak{p} \in \operatorname{Ass}(M)$, that is, $\mathfrak{p} = 0 : m$ for some nonzero m in M. This implies that $\operatorname{Hom}(A/\mathfrak{p}, M) \neq 0$, because $1 \mapsto m$ defines a non-trivial homomorphism. Hence, by Lemma (56.2), we obtain $0 \geq \operatorname{depth}(M) - \dim(A/\mathfrak{p})$. □

Theorem 56.3. *Let $(A, \mathfrak{m})$ be a Noetherian local ring, $M \neq 0$ a finitely generated A-module, and $x \in A$.*

1. *Let M be Cohen-Macaulay. Then $\dim(A/\mathfrak{p}) = \dim(M)$ for all $\mathfrak{p} \in \operatorname{Ass}(M)$.*
2. *If $\dim(M/xM) = \dim(M) - 1$, then x is M-regular.*
3. *Let $x_1, \ldots, x_r \in \mathfrak{m}$ be an M-sequence. Then M is Cohen-Macaulay if and only if $M/\langle x_1, \ldots, x_r\rangle M$ is Cohen-Macaulay.*
4. *If M is Cohen-Macaulay, then $M_\mathfrak{p}$ is Cohen-Macaulay for all prime ideal $\mathfrak{p}$ and $\operatorname{depth}(\mathfrak{p}, M) = \operatorname{depth}_{A_\mathfrak{p}}(M_\mathfrak{p})$ if $M_\mathfrak{p} \neq 0$.*

Proof.

1. For all associated primes $\mathfrak{p}$ of M, we have
$$\operatorname{depth}(M) \leq \dim(A/\mathfrak{p}) \leq \dim(M).$$
Thus $\dim(A/\mathfrak{p}) = \dim(M)$ for all $\mathfrak{p} \in \operatorname{Ass}(M)$ since $\operatorname{depth}(M) = \dim(M)$.
2. Observe that
$$\begin{aligned}\dim(A/\langle x, \operatorname{Ann}(M)\rangle) &= \dim(M/xM) \\ &< \dim(M) \\ &= \dim(A/\mathfrak{p})\end{aligned}$$
implies $x \notin \mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Ass}(M)$. Therefore x is M-regular.
3. We have
$$\begin{aligned}\operatorname{depth}(M/\langle x_1, \ldots, x_r\rangle M) &= \operatorname{depth}(M) - r \\ &= \dim(M) - r \\ &= \dim(M/\langle x_1, \ldots, x_r\rangle M).\end{aligned}$$

□

56.1 Auslander-Buchsbaum Formula

We want to prove the Auslander-Buchsbaum formula, which is of fundamental importance for modules which allow a finite projective resolution. First we need a definition and a lemma.

Definition 56.2. Let $(A, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated A-module. We say M has finite **projective dimension** if there exists an exact sequence (a free resolution)

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \longrightarrow F_0 \xrightarrow{\varphi_0} M \longrightarrow 0 \tag{201}$$

with finitely generated free A-modules F_i. The integer n is called the **length** of the resolution. The minimal length of a free resolution is called the **projective dimension** of M, and is denoted $\operatorname{pd}_A(M)$.

Lemma 56.4. *Let $(R, \mathfrak{m}, \Bbbk)$ be a noetherian local ring and let*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{202}$$

be a short exact sequence of R-modules. Set $\delta_i := \operatorname{depth} M_i$ for each $i = 1, 2, 3$. Then we have the following inequalities:

$$\begin{aligned} \delta_1 &\geq \min\{\delta_2, \delta_3 + 1\} \\ \delta_2 &\geq \min\{\delta_1, \delta_3\} \\ \delta_3 &\geq \min\{\delta_1 - 1, \delta_2\}. \end{aligned} \tag{203}$$

In particular, the triple $(\delta_1, \delta_2, \delta_3)$ has one of the following forms:

$$\begin{aligned} (\delta_1, \delta_2, \delta_3) &= (\varepsilon, 0, 0) + (\delta, \delta, \delta) \\ (\delta_1, \delta_2, \delta_3) &= (1, \varepsilon, 0) + (\delta, \delta, \delta) \\ (\delta_1, \delta_2, \delta_3) &= (0, 0, \varepsilon) + (\delta, \delta, \delta) \\ (\delta_1, \delta_2, \delta_3) &= (0, 0, 0) \end{aligned}$$

where $\varepsilon > 0$ and $\delta \geq 1$.

Proof. Applying $\operatorname{Ext}_R(\Bbbk, -)$ to (202) gives us a long exact sequence in Ext modules:

$$\cdots \longrightarrow \operatorname{Ext}_R^{i-1}(\Bbbk, M_3) \longrightarrow \operatorname{Ext}_R^{i}(\Bbbk, M_1) \longrightarrow \operatorname{Ext}_R^{i}(\Bbbk, M_2) \longrightarrow \operatorname{Ext}_R^{i}(\Bbbk, M_3) \longrightarrow \operatorname{Ext}_R^{i+1}(\Bbbk, M_1) \longrightarrow \cdots.$$

Observe that $\operatorname{Ext}_R^i(\Bbbk, M_2)$ vanishes if both $\operatorname{Ext}_R^i(\Bbbk, M_1)$ and $\operatorname{Ext}_R^i(\Bbbk, M_3)$ vanish. Therefore the second inequality in (203) follows from the Ext characterization of depth. Similar arguments show the other inequalities. □

Proof. First assume all three modules have positive depth. Observe that we can find a common nonzerodivisor $x \in \mathfrak{m}$ of M_1, M_2 and M_3. Indeed, the set of all zerodivisors of M_j is

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass}(M_j)} \mathfrak{p}.$$

Assuming for a contradiction that we cannot find a common nonzerodivisor $x \in \mathfrak{m}$ of M_1,M_2, and M_3, then we would have

$$\bigcup_{\substack{\mathfrak{p} \in \operatorname{Ass}(M_j) \\ j = 1,2,3}} \mathfrak{p} = \mathfrak{m}.$$

Since the number associated primes is finite, we must have $\mathfrak{m} = \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass}(M_j)$ and $j \in \{1, 2, 3\}$, by prime avoidance. However this is a contradiction, since it would imply that every $x \in \mathfrak{m}$ is a zerodivisor for M_j. Thus we can find a common nonzerodivisor $x \in \mathfrak{m}$ of M_1, M_2, and M_3.

Since x is M_3-regular, we obtain a short exact sequence

$$0 \to M_1/xM_1 \to M_2/xM_2 \to M_3/xM_3 \to 0$$

Since depth drops by one when we divide by x, we see that the proof of the lemma can be reduced to the case that the depth of one of the M_j is zero.

Case 1: Suppose that $\operatorname{depth} M_1 = 0$. Then $\operatorname{depth} M_2 = 0$, because any nonzerodivisor of M_2 is a nonzerodivisor of M_1. The lemma is proved in this case.

Case 2: Suppose that $\operatorname{depth} M_2 = 0$ and assume for a contradiction that $\operatorname{depth} M_1 > 0$ and $\operatorname{depth} M_3 > 0$. Let $x \in \mathfrak{m}$ be a common nonzerodivisor of M_1 and M_3. From the snake lemma we obtain that x is a nonzerodivisor for M_2 too. This is a contradiction.

Case 3: Suppose that $\operatorname{depth} M_3 = 0$. If $\operatorname{depth} M_2 > 0$, let $x \in \mathfrak{m}$ be a nonzerodivisor of M_2. This is also a nonzero divisor for M_1, and therefore $\operatorname{depth} M_1 > 0$. Using the snake lemma, we obtain an injective map

$$\ker(M_3 \xrightarrow{x} M_3) \rightarrowtail M_1/xM_1.$$

As $\operatorname{depth} M_3 = 0$, we have $\ker(M_3 \xrightarrow{x} M_3) \neq 0$. Any nonzerodivisor of M_1/xM_1 would give a nonzerodivisor of $\ker(M_3 \xrightarrow{x} M_3)$. But this is not possible, and therefore $\operatorname{depth} M_1 = 1$. □

Lemma 56.5. *Let $(R, \mathfrak{m}, \Bbbk)$ be a Noetherian local ring and let*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{204}$$

be a short exact sequence of R-modules. Then

$$\operatorname{depth} M_2 \geq \min(\operatorname{depth} M_1, \operatorname{depth} M_3).$$

If the inequality is strict, then

$$\operatorname{depth} M_1 = \operatorname{depth} M_3 + 1.$$

Proof. First assume all three modules have positive depth. Observe that we can find a common nonzerodivisor $x \in \mathfrak{m}$ of M_1, M_2 and M_3. Indeed, the set of all zerodivisors of M_j is

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass}(M_j)} \mathfrak{p}.$$

Assuming for a contradiction that we cannot find a common nonzerodivisor $x \in \mathfrak{m}$ of M_1,M_2, and M_3, then we would have

$$\bigcup_{\substack{\mathfrak{p} \in \operatorname{Ass}(M_j) \\ j=1,2,3}} \mathfrak{p} = \mathfrak{m}.$$

Since the number associated primes is finite, we must have $\mathfrak{m} = \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass}(M_j)$ and $j \in \{1, 2, 3\}$, by prime avoidance. However this is a contradiction, since it would imply that every $x \in \mathfrak{m}$ is a zerodivisor for M_j. Thus we can find a common nonzerodivisor $x \in \mathfrak{m}$ of M_1, M_2, and M_3.

Since x is M_3-regular, we obtain a short exact sequence

$$0 \to M_1/xM_1 \to M_2/xM_2 \to M_3/xM_3 \to 0$$

Since depth drops by one when we divide by x, we see that the proof of the lemma can be reduced to the case that the depth of one of the M_j is zero.

Case 1: Suppose that $\operatorname{depth} M_1 = 0$. Then $\operatorname{depth} M_2 = 0$, because any nonzerodivisor of M_2 is a nonzerodivisor of M_1. The lemma is proved in this case.

Case 2: Suppose that $\operatorname{depth} M_2 = 0$ and assume for a contradiction that $\operatorname{depth} M_1 > 0$ and $\operatorname{depth} M_3 > 0$. Let $x \in \mathfrak{m}$ be a common nonzerodivisor of M_1 and M_3. From the snake lemma we obtain that x is a nonzerodivisor for M_2 too. This is a contradiction.

Case 3: Suppose that $\operatorname{depth} M_3 = 0$. If $\operatorname{depth} M_2 > 0$, let $x \in \mathfrak{m}$ be a nonzerodivisor of M_2. This is also a nonzero divisor for M_1, and therefore $\operatorname{depth} M_1 > 0$. Using the snake lemma, we obtain an injective map

$$\ker(M_3 \xrightarrow{x} M_3) \rightarrowtail M_1/xM_1.$$

As $\operatorname{depth} M_3 = 0$, we have $\ker(M_3 \xrightarrow{x} M_3) \neq 0$. Any nonzerodivisor of M_1/xM_1 would give a nonzerodivisor of $\ker(M_3 \xrightarrow{x} M_3)$. But this is not possible, and therefore $\operatorname{depth} M_1 = 1$. □

Example 56.1. Let $R = \Bbbk[x,y,z,w]$ and let $I = \langle x^2, xy, xz, xw\rangle$. Then we have $I : x = \langle x,y,z,w\rangle$ and $\langle I, x\rangle = \langle x\rangle$, so we have a short exact sequence of R-modules

$$0 \longrightarrow \Bbbk \longrightarrow R/I \longrightarrow \Bbbk[y,z,w] \longrightarrow 0. \tag{205}$$

We have $\operatorname{depth} \Bbbk = 0 = \operatorname{depth} R/I$ but $\operatorname{depth} \Bbbk[y,z,w] = 3$. On the other hand, we have $I : y = \langle x\rangle$ and $\langle I, y\rangle = \langle x^2, y, xz, xw\rangle$, so we have a short exact sequence of R-modules

$$0 \longrightarrow \Bbbk[y,z,w] \longrightarrow R/I \longrightarrow R/\langle I, y\rangle \longrightarrow 0. \tag{206}$$

This time we have $\operatorname{depth} R/I = 0 = \operatorname{depth} R/\langle I,y\rangle$ but $\operatorname{depth} \Bbbk[y,z,w] = 3$.

We are now ready to state the Auslander-Buchsbaum Formula.

Theorem 56.6. *(Auslander-Buchsbaum Formula) Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module of finite projective dimension. Then*

$$\operatorname{depth} M + \operatorname{pd}_R M = \operatorname{depth} R.$$

Proof. Denote $q_M = \operatorname{depth} M$, $q_R = \operatorname{depth} R$, and $p = \operatorname{pd}_R M$. The proof is by induction on q_R. First assume $q_R = 0$. Then $\mathfrak{m}$ consists of zerodivisors. In particular,

$$\mathfrak{m} \subseteq \bigcup_{\mathfrak{p} \in \operatorname{Ass} R} \mathfrak{p},$$

and since the number of associated primes of R is finite (R is Noetherian!), we must have $\mathfrak{m} = \mathfrak{p}$ for some associated prime by prime avoidance. Therefore, there exists a nonzero $x \in R$ such that $x\mathfrak{m} = 0$. Choose such an $x \in R$ and let (F, d) be a minimal free resolution of M over R of finite length n. If $n > 0$, then by minimality of the resolution, we have

$$\begin{aligned} \mathrm{d}_n(xF_n) &= x\mathrm{d}_n(F_n) \\ &\subseteq x\mathfrak{m}F_{n-1} \\ &= 0. \end{aligned}$$

This implies $xF_n = 0$ since d_n is injective, and thus $F_n = 0$ since F_n is free. This contradicts the minimality of the resolution. In particular, we must have $n = 0$, which implies $F_0 \cong M$. In other words, we have $p = 0$ and $q_M = q_R$.

Now we assume $q_R > 0$ and $q_M > 0$. Let $x \in \mathfrak{m}$ be a common nonzerodivisor of both M and R (such an element exists since both M and R have positive depth). Then the projective dimension is constant if we divide by x, that is,

$$\operatorname{pd}_{R/x}(M/xM) = \operatorname{pd}_R M,$$

but the depth drops by one. This is because the sequence if (F, d) is a minimal free resolution of M over R, then $(F/xF, \overline{\mathrm{d}})$ is a minimal free resolution of M/xM over R/xR as long as x is both M-regular and R-regular. It follows from the induction hypothesis, that

$$\begin{aligned} \operatorname{pd}_R M + \operatorname{depth}_R M &= \operatorname{pd}_{R/x}(M/xM) + \operatorname{depth}_{R/x}(M/xM) + 1 \\ &= \operatorname{depth}_{R/x}(R/x) + 1 \\ &= \operatorname{depth}_R R. \end{aligned}$$

Finally, assume $q_R > 0$ and $q_M = 0$. Then $p > 0$, because otherwise M would be free and we would have $q_M = q_R > 0$, which is a contradiction. Let

$$0 \to N \to F \to M \to 0$$

be a short exact sequence of R-modules where F is a finitely-generated free R-module and where $0 \neq N \subseteq \mathfrak{m}F$. We apply Lemma (56.5) and obtain $\operatorname{depth} N = 1$. Therefore by the previous case, we have

$$\begin{aligned} \operatorname{depth} M + \operatorname{pd}_R M &= \operatorname{depth} N - 1 + \operatorname{pd}_R N + 1 \\ &= \operatorname{depth} N + \operatorname{pd}_R N \\ &= \operatorname{depth} R. \end{aligned}$$

□

Example 56.2. Let $R = K[x,y,z]_{\langle x,y,z\rangle}$ and let $I = \langle xz, yz\rangle$. The minimal free resolution of R/I over R is given by

$$0 \longrightarrow R \xrightarrow{\begin{pmatrix} -y \\ x \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} xz & yz \end{pmatrix}} R \longrightarrow 0$$

In particular, $\mathrm{pd}_R(R/I) = 2$, and hence $\mathrm{depth}(R/I) = 1$ since $\mathrm{depth}\, R = 3$. On the other hand, we know that $\dim(R/I) \geq 2$, since

$$\langle \overline{x}, \overline{y}, \overline{z}\rangle \supset \langle \overline{y}, \overline{z}\rangle \supset \langle \overline{z}\rangle$$

gives a chain of prime ideals of length 2. Therefore R/I is not a Cohen-Macaulay R-module.

Example 56.3. Let $R = K[x,y,z]_{\langle x,y,z\rangle}$ and let $I = \langle xy, xz, yz\rangle$. The minimal free resolution of R/I over R is given by

$$0 \longrightarrow R^2 \xrightarrow{\begin{pmatrix} 0 & -z \\ -y & y \\ x & 0 \end{pmatrix}} R^3 \xrightarrow{\begin{pmatrix} xy & xz & yz \end{pmatrix}} R \longrightarrow 0$$

So $\mathrm{pd}_R(R/I) = 2$, and hence $\mathrm{depth}(R/I) = 1$ since $\mathrm{depth}\, R = 3$. We also have $\dim(R/I) = 1$, so R/I is a Cohen-Macaulay R-module.

57 Duality Canonical Modules, and Gorenstein Rings

Unless otherwise specified, let K be a field and let R be a local zero-dimensional ring that is finite-dimensional as a K-algebra. If we wish to imitate the usual duality theory for vector spaces, we might at first try to work with the functor $\mathrm{Hom}_R(-, R)$. But this is often very badly behaved; for example, it does not usually preserve exact sequences, and if we do it twice we do not get the identity, that is,

$$\mathrm{Hom}_R(\mathrm{Hom}_R(M, R), R) \not\cong M$$

in general. For instance, consider the following example. For instance, consider the case where $M = R/I$ where I is an ideal of R. Then $\mathrm{Hom}_R(R/I, R) \cong \mathrm{Ann}\, I$, but in general we need not have $\mathrm{Hom}_R(\mathrm{Ann}\, I, R) \cong R/I$.

57.1 Dualizing Functors

Lemma 57.1. *Let E be an R-linear functor from the category of R-modules to itself such that $E^2 \cong 1$. Then we have an isomorphism of functors $E(-) \cong \mathrm{Hom}_R(-, E(R))$.*

Proof. Since $E^2 \cong 1$ as functors, the map $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(E(N), E(M))$ given by $\varphi \mapsto E(\varphi)$ is an isomorphism. Thus, there is an isomorphism, functorial in M,

$$\begin{aligned} E(M) &\cong \mathrm{Hom}_R(R, E(M)) \\ &\cong \mathrm{Hom}_R(E(E(M)), E(R)) \\ &\cong \mathrm{Hom}_R(M, E(R)). \end{aligned}$$

□

Definition 57.1. Let D be a contravariant functor from the category of finitely-generated R-modules to itself. We say D is a **dualizing functor** if it is R-linear, exact, and D^2 is naturally isomorphic to the identity functor.

By Lemma (57.1), we see that if D is a dualizing functor, then it is must take the form $\mathrm{Hom}_R(-, D(R))$ for some R-module $D(R)$. Furthermore, note that $\mathrm{Hom}_R(-, D(R))$ is exact if and only if $D(R)$ is an injective R-module.

Proposition 57.1. *Let D bea dualizing functor from the category of finitely-generated R-modules to itself.*

1. *Suppose $\mathfrak{m}$ is a maximal ideal of R. Then D takes the simple module $R/\mathfrak{m}$ to an isomorphic copy of itself.*

2. *Suppose M is a finitely-generated R-module of finite length. Then $D(M)$ has finite length and* $\mathrm{length}\, M = \mathrm{length}\, D(M)$.

3. *d*

4. *s*

Proof. □

A good duality theory may be defined in a different way: If M is a finitely generated R-module, we provisionally define the dual of M to be

$$D(M) = \mathrm{Hom}_K(M, K)$$

The vector space $D(M)$ is naturally an R-module by the action

$$(a\varphi)(u) = \varphi(au)$$

for all $a \in R$, $\varphi \in D(M)$, and $u \in M$. With D defined above, we see that D a contravariant functor from the category of finitely generated R-modules to itself. Since M is finite-dimensional over K, the natural map $M \to D(D(M))$ sending $u \in M$ to the functional $\widehat{u} : \varphi \mapsto \varphi(u)$, for $\varphi \in \mathrm{Hom}_K(M, K)$ is an isomorphism of vector spaces. In fact, it is an isomophism of R-modules. Indeed, we have $\widehat{au} = a\widehat{u}$ since

$$\begin{aligned}(a\widehat{u})(\varphi) &= \widehat{u}(a\varphi)\\ &= (a\varphi)(u)\\ &= \varphi(au)\\ &= \widehat{au}(\varphi)\end{aligned}$$

for all $\varphi \in D(M)$. Since K is a field, D is **exact** in the sense that it takes exact sequences to exact sequences (with arrows reversed). Thus D is a dualizing functor on the category of finitely generated R-modules.

To get an idea of how D acts, note first that if $\mathfrak{m}$ is a maximal ideal of R, then any dualizing functor D takes the simple module $R/\mathfrak{m}$ to itself. Indeed, $D(R/\mathfrak{m})$ must be simple, because else it would have a proper factor module M and then $D(M)$ would be a proper submodule of $R/\mathfrak{m}$. As R is local, it has only one simple module up to isomorphism, and thus $D(R/\mathfrak{p}) \cong R/\mathfrak{p}$. Since D takes exact sequences to exact sequences, reversing the arrows, D "turns composition series upside down" in the sense that if

$$0 \subset M_1 \subset \cdots \subset M_n \subset M$$

is a chain of modules with simple quotients $M_i/M_{i-1} \cong R/\mathfrak{m}$, then

$$D(M) \supset D(M_n) \supset \cdots \supset D(M_1) \supset D(0) = 0$$

is a chain of surjections whose kernels N_i are simple. In particular, for any module of finite length, then length of $D(M)$ equals the length of M.

57.2 Top and Socle of Module

A central role in the theory of modules over a local ring $(R, \mathfrak{m})$ is played by what might be thought of as the **top** of a module M, defined to be the quotient

$$\mathrm{Top}\, M := M/\mathfrak{m}M.$$

Nakayama's lemma shows that this quotient controls the generators of M. It could be defined categorically as the largest quotient of M that is a direct sum of simple modules. That is,

$$M/\mathfrak{m}M = \bigoplus_i R/\mathfrak{m}.$$

The dual notion is that of the **socle** of M, defined to be

$$\mathrm{Soc}\, M = 0 :_M \mathfrak{m} = \{u \in M \mid u\mathfrak{m} = 0\}.$$

Equivalently, the socle of M is the sum of all the simple submodules of M. Note that since the top of R is $R/\mathfrak{m}$, a simple module, hence the socle of $D(R)$ must be a simple module as well.

Example 57.1. Let $A = K[x, y]/\langle x^2, y^3\rangle$. Then $\mathrm{Soc}(A) = Kxy^2$ and $\mathrm{Top}(A) = K$. To calculate $D(A)$, we first write A as a K-vector space:

$$A = K + Kx + Ky + Kxy + Ky^2 + Kxy^2.$$

Then a dual basis for $D(A)$ is given by

$$D(A) = K\varphi_1 + K\varphi_x + K\varphi_y + K\varphi_{xy} + K\varphi_{y^2} + K\varphi_{xy^2}.$$

Then one can check that $\mathrm{Soc}(D(A)) = K\varphi_1$ and $\mathrm{Top}(D(A)) = K\varphi_{xy^2}$.

Remark 94. This remark is for those who are familiar with the Koszul Complex construction. Let $(A, \mathfrak{p})$ be a local ring and suppose $\mathfrak{p} = \langle x_1, \ldots, x_n \rangle$. Then

$$H_n(K(x_1, \ldots, x_n; M) \cong \mathrm{Soc}(M)$$
$$H_0(K(x_1, \ldots, x_n; M) \cong \mathrm{Top}(M)$$

Any dualizing functor preserves endomorphism rings; more generally, we have $\mathrm{Hom}_R(D(M), D(N)) \cong \mathrm{Hom}_R(N, M)$. In particular, $D(R)$ is a module with endomorphism ring A. To see this, consider the mappings given by applying D :

$$\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(D(N), D(M)) \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(D(N), D(M)).$$

Since $D^2 \cong 1$, the composite of two successive maps in this sequence is an isomorphism, so each of the maps is an isomorphism too. For instance, suppose $\varphi \in \mathrm{Hom}_A(M, N)$ was in the first map, that is, $D(\varphi) = 0$. Then $D^2(\varphi) = 0$ implies $\varphi = 0$ since D^2 is an isomorphism, which shows the map $D : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(D(N), D(M))$ is injective. Next, suppose $\varphi \in \mathrm{Hom}_A(D(N), D(M))$. Since D^2 is an isomorphism, there exists a $\psi \in \mathrm{Hom}_A(D(N), D(M)$ such that $D^2(\psi) = \varphi$. Then $D(\psi) \in \mathrm{Hom}_A(M, N)$ and $D(D(\psi)) = \varphi$, which shows the map $D : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(D(N), D(M))$ is surjective.

57.3 Canonical module of a local zero-dimensional ring

Proposition 57.2. *Let $(R, \mathfrak{m})$ be a local zero-dimensional ring. If E is any dualizing functor from the category of finitely generated R-modules to itself, then there is an isomorphism of functors $E(-) \cong \mathrm{Hom}_R(-, E(R))$. Further, $E(R)$ is isomorphic to the injective hull of $R/\mathfrak{m}$. Thus there is up to isomorphism at most one dualizing functor.*

Proof. Since $E^2 \cong 1$ as functors, the map $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(E(N), E(M))$ given by $\varphi \mapsto E(\varphi)$ is an isomorphism. Thus, there is an isomorphism, functorial in M,

$$\begin{aligned} E(M) &\cong \mathrm{Hom}_R(R, E(M)) \\ &\cong \mathrm{Hom}_R(E(E(M)), E(R)) \\ &\cong \mathrm{Hom}_R(M, E(R)) \end{aligned}$$

This proves the first statement.

Since R is projective, $E(R)$ is injective. As we observed above, R has a simple top, so $E(R)$ has a simple socle. Because R is zero-dimensional, every module contains simple submodules. The socle of a module M contains all the simple submodules of M, and thus meets every submodule of M; that is, it is an essential submodule of M. Since $R/\mathfrak{m}$ appears as an essential submodule of $E(R)$, we see that $E(R)$ is an injective hull of $R/\mathfrak{m}$. □

With Proposition (57.2) for justification, we define the **canonical module** ω_R of a local zero-dimensional ring R to be the injective hull of the residue class field of R. By Proposition (57.2), any dualizing functor on the category of finitely generated R-modules is naturally isomorphic to $\mathrm{Hom}_R(-, \omega_R)$, which is itself a dualizing functor.

Proposition 57.3. *Let $(R, \mathfrak{m}, \Bbbk)$ be a local zero-dimensional ring. The functor $D := \mathrm{Hom}_R(-, \omega_R)$ is a dualizing functor on the category of finitely generated R-modules.*

Proof. The functor D is contravariant. It is also exact since ω_R is an injective R-module. Thus it suffices to show that D^2 is naturally isomorphic to the identity. Let $\alpha : 1 \to D^2$ be the natural transformation given by maps

$$\alpha_M : M \to \mathrm{Hom}_R(\mathrm{Hom}_R(M, \omega_R), \omega_R)$$

given by mapping $u \in M$ to $\widehat{u}$, where $\widehat{u}$ is the R-linear map taking $\varphi \in \mathrm{Hom}_R(M, \omega_R)$ to $\varphi(u)$. We shall show that α is an isomorphism by showing that each α_M is an isomorphism.

We do induction on the length of M. First suppose that the length is 1, so that $M \cong \Bbbk$, thus it suffices to show that $\alpha_{\Bbbk}$ is an isomorphism. Since ω_R is the injective hull of $\Bbbk$, the socle of ω_R is isomorphic to $\Bbbk$, and we have $\mathrm{Hom}_R(\Bbbk, \omega_R) \cong \Bbbk$, generated by any nonzero map $\Bbbk \to \omega_R$. Thus

$$\mathrm{Hom}_R(\mathrm{Hom}_R(\Bbbk, \omega_R), \omega_R) \cong \mathrm{Hom}_R(\Bbbk, \omega_R) \cong \Bbbk,$$

generated by any nonzero map. But if $1 \in \Bbbk$ is the identity, then the map induced by 1 takes the inclusion $\Bbbk \hookrightarrow \omega_R$ to the image of 1 under that inclusion, and is thus nonzero, so $\alpha_{\Bbbk}$ is an isomorphism.

If the length of M is greater than 1, let M' be any proper submodule and let $M'' = M/M'$. By the naturality of α and the exactness of D^2 it follows that there is a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha'_M} & & \downarrow{\scriptstyle \alpha_M} & & \downarrow{\scriptstyle \alpha'_M} & & \\
0 & \longrightarrow & D^2(M') & \longrightarrow & D^2(M) & \longrightarrow & D^2(M'') & \longrightarrow & 0
\end{array}$$

Both M' and M'' have lengths stricly less than the length of M, so the left-hand and right-hand vertical maps are isomorphisms by induction. It follows by the five lemma that the middle map α_M is an isomorphism too. □

Corollary 59. *Let R be a local Artinian ring. Then the annihilator of ω_R is 0; the length of ω_R is the same as the length of R; and the endomorphism ring of ω_R is R.*

Proof. The dualizing functor preserves annihilators, lengths, and endomorphism rings, and takes R to ω_R. □

Proposition 57.4. *Let $(R, \mathfrak{m})$ be a local ring, let $(S, \mathfrak{n})$ be a zero-dimensional local ring, and let $f\colon R \to S$ be a local ring homomorphism. Suppose that S is finitely generated as an R-module. If E is the injective hull of the residue class field of R, then $\omega_S \cong \operatorname{Hom}_R(S, E)$. In particular, if R is also zero-dimensional, then*

$$\omega_S \cong \operatorname{Hom}_R(S, \omega_R).$$

Proof. Note that Lemma (51.4) implies $\operatorname{Hom}_R(S, E)$ is an injective S-module. To show that it is the injective hull of the residue class field of S, it suffices to show that it is an essential extension of the residue class field of S. The preimage of $\mathfrak{n}$ under f is a prime ideal of R which contains $\mathfrak{m}$, so it must in fact be $\mathfrak{m}$ itself. Therefore f induces a homomorphism of the residue class fields $\overline{f}\colon R/\mathfrak{m} \to S/\mathfrak{n}$. As $S/\mathfrak{n}$ is a finite-dimensional vector space over $R/\mathfrak{m}$, we have

$$S/\mathfrak{n} = \omega_{S/\mathfrak{n}} \cong \operatorname{Hom}_{R/\mathfrak{m}}(S/\mathfrak{n}, R/\mathfrak{m})$$

as $S/\mathfrak{n}$-vector spaces.

Let $\mathcal{K} \subseteq \operatorname{Hom}_R(S, E)$ be the S-submodule of homomorphisms whose kernel contains $\mathfrak{n}$, or equivalently, $\mathcal{K} = \{\varphi \in \operatorname{Hom}_R(S, E) \mid \mathfrak{n}\varphi = 0\}$. In particular, the module $\mathcal{K}$ is the socle of $\operatorname{Hom}_R(S, E)$ as an S-module. If $\varphi \in \mathcal{K}$, then since $\mathfrak{m}S \subseteq \mathfrak{n}$, the image of φ is annihilated by $\mathfrak{m}$; that is, the image of φ is in the socle of E as an R-module, and since E is the injective hull of $R/\mathfrak{m}$, this means $\operatorname{im}\varphi \subseteq R/\mathfrak{m}$. Since the homomorphisms in $\mathcal{K}$ all factor through the projection $S \to S/\mathfrak{n}$, we have

$$\begin{aligned}
\mathcal{K} &\cong \operatorname{Hom}_R(S/\mathfrak{n}, R/\mathfrak{m}) \\
&= \operatorname{Hom}_{R/\mathfrak{m}}(S/\mathfrak{n}, R/\mathfrak{m}) \\
&\cong S/\mathfrak{n}.
\end{aligned}$$

If $\psi\colon S \to E$ is any R-module homomorphism, then since $\mathfrak{n}$ is nilpotent, ψ is annihilated by a power of $\mathfrak{n}$, and thus there is a multiple $b\psi \neq 0$ where $b \in S$ that is annihilated by $\mathfrak{n}$. Thus $\mathcal{K}$ is an essential S-submodule of $\operatorname{Hom}_R(S, E)$, as required. □

57.4 Zero Dimensional Local Gorenstein Rings

Definition 57.2. A zero-dimensional local ring R is **Gorenstein** if $R \cong \omega_R$.

Proposition 57.5. *Let $(R, \mathfrak{m})$ be a zero-dimensional local ring. The following are equivalent.*

1. *R is Gorenstein.*
2. *R is injective as an R-module.*
3. *The socle of R is simple.*
4. *ω_R can be generated by one element.*

Proof.

That 1 implies 2 follows by definition. Let us show 2 implies 3. As R is a local ring, it is indecomposable as an R-module. Indeed, if $R \cong I \oplus J$ for two proper submodules $I, J \subseteq R$ (that is, ideals of R), then there exists $x \in I$ and $y \in J$ such that $x + y = 1$. But since $\mathfrak{m}$ is the unique maximal ideal of R, we have $I, J \subseteq \mathfrak{m}$, and so $1 = x + y \in \mathfrak{m}$ leads to a contradiction. Since

$$\operatorname{Soc} R \subseteq \bigcup_{n=1}^{\infty} 0 :_R \mathfrak{m}^n = R$$

is an essential extension, if R is injective as an R-module, then it must be the injective hull of its socle. The injective hull of a direct sum is the direct sum of the injective hulls of the summands, so the socle must be simple.

Now we show 3 implies 4. Suppose the socle of R is simple. This implies $\omega_R/\mathfrak{m}\omega_R$ is simple. By Nakayama's lemma, ω_R can be generated by one element. Finally, let's show 4 implies 1. Suppose ω_R can be generated by one element. Then it is a homomorphic image of R. But R and ω_R have the same length by Proposition (57.3), so $R \cong \omega_R$. □

Example 57.2. Let $A = K[x, y, z]/\langle x^2, y^2, xz, yz, z^2 - xy\rangle$. Then A is a 0-dimensional Gorenstein ring that is not a complete intersection ring. In more detail: a basis for A as a K-vector space is

$$A = K + Kx + Ky + Kz + Kz^2$$

The ring A is Gorenstein because the socle has dimension 1 as K-vector space, namely $\mathrm{Soc}(A) = Kz^2$. Finally, A is not a complete intersection because it has 3 generators and a minimal set of 5 relations.

Most of the common methods of constructing Gorenstein rings work just as well in the case where A is not zero-dimensional, and we shall postpone them for a moment. However, one technique, Macaulay's method of **inverse systems**, is principally of interest in the zero-dimensional case.

Let $S = K[x_1, \ldots, x_r]$. For each $d \geq 0$, let S_d be the vector space of forms of degree d in the x_i. Let $T = K[x_1^{-1}, \ldots, x_r^{-1}] \subset K(A) = K(x_1, \ldots, x_r)$ be the polynomial ring on the inverses of the x_i. We make T into an S-module as follows: Let x^α be a monomial in A and x^β be a monomial in T, where $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{Z}^r_{\geq 0}$ and $\beta = (\beta_1, \ldots, \beta_r) \in \mathbb{Z}^r_{\leq 0}$. Then

$$x^\alpha \cdot x^\beta = \begin{cases} 0 & \text{if } \alpha_i > \beta_i \text{ for some } i \\ x^{\alpha+\beta} & \text{else.} \end{cases}$$

Theorem 57.2. *With the notation above, there is a one-to-one inclusion reversing correspondence between finitely generated S-modules $M \subset T$ and ideal $I \subset S$ such that $I \subset \langle x_1, \ldots, x_r\rangle$ and A/I is a local zero-dimensional ring, given by*

$$M \mapsto (0 :_S M), \text{ the annihilator of } M \text{ in } S.$$
$$I \mapsto (0 :_T I), \text{ the submodule of } T \text{ annihilated by } I.$$

Proof. The S-module T may be identified with the graded dual $\bigoplus_d \mathrm{Hom}_K(S_d, K)$ of S; indeed the dual basis vector to $x^\alpha \in S_d$ is $x^{-\alpha} \in T$. Moreover, the graded dual is the injective hull of $K = S/\langle x_1, \ldots, x_r\rangle$ as an S-module. □

57.5 Canonical Modules and Gorenstein Rings in Higher Dimension

Definition 57.3. Let A be a local Cohen-Macaulay ring. A finitely generated A-module ω_A is a **canonical module for** A if there is a nonzerodivisor $x \in A$ such that $\omega_A/x\omega_A$ is a canonical module for $A/\langle x\rangle$. The ring A is **Gorenstein** if A is itself a canonical module; that is, A is Gorenstein if there is a nonzerodivisor $x \in A$ such that $A/\langle x\rangle$ is Gorenstein.

The induction in this definition terminates because $\dim(A/\langle x\rangle) = \dim(A) - 1$. We may easily unwind the induction, and say that ω_A is a canonical module if some maximal regular sequence $x_1, \ldots, x_d$ on A is also an ω_A-sequence, and $\omega_A/\langle x_1, \ldots, x_d\rangle\omega_A$ is the injective hull of the residue class field of $A/\langle x_1, \ldots, x_d\rangle$. Similarly, A is Gorenstein if and only if $A/\langle x_1, \ldots, x_d\rangle$ is a zero-dimensional Gorenstein ring for some maximal regular sequence $x_1, \ldots, x_d$. By Nakayama's lemma and Proposition (57.5), this is the case if and only if A has a canonical module generated by one element.

For a simple example, consider the case when A is a regular local ring. We claim that A has a canonical module, and in fact $\omega_A = A$. When $\dim(A) = 0$ the result is obvious, since A is a field. For the general case we do inductino on the dimension. If we choose x in the maximal ideal of A, but not its square, then x is a nonzerodivisor and A/x is again a regular local ring, so A/x is a canonical module for A/x . Therefore A is a canonical module for A, by defintion.

There are three problems with these notions. First, it is not at all obvious from the definitions that they are independent of the nonzero divisor x that was chosen. Second, something called a canonical module should at least be unique, and uniqueness is not clear either. Our first goal is to show that this independence and uniqueness do hold.

The third problem is that it is not obvious that a canonical module should even exist. Here we are not quite so lucky: There are local Cohen-Macaulay rings with no canonical module. However, our second goal will be to establish that canonical modules do exist for any Cohen-Macaulay rings that are homomorphic images of regular local rings (and a little more generally). This includes complete local rings and virtually all other rings of interest in algebraic geometry and number theory.

Example 57.3. Let $A = K[x,y,z]_{\langle x,y,z\rangle}/\langle xy, xz, yz\rangle$. Then $x+y+z$ is a nonzerodivisor in A, and

$$A/\langle x+y+z\rangle = K[x,y,z]_{\langle x,y,z\rangle}/\langle x+y+z, xy, xz, yz\rangle \cong K[y,z]_{\langle y,z\rangle}/\langle y^2, yz, z^2\rangle = K + Ky + Kz,$$

which does not have a simple socle, so this is not Gorenstein.

Example 57.4. Let $A = K[x,y,z]_{\langle x,y,z\rangle}/\langle x+y+z, xz, yz\rangle$. Then $x+y+z$ is a nonzerodivisor in A, and

$$A/\langle x+y+z\rangle = K[x,y,z]_{\langle x,y,z\rangle}/\langle x+y+z, xy, xz, yz\rangle \cong K[y,z]_{\langle y,z\rangle}/\langle y^2, yz, z^2\rangle = K + Ky + Kz,$$

which does not have a simple socle, so this is not Gorenstein.

57.6 Maximal Cohen-Macaulay Modules

Proposition 57.6. *Let R be a local ring of dimension d, and let M be a finitely-generated R-module. The following conditions are equivalent:*

1. *Every system of parameters in R is an M-sequence.*
2. *Some system of parameters in R is an M-sequence.*
3. $\operatorname{depth} M = d$

*If these conditions are satisfied, we say that M is a **maximal Cohen-Maculay module over** R. Every element outside the minimal primes of R is a nonzerodivisor on M.*

Proof. The implications 1 implies 2 implies 3 are immediate from the definitions. Let us show 3 implies 1. Suppose $\operatorname{depth} M = d$. If $x_1, \dots, x_d$ is a system of parameters, then $Q = \langle x_1, \dots, x_d\rangle$ is $\mathfrak{m}$-primary. In particular, $\sqrt{Q} = \mathfrak{m}$. Therefore

$$\begin{aligned}\operatorname{depth}(Q, M) &= \operatorname{depth}(\sqrt{Q}, M)\\ &= \operatorname{depth}(\mathfrak{m}, M)\\ &= \operatorname{depth} M\\ &= d,\end{aligned}$$

which implies $x_1, \dots, x_d$ is an M-regular sequence.

To prove the last statement, note that if x_1 is not in any minimal prime of R, then $\dim(R/x_1) = \dim R - 1$, so a system of parameters mod x_1 may be lifted to a system of parameters for R beginning with x_1. Thus, x_1 is a nonzerodivisor on M. □

Corollary 60. *Let $(A, \mathfrak{m})$ be a local ring of dimension d, $Q = \langle x_1, \dots, x_d\rangle$ and $\mathfrak{m}$-primary ideal, and M a maximal Cohen-Macaulay module over A. Then*

$$Gr_{\mathfrak{q}}(M) \cong Gr_{\mathfrak{q}}(A) \otimes_A M.$$

In case A is zero-dimensional, all finitely generated modules are maximal Cohen-Macaulay modules. On the other hand, if A is a regular local ring, then by the Auslander-Buchsbaum formula, the maximal Cohen-Macaulay A-modules are exactly the free A-modules.

More generally, if A is a finitely generated module over some regular local ring S of dimension d, then by the Auslander-Buchsbaum theorem, the maximal Cohen-Macaulay modules over A are those A-modules that are free as S-modules. Thus maximal Cohen-Macaulay modules may be thought of as representations of A as a ring of matrices over a regular local ring–as such they generalize the objects studied in integral representation theory of finite groups under the name **lattices**. We shall exploit the following example. If $B = A/J$ is a homomorphic image of A such that B is again Cohen-Macaulay of dimension d as a ring, then B is a Cohen-Macaulay A-module.

57.7 Modules of Finite Injective Dimension

Proposition 57.7. *Let N be an R-module, let $x \in R$ be an R-regular and an N-regular element, and let (E, d) be a minimal injective resolution of N over R. Set $(\widetilde{E}, \widetilde{\mathrm{d}})$ to be the R-complex give by $\widetilde{E} = \bigoplus_i 0 :_{E^i} x$ and $\widetilde{\mathrm{d}} = \mathrm{d}|_{\widetilde{E}}$. In particular, $\widetilde{E} \cong \operatorname{Hom}^\star_R(R/x, E)$ as R-complexes. Then $\Sigma\widetilde{E}$ is a minimal injective resolution of N/xN over R/x. Thus*

$$\operatorname{id}_{R/x}(N/xN) \leq \operatorname{id}_R R - 1.$$

Furthermore, let M be an R-module which is annihilated by x, then

$$\operatorname{Ext}^{i+1}_R(M, N) \cong \operatorname{Ext}^i_{R/x}(M, N/xN)$$

for all $i \geq 0$.

Proof. By Lemma (51.4), we see that each $\widetilde{E}^i$ is an injective (R/x)-module. Furthermore, note that E^0 is an essential extension of N since E is a *minimal* injective resolution of N over R. In particular, since

$$\widetilde{E}^0 \cap N = 0 :_N x = 0,$$

we see that $\widetilde{E}^0 = 0$. It remains to show that $\mathrm{H}^0(\Sigma\widetilde{E}) \cong N/xN$ and $\mathrm{H}^i(\Sigma\widetilde{E}) \cong 0$ for all $i \geq 1$, or equivalently, that $\mathrm{H}^1(\widetilde{E}) \cong N/xN$ and $\mathrm{H}^i(\widetilde{E}) \cong 0$ for all $i \geq 2$. Note that $\mathrm{H}(\widetilde{E}) = \mathrm{Ext}_R(R/x, N)$ by definition. Computing this homology using the short exact sequence

$$0 \to R \xrightarrow{x} R \to R/x \to 0$$

gives us $\mathrm{Ext}^1_R(R/x, N) \cong N/xN$ and $\mathrm{Ext}^i_R(R/x, N) \cong 0$ for all $i \geq 2$. It follows that $\Sigma\widetilde{E}$ is an injective resolution of N/xN over R/x. To see that $\Sigma\widetilde{E}$ is minimal, note that $\ker \widetilde{\mathrm{d}}^n$ is the intersection of the essential submodule $\ker \mathrm{d}^n$ with $\widetilde{E}^n$, and is thus essential in $\widetilde{E}^n$. It follows at once that

$$\mathrm{id}_{R/x}(N/xN) \leq \mathrm{id}_R(N) - 1.$$

For the latter part of the proposition, note that every map from M to an E^i has image killed by x, so

$$\begin{aligned}
\mathrm{Hom}^\star_R(M, E) &= \mathrm{Hom}^\star_R(M, \widetilde{E}) \\
&= \mathrm{Hom}^\star_{R/x}(M, \widetilde{E}) \\
&= \Sigma^{-1}\mathrm{Hom}^\star_{R/x}(M, \Sigma\widetilde{E})
\end{aligned}$$

Taking homology gives us the last statement of the proposition. □

Remark 95. Recall that if $(R, \mathfrak{m})$ is a local ring, M is a finitely-generated R-module, and $x \in \mathfrak{m}$ is an R-regular and M-regular element, then $\mathrm{pd}_{R/x}(M/xM) = \mathrm{pd}_R(M)$. The idea behind that proof is as follows: we start with a minimal projective resolution P of M over R and denote $p = \mathrm{pd}\, M$. Then one shows that P/xP is a minimal projective resolution of M/xM over R/xR. They key here however is that $(P/xP)_p = P_p/xP_p \neq 0$ by Nakayama's lemma.

To exploit this result, we need to know the modules of finite injective dimension over a zero-dimensional ring.

Proposition 57.8. *Let R be a local Cohen-Macaulay ring of dimension d and let M be a maximal Cohen-Macaulay module of finite injective dimension. Then $\mathrm{id}_R\, M = d$. Moreover, if $d = 0$, then M is a direct sum of copies of ω_R, and $M \cong \omega_R$ if and only if $\mathrm{End}_R(M) = R$.*

Proof. Let (E, d) be a finite injective resolution of M of length k, let $\mathrm{D}^\star = \mathrm{Hom}^\star_R(-, \omega_R)$, and let $\mathrm{D} = \mathrm{Hom}_R(-, \omega_R)$. Then $\mathrm{D}^\star(E)$ is a finite projective resolution of $\mathrm{D}(M)$ of length k. By the Auslander-Buchsbaum formula, we must have $k \leq d$. In particular, if $d = 0$, then $k = 0$ which implies $\mathrm{D}(M)$ is free. Applying D again we see that $M \cong \mathrm{D}^2(M)$ is a direct sum of copies of $\mathrm{D}(R) = \omega_R$. Using D, we see that the endomorphism ring of ω_R^n is the same as the endomorphism ring of R^n. Thus it is equal to R if and only if $n = 1$.

Since $k \leq d$, we certainly have $\mathrm{id}_R\, M \leq d$. Conversely, choose an R-regular sequence $x_1, \dots, x_d$ that is also an M-regular sequence. Then by Proposition (57.7), together with an induction argument, we conclude that

$$\begin{aligned}
\mathrm{id}_R(M) &\geq d + \mathrm{id}_{R/\langle x_1,\dots,x_d\rangle}(M/\langle x_1, \dots, x_d\rangle M) \\
&= d + 0 \\
&= d.
\end{aligned}$$

□

Proposition 57.9. *Let $(R, \mathfrak{m})$ be a local Cohen-Macaulay ring of dimension d and let N be a maximal Cohen-Macaulay module of finite injective dimension.*

1. *Let M be a finitely-generated R-module of depth q, then $\mathrm{Ext}^i_R(M, N) = 0$ for $i > d - q$.*
2. *Let x be an N-regular element. Then x is a $\mathrm{Hom}_R(M, N)$-regular element. Furthermore, if M is also a maximal Cohen-Macaulay module, then*

$$\mathrm{Hom}_R(M, N)/x\mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_{R/x}(M/xM, N/xN)$$

by the homomorphism taking the class of a map $\varphi : N \to M$ to the map $N/xN \to M/xM$ induced by φ.

Proof. 1. We do induction on q. By Proposition (57.8), the injective dimension of N is d, so that $\mathrm{Ext}^i_R(M, N) = 0$ for any N if $i > d$. This gives the case where $q = 0$. Now suppose $q > 0$ and let $x \in \mathfrak{m}$ be an M-regular element. From the short exact sequence

$$0 \longrightarrow M \xrightarrow{x} M \longrightarrow M/xM \longrightarrow 0 \tag{207}$$

we get a long exact sequence in Ext

$$\begin{tikzcd}
 & \mathrm{Ext}^{i+1}_R(M/xM, N) \arrow[r] & \cdots \\
\mathrm{Ext}^{i}_R(M/xM, N) \arrow[r] & \mathrm{Ext}^{i}_R(M, N) \arrow[r, "x"] & \mathrm{Ext}^{i}_R(M, N) \arrow[ul, rounded corners] \\
\cdots \arrow[r] & \mathrm{Ext}^{i-1}_R(M, N) \arrow[ul, rounded corners] &
\end{tikzcd}$$

The module M/xM has depth $q - 1$, so by induction $\mathrm{Ext}^{i+1}_R(M/xM, N)$ vanishes if $i + 1 > d - (q - 1)$, that is, if $i > d - q$. By Nakayama's lemma, we conclude that $\mathrm{Ext}^i_R(M, N)$ vanishes if $i > d - q$.

2. From the short exact sequence

$$0 \to N \xrightarrow{x} N \to N/xN \to 0,$$

we derive a long exact sequence in Ext beginning

$$0 \to \mathrm{Hom}_R(M, N) \xrightarrow{x} \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N/xN) \to \mathrm{Ext}^1_R(M, N) \to \cdots$$

Thus x is $\mathrm{Hom}_R(M, N)$-regular. Now assume that M is maximal Cohen-Macaulay, so $q = d$. Then $\mathrm{Ext}^1_R(M, N) \cong 0$ by part 1. Every R-linear map $M \to N/xN$ factors uniquely through M/xM, so $\mathrm{Hom}_R(M, N/xN) = \mathrm{Hom}_R(M/xM, N/xN)$. The short exact sequence above thus becomes

$$0 \to \mathrm{Hom}_R(M, N) \xrightarrow{x} \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M/xM, N/xN) \to 0$$

Finally since $\mathrm{Hom}_R(M/xM, N/xN) = \mathrm{Hom}_{R/x}(M/xM, N/xN)$, we obtain part 2. $\square$

Proposition 57.10. *Let $(R, \mathfrak{m})$ be a local ring, and let M and N be finitely generated R-modules, and let $x \in \mathfrak{m}$ be an N-regular element. If $\varphi\colon M \to N$ is an R-linear map and $\overline{\varphi}\colon M/xM \to N/xN$ is the map induced by φ, then*

1. *If $\overline{\varphi}$ is surjective, then φ is surjective.*

2. *If $\overline{\varphi}$ is injective, then φ is injective.*

In particular, if $\overline{\varphi}$ is an isomorphism, then φ is an isomorphism.

Proof. 1. Suppose $\overline{\varphi}$ is surjective. Then $N = \varphi(M) + xN$. By Nakayama's lemma, this implies $N = \varphi(M)$. Thus φ is surjective.

2. Suppose $\overline{\varphi}$ is injective. Let $L = \ker \varphi$. Since L goes to zero in N/xN, we must have $L \subseteq xM$. On the other hand, since x is a nonzerodivisor on the image of φ, we must have $L :_M x = L$. To see this, note that $v \in L :_M x$ implies $xv \in L$, thus

$$0 = \varphi(xv) = x\varphi(v),$$

then x being a nonzerodivisor on the image of φ implies $\varphi(v) = 0$, or $v \in L$. So $L :_M x = L$ and $L \subseteq xM$ implies $xL = L$, and hence $L = 0$ by Nakayama's lemma. $\square$

Theorem 57.3. *Let R be a local Cohen-Macaulay ring of dimension d, and let W be a finitely generated R-module of depth q. Then W is a canonical module for R if and only if*

1. $\operatorname{depth} W = \dim R$.

2. *W is a module of finite injective dimension (necessarily equal to d).*

3. $\mathrm{End}_R\, W = R$

Proof. First suppose that W is a canonical module. We do induction on the dimension of R. Suppose $d = 0$. Then condition 1 is vacuous, since $q \leq d$. Also, condition 2 is satisfied because $W = \omega_R$ is injective. Lastly, condition 3 follows because, by duality

$$\begin{aligned}\operatorname{End}_R(\omega_R) &\cong \operatorname{End}_R(D(\omega_R)) \\ &\cong \operatorname{End}_R R \\ &\cong R.\end{aligned}$$

Now suppose $d > 0$, and let x be a nonzerodivisor. By hypothesis, W/xW is a canonical module over R/x, and by induction it satisfies conditions 1,2, and 3 as an (R/x)-module. Since x is a nonzerodivisor on W and W/xW has depth $d-1$, condition 1 is satisfied. By Proposition (57.7), W has finite injective dimension, in particular

$$d - 1 = \operatorname{id}_{R/x}(W/xW) = \operatorname{id}_R W - 1.$$

Let $S = \operatorname{End}_R W$, and consider the homothety map $\varphi\colon R \to S$ sending each element $a \in R$ to the map $\mathrm{m}_a \in \operatorname{End}_R W$, where $\mathrm{m}_a(w) = aw$ for all $w \in W$. We must show that φ is an isomorphism. By Proposition (57.9), x is a nonzerodivisor on S, and $S/xS = \operatorname{End}_{R/x}(W/xW) = R/x$. Thus by induction the map φ induces an isomorhpism $R/x \to S/xS$. It follows from Proposition (57.7) that φ is an isomorphism.

Next suppose that W is an R-module satisfying conditions 1,2, and 3. Again, we do induction on d. In case $d = 0$ we must show that $W = \omega_R$. By Proposition (57.8), this follows from conditions 2 and 3. Now suppose that $d > 0$, and let x be a nonzerodivisor in R. The element x is also a nonzerodivisor on W by Proposition (57.6), so W/xW has depth $d-1$ over R/x. By Proposition (57.7), $\operatorname{id}_{R/x}(W/xW) < \infty$, and by Proposition (57.9),

$$\operatorname{End}_{R/x}(W/xW) = \operatorname{End}_R(W)/x\operatorname{End}_R(W) = R/x.$$

Thus, W/xW is a canonical module for R/x by induction, and W is a canonical module for R. □

57.8 Uniqueness and (Often) Existence

These results imply a strong uniqueness result.

Corollary 61. *(Uniqueness of canonical modules). Let R be a local Cohen-Macualay ring of dimension d with a canonical module W, and let M be a finitely-generated maximal Cohen-Macaulay R-module of finite injective dimension. Then M is a direct sum of copies of W. In particular, any two canonical module of R are isomorphic.*

Proof. We do induction on d, the case $d = 0$ being Proposition (57.8). If $x \in R$ is a nonzerodivisor, then x is a nonzerodivisor on W and on M, and $M/xM \cong (W/xW)^n$ for some n by induction. By Proposition (57.10), there is an isomorphism $M \cong W^n$. □

Corollary 62. *(Uniqueness of canonical modules). Let A be a local Cohen-Macualay ring with a canonical module W. If M is any finitely generated maximal Cohen-Macaulay A-module of finite injective dimension, then M is a direct sum of copies of W. In particular, any two canonical module of A are isomorphic.*

Proof. We do induction on $\dim(A)$, the case $\dim(A) = 0$ being Proposition (57.8). If $x \in A$ is a nonzerodivisor, then x is a nonzerodivisor on W and on M, and $M/xM \cong (W/xW)^n$ for some n by induction. By Proposition (57.10), there is an isomorphism $M \cong W^n$. □

Henceforth, we shall write ω_A for a canonical module of A (if one exists). We now come to the question of existence. We have already seen that if R is a regular local ring, then R has canonical module $\omega_R = R$. We shall now show that if A is a homomorhpic image of a local ring with a canonical module, then A has a canonical module too.

Theorem 57.4. *(Construction of canonical modules). Let $(R, \mathfrak{m})$ be a local Cohen-Macaulay ring with canonical module ω_R. If A is a local R-algebra that is finitely generated as an R-module, and A is Cohen-Macaulay, then A has a canonical module. In fact, if $c = \dim(R) - \dim(A)$, then*

$$\omega_A \cong \mathit{Ext}^c_R(A, \omega_R)$$

Proof. We shall do induction on $\dim(A)$. First suppose that $\dim(A) = 0$. In this case, c is the dimension of R. The annihilator of A contains a power of the maximal ideal of R, say $\mathfrak{m}^n$. Since $\operatorname{depth}(\mathfrak{m}^n, R) = \operatorname{depth}(\mathfrak{m})$, we may choose a regular sequence $x_1, \ldots, x_c$ of length c in the annihilator of A. Let $R' = R/\langle x_1, \ldots, x_c\rangle$. Then R' is a local Cohen-Macaulay ring of dimension 0, and A is a finitely generated R'-module.

By definition, $\omega_R/\langle x_1, \ldots, x_c\rangle\omega_R$ is a canonical module for R', for which we shall write $\omega_{R'}$. By Proposition (57.7), applied c times,

$$\operatorname{Ext}^c_R(A, \omega_R) \cong \operatorname{Ext}^0_{R'}(A, \omega_{R'}) = \operatorname{Hom}_{R'}(A, \omega_{R'}).$$

By Proposition (57.4), this is a canonical module for A, as required.

Now suppose $\dim(A) > 0$. It suffices to show that if x is a nonzerodivisor on A, then x is a nonzerodivisor on $\mathrm{Ext}^c_R(A, \omega_R)$ and $\mathrm{Ext}^c_R(A, \omega_R)/x\mathrm{Ext}^c_R(A, \omega_R)$ is a canonical module for A/x. The short exact sequence

$$0 \longrightarrow A \xrightarrow{\cdot x} A \longrightarrow A/x \longrightarrow 0$$

gives rise to a long exact sequence in Ext of which a part is

$$\cdots \longrightarrow \mathrm{Ext}^c_R(A/x, \omega_R) \longrightarrow \mathrm{Ext}^c_R(A, \omega_R) \xrightarrow{\cdot x} \mathrm{Ext}^c_R(A, \omega_R) \longrightarrow \mathrm{Ext}^{c+1}_R(A/x, \omega_R) \longrightarrow \mathrm{Ext}^{c+1}_R(A, \omega_R) \longrightarrow \cdots$$

By induction, $\mathrm{Ext}^{c+1}_R(A/x, \omega_R)$ is a canonical module for A/x, so it suffices to show that the outer terms are 0, which we may do as follows:

Set $I = \mathrm{Ann}_R(A)$. The ring A/x is annihilated by $\langle I, x\rangle$, which has depth $c+1$ in R. Thus, $\mathrm{Ext}^c_R(A/x, \omega_R) = 0$. The ring A, being Cohen-Macaulay, has depth equal to $\dim(R) - c$, so $\mathrm{Ext}^{c+1}_R(A, \omega_R) = 0$ by Proposition (57.9). □

58 Module of Differentials

Definition 58.1. Let R be a ring, let A be an R-algebra, and let M be an A-module. An **R-derivation of A with values in M** is an R-linear map $\partial\colon A \to M$ which satisfies Leibniz rule: for all $a_1, a_2 \in A$, we have

$$\partial(a_1 a_2) = a_1 \partial a_2 + a_1 \partial a_2.$$

Note that R-linearity and the Leibniz rule implies $\partial r = 0$ for all $r \in R$. We denote by $\mathrm{Der}_R(A, M)$ to be the set of all R-derivations of A with values in M. This set is naturally an A-module with multiplication defined by

$$(a\partial)(a') := a\partial a'$$

for all $a, a' \in A$ and $\partial \in \mathrm{Der}_R(A, M)$.

Example 58.1. Consider $R = \mathbb{k}$ and $A = \mathbb{k}[x, y] = M$. Then $\partial_x\colon A \to A$ is a $\mathbb{k}$-derivation of A to itself. In fact, this derivation is $\mathbb{k}[y]$-linear, so we could also consider it to be a $\mathbb{k}[y]$-derivation of A to itself. We will later be able to show that $\mathrm{Der}_{\mathbb{k}[y]}(A, A)$ is a free A-module of rank 1, generated by ∂_x.

Example 58.2. Let $A = \mathbb{k}[x_1, \dots, x_n]$ and let $\boldsymbol{p} = (p_1, \dots, p_n)$ be a point in $\mathbb{k}^n$. We can consider $\mathbb{k}$ as an A-module via the evaluation at $\boldsymbol{p}$ map, given by $f \cdot c \mapsto f(\boldsymbol{p})c$ for all $f \in A$ and $c \in \mathbb{k}$. Then a $\mathbb{k}$-derivation $\partial\colon A \to \mathbb{k}$ is the same thing as a point derivation at $\boldsymbol{p}$:

$$\partial(f_1 f_2) = f_1 \cdot \partial f_2 + f_2 \cdot \partial f_1 = f_1(\boldsymbol{p})\partial f_1 + f_2(\boldsymbol{p})\partial f_2.$$

For instance, $\partial_{x_1}|_{\boldsymbol{p}}$ is an example of such a $\mathbb{k}$-derivation.

In practice, it is most interesting to consider to take $M = A$ and consider $\mathrm{Der}_R(A, A)$, the collection of all R-derivations of A to itself. One source of interest is the case where $R = \mathbb{k}$ is a field and A is the coordinate ring of an affine variety X defined over $\mathbb{k}$. As we will see later on, $\mathrm{Der}_{\mathbb{k}}(A, A)$ is then the set of algebraic tangent vector fields on X. A dual view of derivations may be had by means of the following extremely important device:

Definition 58.2. Let A be an R-algebra. The **module of Kähler differentials** of A over R, denoted $\Omega^1_{A/R}$, is the A-module generated by the set $\{\mathrm{d}a \mid a \in A\}$ subject to the relations

$$\mathrm{d}(a_1 a_2) = a_2 \mathrm{d}a_1 + a_1 \mathrm{d}a_2 \quad \text{and} \quad \mathrm{d}(r_1 a_1 + r_2 a_2) = r_1 \mathrm{d}a_1 + r_2 \mathrm{d}a_2$$

for all $r_1, r_2 \in R$ and $a_1, a_2 \in A$. The map $\mathrm{d}\colon A \to \Omega^1_{A/R}$ defined by $a \mapsto \mathrm{d}a$ is an R-derivation, called the **universal R-derivation**.

The map d satisfies the following universal mapping property: given any A-module M and an R-derivation $\partial\colon A \to M$, there is a unique A-linear homomorphism $\widetilde{\partial}\colon \Omega^1_{A/R} \to M$ such that $\partial = \widetilde{\partial} \circ \mathrm{d}$. Indeed, $\widetilde{\partial}$ is defined by $\widetilde{\partial}(\mathrm{d}a) = \partial a$ for all $a \in A$. Asserting the universal mapping property is the same as asserting that

$$\mathrm{Der}_R(A, M) \simeq \mathrm{Hom}_A(\Omega^1_{A/R}, M)$$

naturally, as functors of M. In this sense the construction of $\Omega^1_{A/R}$ "linearizes" the construction of derivations. Since the formula above allows us to compute $\mathrm{Der}_R(A, M)$ in terms of $\Omega^1_{A/R}$, we shall concentrate mostly on $\Omega^1_{A/R}$ in what follows.

Proposition 58.1. *Suppose $A = R[x_1, \dots, x_n]$. Then $\Omega^1_{A/R} = A\mathrm{d}x_1 \oplus \cdots \oplus A\mathrm{d}x_n$.*

Proof. Note that Leibniz law implies

$$\mathrm{d}(x_i^n) = nx_i^{n-1}\mathrm{d}x_i = \partial_{x_i}(x_i^n)\mathrm{d}x_i.$$

More generally, for any monomial $x^{\alpha} = x_1^{\alpha_1} \cdots x_i^{\alpha_i} \cdots x_n^{\alpha_n}$ in A, the Leibniz law implies

$$\begin{aligned}
\mathrm{d}(x^{\alpha}) &= \alpha_1 x_1^{\alpha_1 - 1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mathrm{d}x_1 + \sum_{i=2}^{n} \alpha_i x_1^{\alpha_1} \cdots x_{i-1}^{\alpha_{i-1}} x_i^{\alpha_i - 1} \cdots x_n^{\alpha_n} \mathrm{d}x_i \\
&= \partial_{x_1}(x^{\alpha})\mathrm{d}x_1 + \sum_{i=2}^{n} \partial_{x_i}(x^{\alpha})\mathrm{d}x_n \\
&= \sum_{i=1}^{n} \partial_{x_i}(x^{\alpha})\mathrm{d}x_i.
\end{aligned}$$

It follows by R-linearity that

$$\mathrm{d}f = \sum_{i=1}^{n} (\partial_{x_i} f)\mathrm{d}x_i = \mathrm{J}_f \mathrm{d}\boldsymbol{x}$$

for all $f \in A$, where we write $\mathrm{J}_f(\boldsymbol{x}) = (\partial_{x_1} f, \dots, \partial_{x_n} f)$ and $\mathrm{d}\boldsymbol{x} = (\mathrm{d}x_1, \dots, \mathrm{d}x_n)^{\top}$. This shows that every element in $\Omega^1_{A/R}$ can be expressed as an A-linear combination of the $\mathrm{d}x_i$'s. Moreover, suppose that $\sum_{i=1}^{n} f_i \mathrm{d}x_i = 0$. We claim that $f_i = 0$ for all i. Indeed, consider the $\Bbbk$-linear A-derivation $\partial_{x_i} \colon A \to A$ and let $\widetilde{\partial}_{x_i} \colon \Omega_{A/\Bbbk} \to A$ be the unique A-linear which corresponds to ∂_{x_i} via the universal mapping property. Then note that $\widetilde{\partial}_{x_i}(\mathrm{d}x_j) = 0$ whenever $i \neq j$ and $\widetilde{\partial}_{x_i}(\mathrm{d}x_i) = 1$ implies

$$0 = \widetilde{\partial}_{x_i}\left(\sum_{i=1}^{n} f_i \mathrm{d}x_n\right) = f_i.$$

It follows that $f_i = 0$ for all i as claimed. $\square$

We now discuss an alternative construction of the module of Kähler differentials.

Proposition 58.2. *Let $A \to B$ be a ring map, let $\mu \colon B \otimes_A B \to B$ be the multiplication ring map, and let $I = \ker \mu$. We view $B^{\otimes 2} = B \otimes_A B$ as a B-algebra via the ring map $B \to B^{\otimes 2}$ given by $b \mapsto b \otimes 1$. Let $\mathrm{d} \colon B \to I/I^2$ be the map induced by $b \mapsto b \otimes 1 - 1 \otimes b$. Then d is an A-linear derivation. Moreoever, I/I^2 (equipped with d) satisfies the universal mapping property of $\Omega^1_{B/A}$, so we may write $I/I^2 = \Omega^1_{B/A}$.*

Proof. First let us check that d is in fact an A-linear derivation. Clearly we have $\mathrm{d}a = 0$ for all $a \in A$ since we are tensoring over A. Also, if $b_1, b_2 \in B$, then we have

$$\begin{aligned}
\mathrm{d}(b_1)b_2 + b_1\mathrm{d}(b_2) &= (\overline{b_1 \otimes 1} - \overline{1 \otimes b_1})b_2 + b_1(\overline{b_2 \otimes 1} - \overline{1 \otimes b_2}) \\
&= \overline{b_1 \otimes b_2} - \overline{1 \otimes b_1 b_2} + \overline{b_2 \otimes b_1} - \overline{1 \otimes b_1 b_2} \\
&= \overline{b_1 \otimes b_2} - \overline{1 \otimes b_1 b_2} + \overline{b_2 \otimes b_1} + \overline{b_1 b_2 \otimes 1} - \overline{b_1 \otimes b_2} - \overline{b_2 \otimes b_1} \\
&= \overline{b_1 b_2 \otimes 1} - \overline{1 \otimes b_1 b_2} \\
&= \mathrm{d}(b_1 b_2),
\end{aligned}$$

where in the third line we used the fact that:

$$b_1 b_2 \otimes 1 - b_1 \otimes b_2 - b_2 \otimes b_1 + 1 \otimes b_1 b_2 = (b_1 \otimes 1 - 1 \otimes b_1)(b_2 \otimes 1 - 1 \otimes b_2) \in I^2.$$

Therefore we have shown that $\mathrm{d} \colon B \to I/I^2$ is in fact an A-linear derivation. We now want to show that I/I^2 satisfies the universal mapping property of $\Omega^1_{B/A}$. Suppose that $\partial \colon B \to M$ is an A-linear M-derivation. Note that $\{b \otimes 1 - 1 \otimes b \mid b \in B\}$ spans I as a $B^{\otimes 2}$ ideal. Since $B = B^{\otimes 2}/I$, it follows that $\{\overline{b \otimes 1} - \overline{1 \otimes b} \mid b \in B\}$ spans I/I^2 as a B-module. In particular, any B-linear map out of I/I^2 is completely determined by where it maps $\overline{b \otimes 1} - \overline{1 \otimes b}$. Thus we define $\widetilde{\partial} \colon I/I^2 \to M$ by

$$\widetilde{\partial}(\overline{b \otimes 1} - \overline{1 \otimes b}) = \partial b.$$

It is straightforward to check that this is well-defined and it is unique since every map out of I/I^2 is completely determined by where it sends $\overline{b \otimes 1} - \overline{1 \otimes b}$. $\square$

58.0.1 The Noether different

Definition 58.3. Let $A \to B$ be a ring map. Set $I = \ker \mu$ where $\mu\colon B \otimes_A B \to B$ is the multiplication map and set $J = \operatorname{Ann} I$. The **Noether different** of B over A is the ideal $\mu(J)$ of B.

Remark 96. Observe that if $\beta \in J$ and $b \in B$, then we have $(1 \otimes b)\beta = (b \otimes 1)\beta$. In particular, if $\beta = \sum_i b_{i1} \otimes b_{i2}$, then we have

$$\sum_i b_{i1} b \otimes b_{i2} = \sum_i b_{i1} \otimes b b_{i2}.$$

Thus J is a B-module in a canonical manner. Observe that in I/I^2 we have

$$\begin{aligned}(1 \otimes \mu(\beta))(b \otimes 1 - 1 \otimes b) &= b \otimes \mu(\beta) - 1 \otimes b\mu(\beta) \\ &= b \otimes \sum b_{i1}b_{i2} - 1 \otimes b \sum b_{i1}b_{i2} \\ &= b \otimes \sum b_{i1}b_{i2} + b\sum b_{i1}b_{i2} \otimes 1 - b \otimes \sum b_{i1}b_{i2} - \sum b_{i1}b_{i2} \otimes b \\ &= b\sum b_{i1}b_{i2} \otimes 1 - \sum b_{i1}b_{i2} \otimes b\end{aligned}$$

Lemma 58.1. *Let $A \to B$ be a finite type ring map, let $A \to A'$ be a flat ring map, set $B' = B \otimes_A A'$, and set $\mu\colon B \otimes_A B \to B$ and $\mu'\colon B' \otimes_{A'} B' \to B'$ to be the corresponding multiplication maps.*

1. *The annihilator J' of $\ker \mu'$ is $J \otimes_A A'$ where J is the annihilator of $\ker \mu$.*
2. *The Noether different $\mathfrak{d}' := \mu'(J')$ of B' over A' is $\mathfrak{d}B'$ where $\mathfrak{d} := \mu(J)$ is the Noether different of B over A.*

Proof. Choose generators $b_1, \dots, b_n$ of B as an A-algebra. Then $b_1', \dots, b_n'$ are generators of B' as an A'-algebra, where $b_i' := b_i \otimes 1$ for all $1 \le i \le n$. Note that

$$\begin{aligned}B' \otimes_{A'} B' &= (B \otimes_A A') \otimes_{A'} (B \otimes_A A') \\ &\simeq (B \otimes_A A') \otimes_{A'} (A' \otimes_A B) \\ &\simeq B \otimes_A A' \otimes_{A'} A' \otimes_A B \\ &\simeq B \otimes_A A' \otimes_A B \\ &\simeq (B \otimes_A B) \otimes_A A'.\end{aligned}$$

Therefore since

$$J = \ker(B \otimes_A B \xrightarrow{b_i \otimes 1 - 1 \otimes b_i} (B \otimes_A B)^{\oplus n}),$$

and since A' is flat over A, it follows that

$$\begin{aligned}J' &= \ker(B' \otimes_{A'} B' \xrightarrow{b_i' \otimes 1 - 1 \otimes b_i'} (B' \otimes_{A'} B')^{\oplus n}) \\ &\simeq \ker((B \otimes_A B) \otimes_A A' \xrightarrow{b_i' \otimes 1 - 1 \otimes b_i'} ((B \otimes_A B) \otimes_A A')^{\oplus n}) \\ &= J \otimes_A A'.\end{aligned}$$

Furthermore we have

$$\begin{aligned}\mathfrak{d}' &= \mu'(J') \\ &= \mu(J) \otimes_A A' \\ &= \mathfrak{d}(B \otimes_A A') \\ &= \mathfrak{d}B'.\end{aligned}$$

□

58.1 Some Useful Exact Sequences

We'd would now like to discuss some useful exact sequences involving Kähler differentials which arise from a sequence of ring maps. The first sequence we discuss is called the **cotangent sequence**:

Proposition 58.3. *Let $R \to A \to B$ be a map of rings. Then there is a canonical exact sequence of B-modules*

$$B \otimes_A \Omega^1_{A/R} \longrightarrow \Omega^1_{B/R} \longrightarrow \Omega^1_{B/A} \longrightarrow 0 \tag{208}$$

where the map $B \otimes_A \Omega^1_{A/R} \to \Omega^1_{B/R}$ is defined by $b \otimes \mathrm{d}a \mapsto b\mathrm{d}a$ and where the map $\Omega^1_{B/R} \to \Omega^1_{B/A}$ is defined by $\mathrm{d}b \mapsto \mathrm{d}b$.

Proof. The generators for $\Omega^1_{B/A}$ as a B-module are the same as the generators of $\Omega^1_{B/R}$, but there are extra relations of the form $\mathrm{d}a = 0$ where $a \in A$. These relations are precisely the images of the generators $1 \otimes \mathrm{d}a$ of $B \otimes_A \Omega^1_{A/R}$. $\square$

Assume that $A \to B$ is an epimorphism. In this case, one has $\Omega^1_{B/A} = 0$, and one can extend (208) to the left and yield another useful exact sequence, called the **conormal sequence**:

Proposition 58.4. *Let $R \to A \to B$ be a rings with $\pi\colon A \to B$ an epimorphism and set $I = \ker \pi$. Then there is a canonical exact sequences of B-modules*

$$I/I^2 \longrightarrow B \otimes_A \Omega^1_{A/R} \longrightarrow \Omega^1_{B/R} \longrightarrow 0 \tag{209}$$

where the map $I/I^2 \to B \otimes_A \Omega^1_{A/R}$ is defined by $\overline{x} \mapsto 1 \otimes \mathrm{d}x$ where $x \in I$ and where the map $B \otimes_A \Omega^1_{A/R} \to \Omega^1_{B/R}$ is defined by $b \otimes \mathrm{d}a \mapsto b\mathrm{d}a$.

Proof. Note that the map $I/I^2 \to B \otimes_A \Omega^1_{A/R}$ given by $\overline{x} \mapsto 1 \otimes \mathrm{d}x$ is well-defined since if $x_1, x_2 \in I$, then the Leibniz law implies

$$\begin{aligned} 1 \otimes \mathrm{d}(x_1x_2) &= 1 \otimes (\mathrm{d}(x_1)x_2 + x_1\mathrm{d}(x_2)) \\ &= \overline{x}_2 \otimes \mathrm{d}x_1 + \overline{x}_1 \otimes \mathrm{d}x_2 \\ &= 0 \otimes \mathrm{d}x_1 + 0 \otimes \mathrm{d}x_2 \\ &= 0. \end{aligned}$$

A similar computation shows that this is B-linear. Let's consider how to describe $B \otimes_A \Omega^1_{A/R}$ by generators and relations: from the definition of $\Omega^1_{A/R}$, and the right-exactness of tensor products, we see that $B \otimes_A \Omega^1_{A/R}$ is generated as a B-module by the elements $\mathrm{d}a$ for $a \in A$, subject to the relations of R-linearity and the Leibniz rule. This is the same as the description by generators and relations of $\Omega^1_{B/R}$, except that in $\Omega^1_{B/R}$ the elements $\mathrm{d}x$ for $x \in I$ are replaced by $\mathrm{d}0 = 0$. This implies exactness at $B \otimes_A \Omega^1_{A/R}$. $\square$

Example 58.3. Let $A \to B$ be a ring map and set $B^{\otimes 2} = B \otimes_A B$. Then we have a sequence of rings maps $B \rightarrowtail B^{\otimes 2} \twoheadrightarrow B$ where the first map $B \rightarrowtail B^{\otimes 2}$ is given by $b \mapsto b \otimes 1$ and where the second map $\mu\colon B^{\otimes 2} \twoheadrightarrow B$ is the multiplication map. Note Then since $\Omega^1_{B/B} = 0$, the conormal sequence gives us a surjection

$$\Omega^1_{B/A} = I/I^2 \twoheadrightarrow B \otimes_B \Omega^1_{B^{\otimes 2}/B} \simeq \Omega^1_{B^{\otimes 2}/B}$$

where $I = \ker \mu$.

Proposition 58.5. *Let $S = \Bbbk[x_1, \dots, x_n]/\langle f_1, \dots, f_m\rangle = \Bbbk[\boldsymbol{x}]/\langle \boldsymbol{f}\rangle$. We have*

$$\Omega^1_{S/\Bbbk} = \frac{S\mathrm{d}x_1 \oplus \cdots \oplus S\mathrm{d}x_n}{\mathrm{d}\boldsymbol{x} \cdot \mathrm{J}_{\boldsymbol{f}}^{\top}},$$

where $\mathrm{d}\boldsymbol{x} = (\mathrm{d}x_1, \dots, \mathrm{d}x_n)$ and where $\mathrm{J}_{\boldsymbol{f}} = (\partial_{x_j} f_i) \in \mathrm{M}_{m\times n}(S)$ is the Jacobian matrix:

$$\mathrm{J}_{\boldsymbol{f}} = \begin{pmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_n} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_m & \cdots & \partial_{x_n} f_m \end{pmatrix}.$$

Proof. Set $R = \Bbbk[\boldsymbol{x}]$ and $I = \langle \boldsymbol{f}\rangle$. Then Proposition (58.12) gives us the following presentation of $\Omega^1_{A/\Bbbk}$:

$$I/I^2 \xrightarrow{\mathrm{d}} \textstyle\bigoplus_{i=1}^n S\mathrm{d}x_i \longrightarrow \Omega^1_{A/\Bbbk} \longrightarrow 0 \tag{210}$$

where we used the fact that

$$S \otimes_R \Omega^1_{R/\Bbbk} \simeq \bigoplus_{i=1}^n S\mathrm{d}x_i.$$

Writing I/I^2 as a homomorphic image of a free S-module with generators e_i going to the classes of f_i , the composition

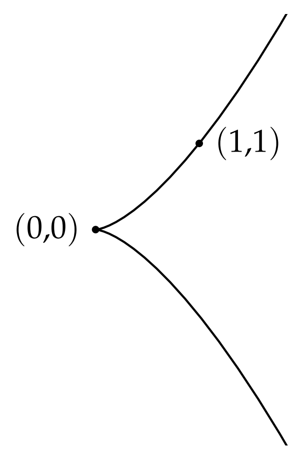
$$\textstyle\bigoplus_{i=1}^n Se_i \longrightarrow I/I^2 \xrightarrow{\mathrm{d}} \bigoplus_{i=1}^n S\mathrm{d}x_i \tag{211}$$

is represented by $\mathrm{J}_{\boldsymbol{f}}^{\top}$. $\square$

Example 58.4. Let $\mathbb{k}$ be a field and let $S = \mathbb{k}[x,y]/f$ where $f = y^2 - x^3$. Then we have

$$\Omega^1_{S/\mathbb{k}} = \frac{S\mathrm{d}x \oplus S\mathrm{d}y}{-3x^2\mathrm{d}x + 2y\mathrm{d}y}.$$

In order to better understand what kind of object $\Omega^1_{S/\mathbb{k}}$ is, we digress a bit and explain how one should think S in terms of geometry. Let $X = \operatorname{Spec} S$. For each $\boldsymbol{p} = (a,b)$ in $\mathbb{k}^2$ such that $b^2 = a^3$, we have a maximal ideal $\mathfrak{m}_{\boldsymbol{p}} = \langle x - a, y - b\rangle$ of S (or alternatively we can consider $\mathfrak{m}_{\boldsymbol{p}}$ as a closed point of X) and we set $\mathbb{k}_{\boldsymbol{p}} := S/\mathfrak{m}_{\boldsymbol{p}} \simeq \mathbb{k}$ to be the corresponding residue field (which is just $\mathbb{k}$ but equipped with an S-module action coming from $\boldsymbol{p}$). If $\mathbb{k}$ is algebraically closed, then these are all of the maximal ideals of S, however if $\mathbb{k}$ is not algebraically closed, then there will be more maximal ideals than just this. For instance, suppose $\mathbb{k} = \mathbb{R}$. Then the set of all such closed points forms the curve below:



However X contains more closed points than just this (alternatively S contains more maximal ideals than just this). Indeed, for each $\boldsymbol{p} = (a,b)$ in $\mathbb{C}^2$ such that $b^2 = a^3$, one gets an $\mathbb{R}$-algebra homomorphism $e_{\boldsymbol{p}} \colon S \to \mathbb{C}$ given by $x \mapsto a$ and $y \mapsto b$. We call $e_{\boldsymbol{p}}$ a **$\mathbb{C}$-valued point** of S (or a $\mathbb{C}$-valued point of X). For any such $\mathbb{C}$-valued point, we set $\mathfrak{m}_{\boldsymbol{p}} := \ker e_{\boldsymbol{p}}$ and $\mathbb{k}_{\boldsymbol{p}} = S/\mathfrak{m}_{\boldsymbol{p}}$ (if $\boldsymbol{p} \in \mathbb{R}^2$ then $\mathbb{k}_{\boldsymbol{p}} \simeq \mathbb{R}$ and if $\boldsymbol{p} \in \mathbb{C}^2 \backslash \mathbb{R}^2$, then $\mathbb{k}_{\boldsymbol{p}} \simeq \mathbb{C}$). Then all maximal ideals of S are obtained this way (i.e. as the kernel of a $\mathbb{C}$-valued point). Furthermore, for two such points $\boldsymbol{p}, \boldsymbol{p}'$, we have $\mathfrak{m}_{\boldsymbol{p}} = \mathfrak{m}_{\boldsymbol{p}'}$ if and only if $e_{\sigma\boldsymbol{p}} = e_{\boldsymbol{p}'}$ for some $\sigma \in \operatorname{Gal}(\mathbb{C}/\mathbb{R})$, where $\sigma\boldsymbol{p} = \sigma(a,b) = (\sigma a, \sigma b)$. This holds more generally in the case where $\mathbb{k} \neq \mathbb{R}$. Indeed, choose an algebraic closure $\overline{\mathbb{k}}$ of $\mathbb{k}$. Then we have natural bijections:

$$\{\text{maximal ideals of } S\} \simeq \{\text{closed points of } X\} \simeq \{\overline{\mathbb{k}}\text{-valued points of } X\}/\sim,$$

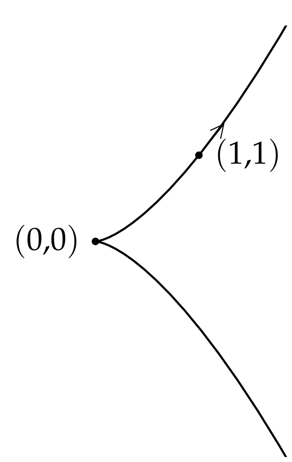
where $\boldsymbol{p} \sim \boldsymbol{p}'$ if $\boldsymbol{p} = \sigma\boldsymbol{p}'$ for some $\sigma \in \operatorname{Gal}(\overline{\mathbb{k}}/\mathbb{k})$. With this in mind, recall that for each closed point $\boldsymbol{p}$ of X, we have

$$\operatorname{Hom}_S(\Omega^1_{S/\mathbb{k}}, \mathbb{k}_{\boldsymbol{p}}) = \{\text{point derivations } \partial \colon S \to \mathbb{k}_{\boldsymbol{p}}\}.$$

Thus we can think of $\operatorname{Hom}_S(\Omega^1_{S/\mathbb{k}}, \mathbb{k}_{\boldsymbol{p}})$ as the set of all tangent vectors at $\boldsymbol{p}$. For instance, the point derivations at the origin $\mathbf{0} = (0,0)$ correspond to all vectors $\boldsymbol{v} = (v_x, v_y) \in \mathbb{k}^2$ since $v_x\widetilde{\partial}_x|_{\mathbf{0}} + v_y\widetilde{\partial}_y|_{\mathbf{0}}$ vanishes on $2y\mathrm{d}y - 3x^2\mathrm{d}x$. On the other hand, the point derivations at the point $\boldsymbol{p} = (1,1)$ correspond to all vector $\boldsymbol{v} \in \mathbb{k}^2$ such that $-3v_x + 2v_y = 0$ since

$$(v_x\widetilde{\partial}_x|_{\boldsymbol{p}} + v_y\widetilde{\partial}_y|_{\boldsymbol{p}})(2y\mathrm{d}y - 3x^2\mathrm{d}x) = -3v_x + 2v_y = 0.$$

For instance, the point derivation $(1/3)\widetilde{\partial}_x|_{\boldsymbol{p}} + (1/2)\widetilde{\partial}_y|_{\boldsymbol{p}}$ can be visualized on the curve as the tangent vector centered at $(1,1)$ as below:



Example 58.5. Let R be a ring, let $A = R[x,y,z]/f$ where $f = x^2 + y^2 + z^2 - 1$, and let $X = \operatorname{Spec} A$. Thus the R-valued points of X (over R) forms the unit sphere in $\mathbb{A}^3(R)$. The conormal sequence gives us the following description of the module of differentials:

$$\Omega = \Omega^1_{A/R} = \frac{A\mathrm{d}x \oplus A\mathrm{d}y \oplus A\mathrm{d}z}{2x\mathrm{d}x + 2y\mathrm{d}y + 2z\mathrm{d}z} = \operatorname{coker}\left(A \xrightarrow{\varphi} A^3\right),$$

where $\varphi = (2x, 2y, 2z)^\top$. Notice that $\mathrm{F}_1(\Omega) = 0$ and $\mathrm{F}_2(\Omega) = \langle 2 \rangle$ since $\{x, y, z\}$ generates the unit ideal in A. Now assume $2 \in R^\times$. In this case, Ω is a finite projective A-module of rank 2. In particular, if we set $\boldsymbol{s} = (s_1, s_2, s_3) = (x, y, z)$, then $\{U_i := \mathrm{D}(s_i)\}_{i=1,2,3}$ forms an open cover of X and $\Omega_{s_i} \cong A^2_{s_i}$ for $i = 1, 2, 3$. Furthermore, the conormal sequence gives us the following split exact sequence:

$$0 \longrightarrow A \xrightarrow{\begin{pmatrix} 2x \\ 2y \\ 2z \end{pmatrix}} A^3 \longrightarrow \Omega \longrightarrow 0 \tag{212}$$

In other words, we have $\Omega \oplus A \cong A^3$. In particular, this implies that A is a smooth R-algebra and Ω is stably-free. Since additive functors take split exact sequences to split exact sequences, applying $\operatorname{Hom}_A(-, A)$ to (213) gives us the following split exact sequence:

$$0 \longrightarrow T \longrightarrow A^3 \xrightarrow{\begin{pmatrix} 2x & 2y & 2z \end{pmatrix}} A \longrightarrow 0 \tag{213}$$

where we set $T = \Omega^\vee = \operatorname{Der}_R(A, A)$. If we apply $\operatorname{Hom}_S(-, S)$ to the presentation of Ω, then we obtain a copresentation of T, namely $T = \ker(A^3 \xrightarrow{\varphi^\top} A)$. The module T is thought of as the "polynomial sections of the tangent bundle". If we write $A^3 = A\partial_x \oplus A\partial_y \oplus A\partial_z$, then T is generated by $y\partial_x - x\partial_y$, $z\partial_x - x\partial_z$, and $z\partial_y - y\partial_z$. If $R = \mathbb{R}$, then it is known that T is an example of a stably-free A-module which isn't free. The proof of this involves a non-trivial topological fact about the 2-sphere, namely the hairy ball theorem.

Example 58.6. Let M be a smooth manifold and let $A = \mathrm{C}^\infty(M)$. Recall that a derivation at a point $p \in M$ is defined to be an $\mathbb{R}$-linear map $\partial \colon A \to \mathbb{R}$ which satisfies the Leibniz law at p which says for all $f, g \in A$ we have

$$\partial(fg) = (\partial f)g(p) + f(p)\partial g.$$

In particular, this is just an $\mathbb{R}$-linear $\mathbb{R}_p$-derivation of A where $\mathbb{R}_p = A/\mathfrak{m}_p$ where $\mathfrak{m}_p = \{f \in A \mid f(p) = 0\}$. In differential geometry, one defines the tangent space of M at p, denoted $\mathrm{T}_p(M)$, to be the $\mathbb{R}$-vector space of all such derivations at p. In particular, we see that

$$\mathrm{T}_p(M) \simeq \operatorname{Hom}_A(\Omega_{A/\mathbb{R}}, \mathbb{R}_p).$$

Example 58.7. Let L/K be a finite extension of fields and assume that L can be presented as a K-algebra $K[x] \twoheadrightarrow L$ where $x \mapsto \alpha$ where $\alpha \in L$. Thus if π is the minimal polynomial of α over K, then we have $K[x]/\pi \cong L$. Then the conormal sequence of $K \to K[x] \twoheadrightarrow L$ has the form

$$\langle \pi \rangle / \langle \pi^2 \rangle \xrightarrow{\mathrm{d}} L\mathrm{d}x \longrightarrow \Omega_{L/K} \longrightarrow 0 \tag{214}$$

where the map d is given by $\mathrm{d}(\overline{\pi}) = \pi'(\alpha)\mathrm{d}x$ where π' is the usual derivative of π with respect to x. Note that $\pi'(\alpha) = 0$ if and only if $\pi' = 0$ since π is the minimal polynomial of α and $\deg \pi' < \deg \pi$. Thus

$$\Omega_{L/K} = \begin{cases} 0 & \text{if } L/K \text{ is separable} \\ L\mathrm{d}x & \text{if } L/K \text{ is inseparable} \end{cases}$$

Example 58.8. Let A be an integral domain, let B be an A-algebra, and assume that $B = A[b]$ where b is integral over A, say $f(b) = 0$ where $f \in A[x]$ is given by

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where $n \geq 2$ is minimal. Then the conormal sequence of $A \to A[x] \twoheadrightarrow B$ has the form

$$\langle f \rangle / \langle f^2 \rangle \xrightarrow{\mathrm{d}} B\mathrm{d}x \longrightarrow \Omega^1_{B/A} \longrightarrow 0 \tag{215}$$

where the map d is given by $\mathrm{d}(\overline{f}) = f'(b)\mathrm{d}x$ where f' is the usual derivative of f with respect to x. In particular, we have $\Omega^1_{B/A} \cong B/f'(b)$.

Lemma 58.2. *Let B be an A-algebra such that B is an integral domain. Suppose b is integral over A, say*

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0, \tag{216}$$

where $n \geq 2$ is minimal. If n is a unit in A, then $\mathrm{d}b = 0$. *In particular, we have $\Omega_{A[b]/A} = 0$.*

Proof. Applying $(1/n)\mathrm{d}$ to both sides of (220) gives us

$$(b^{n-1} + (n-1)(a_{n-1}/n)b^{n-2} + \cdots + (a_1/n))\mathrm{d}b = 0.$$

Thus if $\mathrm{d}b \neq 0$, then we must have

$$b^{n-1} + (n-1)(a_{n-1}/n)b^{n-2} + \cdots + (a_1/n) = 0.$$

However this contradicts minimality of n, so we must have $\mathrm{d}b = 0$. $\square$

Remark 97. Let $(S, \mathfrak{m}, \Bbbk')$ be a local noetherian ring such that S contains a field $\Bbbk$ and the induced field extension $\Bbbk'/\Bbbk$ is finite and separable. Then conormal sequence gives us a surjection $\mathfrak{m}/\mathfrak{m}^2 \twoheadrightarrow \Bbbk' \otimes_S \Omega_{S/\Bbbk}$ of $\Bbbk'$-vector spaces. Let W be the kernel of this map. Then applying $\mathrm{Hom}_{\Bbbk'}(-, \Bbbk')$ as well as tensor-hom adjointness gives us an exact sequence of $\Bbbk'$-vector spaces

$$0 \longrightarrow \mathrm{Hom}_S(\Omega_{S/\Bbbk}, \Bbbk') \longrightarrow \mathrm{T}_{\mathfrak{m}}(R) \longrightarrow W^\star \longrightarrow 0 \tag{217}$$

where we set $W^\star = \mathrm{Hom}_{\Bbbk'}(W, \Bbbk')$. In particular, we see that

$$\begin{aligned} \mathrm{Hom}_S(\Omega_{S/\Bbbk}, \Bbbk) \simeq \mathrm{T}_{\mathfrak{m}}(R) &\iff \mathfrak{m}/\mathfrak{m}^2 \simeq \Bbbk' \otimes_S \Omega_{S/\Bbbk} \\ &\iff \dim_{\Bbbk}(\mathfrak{m}/\mathfrak{m}^2) = \dim_{\Bbbk}(\Bbbk' \otimes_S \Omega_{S/\Bbbk}) \\ &\iff \beta_1(\mathfrak{m}) = \beta_1(\Omega_{S/\Bbbk}), \end{aligned}$$

where we used Nakayama's lemma in the last line.

Example 58.9. Let A be a commutative ring and let $x \in A$. Then the localization A_x can be presented as an A-algebra as $A_x = A[y]/\langle 1 - yx \rangle$. In particular, we see that

$$\Omega_{A_x/A} = \frac{A_x \mathrm{d}y}{x A_x \mathrm{d}y} = 0,$$

where we used the fact that x is a unit in A_x.

Example 58.10. Let $R = \Bbbk[x, y, z, w]$, let $\boldsymbol{m} = x^2, w^2, zw, xy, y^2z^2$, and let $S = R/\boldsymbol{m}$. Then $\Omega_{S/\Bbbk}$ has the following presentation as an S-module:

$$S^5 \xrightarrow{\begin{pmatrix} 2x & 0 & 0 & y & 0 \\ 0 & 0 & 0 & x & 2yz^2 \\ 0 & 0 & w & 0 & y^2z \\ 0 & 2w & z & 0 & 0 \end{pmatrix}} S^4 \xrightarrow{\begin{pmatrix} \mathrm{d}x & \mathrm{d}y & \mathrm{d}z & \mathrm{d}w \end{pmatrix}} \Omega_{S/\Bbbk}$$

In particular, we have the following relations in $\Omega_{S/\Bbbk}$:

$$\begin{aligned} 2x\mathrm{d}x &= 0 \\ 2w\mathrm{d}w &= 0 \\ w\mathrm{d}z + z\mathrm{d}w &= 0 \\ y\mathrm{d}x + x\mathrm{d}y &= 0 \\ 2yz^2\mathrm{d}y + 2y^2z\mathrm{d}z &= 0. \end{aligned}$$

Notice that $\Bbbk \otimes_S \Omega_{S/\Bbbk} = 0$. The Fitting invariants of $\Omega_{S/\Bbbk}$ are given below:

$$\begin{aligned} &\mathrm{F}_0(\Omega_{S/\Bbbk}) = 0 \\ &\mathrm{F}_1(\Omega_{S/\Bbbk}) = \langle x^2w^2, x^2y^2z^2, x^2y^2zw, xyz^2w^2, y^2z^2w^2 \rangle \\ &\mathrm{F}_2(\Omega_{S/\Bbbk}) = \langle x^2z, x^2w, xw^2, yw^2, xy^2z^2, y^3z^2, xyz^3, y^2z^3, xy^2zw, y^3zw, xyz^2w, y^2z^2w \rangle \\ &\mathrm{F}_3(\Omega_{S/\Bbbk}) = \langle x^2, w^2, xz, xw, yw, yz \rangle \\ &\mathrm{F}_4(\Omega_{S/\Bbbk}) = \langle x, y, z, w \rangle \\ &\mathrm{F}_5(\Omega_{S/\Bbbk}) = R. \end{aligned}$$

58.2 Extensions of Algebras by Modules

Definition 58.4. Let R be a ring, let A be an R-algebra, and let M be an A-module. An R**-extension** of A by M is an exact sequence of the form

$$0 \longrightarrow M \xrightarrow{\varepsilon} E \xrightarrow{\pi} A \longrightarrow 0 \tag{218}$$

where E is an R-algebra, where $\pi\colon E \to A$ is an R-algebra homomorphism, and where $\varepsilon\colon M \to E$ is an E-module homomorphism. The last part means that

$$\varepsilon em := \varepsilon\pi em = e\varepsilon m$$

for all $e \in E$ and $m \in M$. In particular, note that this implies εM is an ideal of square zero in E since

$$(\varepsilon m)(\varepsilon m') = \varepsilon\varepsilon mm' = \varepsilon\pi\varepsilon mm' = 0.$$

In order to simplify notation, we often refer to the extension (218) via just E and we view the other data as being "attached" to E. For instance, if we write "let E be an R-extension of M by A", then it'll be understood that this comes with an E-module homomorphism $\varepsilon_E\colon M \to E$ as well as an R-algebra homomorphism $\pi_E\colon E \to A$ which fit together to form a short exact sequence of A-modules. If context is clear, then we often simplify further by writing $\varepsilon = \varepsilon_E$ and $\pi = \pi_E$. With this in mind, two extensions E and E' are called **equivalent** if there exists an R-algebra homomorphism $\phi\colon E \to E'$ making the following diagram commute

$$\begin{tikzcd} & & E \arrow[dd, "\phi"] \arrow[dr] & & \\ 0 \arrow[r] & M \arrow[ur] \arrow[dr] & & A \arrow[r] & 0 \\ & & E' \arrow[ur] & & \end{tikzcd} \tag{219}$$

In other words, ϕ is an R-algebra homomorphism such that

$$\phi\varepsilon m = \varepsilon' m \quad \text{and} \quad \pi'\phi e = \pi e$$

for all $m \in M$ and $e \in E$. Note that ϕ is automatically an isomorphism of R-algebras by the Five Lemma. The set of equivalence classes of R-extensions of A by M is denoted $\mathrm{Ex}_R(A, M)$.

Example 58.11. Define $D = \mathrm{D}_A M$ to be the R-algebra whose underlying module is

$$D = \mathrm{D}_A M = M \oplus A = \varepsilon M + A$$

and whose multiplication is defined by

$$(\varepsilon m + a)(\varepsilon m + a') = \varepsilon(am' + a'm) + aa'$$

for all $a \in A$ and $m \in M$. Intuitively, we think of ε as an element which commutes with everything and satisfies $\varepsilon^2 = 0$. Let $\varepsilon_D\colon M \to D$ be given by $\varepsilon_D m = \varepsilon m$ and let $\pi_D\colon D \to A$ be given by $\pi_D(\varepsilon m + a) = a$. Then D (together with ε_D and π_D) is an R-extension of A by M. We call this the **trivial extension**. Note that an extension is equvalent to the trivial extension if and only if there exists an R-algebra homomorphism $\widetilde{\pi}\colon A \to E$ such that $\pi\widetilde{\pi} = 1$.

Remark 98. Let E be an R-extension of A by M and let $\theta\colon A' \to A$ be an R-algebra homomorphism. Then $\mathrm{Der}_R(A', M)$ acts simply transitively on the set of all R-algebra homomorphisms $\widetilde{\theta}\colon A' \to E$ such that $\pi\widetilde{\theta} = \theta$. This says that if $\widetilde{\theta}_1, \widetilde{\theta}_2\colon A' \to A$ are any two R-algebra homomorphisms which lifts the R-algebra homomorphism $\theta\colon A' \to A$, then there exists a unique R-linear M-derivation $\partial\colon A \to M$ such that $\widetilde{\theta}_1 = \widetilde{\theta}_2 + \partial$.

Remark 99. Let R be a ring, let A be an R-algebra, and let M be an A-module.

1. Observe that $\mathrm{Ex}_R(A, M)$ is functorial in M. Indeed, let $\varphi\colon M \to M'$ be an A-module homomorphism and let E be an R-extension of A by M, then the pushout $E' := E +_M M'$ is an R-extension of A by M'. Here we have
$$E' = (M' \oplus E)/\{(\varphi m, -\alpha m) \mid m \in M\}$$
We denote a coset in E' with representative (m', e) by $\varepsilon_\varphi m' + e$ where we think of ε_φ as an element which commutes with everything and satisfies $\varepsilon_\varphi^2 = 0$ and $\varepsilon_\varphi \varphi m = \alpha m$. This notation suggests we define multiplication on E' by
$$(\varepsilon_\varphi m_1' + e_1)(\varepsilon_\varphi m_2' + e_2) = \varepsilon_\varphi(e_1 m_2' + e_2 m_1') + e_1 e_2,$$
and indeed, if we define multiplication this way then we can show that the map $\varepsilon'\colon M' \to E'$ given by $\varepsilon' m' = \varepsilon_\varphi m'$ is an E'-module homomorphism. Similarly, we can show that the map $\pi'\colon E' \to A$ given by $\pi'(\varepsilon_\varphi m' + e) = \pi e$ is an R-algebra homomorphism.

2. Assume that $M = \prod_{i\in I} M_i$ be a product of A-modules. Then the projections $\rho_i\colon M \to M_i$ induce via functoriality a map
$$\mathrm{Ex}_R(A, M) \to \prod_{i\in I} \mathrm{Ex}_R(A, M_i)$$
which is bijective. The inverse to this map is given by sending $(E_i) \in \prod_{i\in I} \mathrm{Ex}_R(A, M_i)$ to the R-extension of A by M given by
$$E := \left\{ (e_i) \in \prod_{i\in I} E_i \mid \pi_i(e_i) = \pi_j(e_j) \text{ for all } i, j \right\}.$$

Assertions (1) and (2) show that addition and scalar-multiplication on M yield the structure of an A-module on $\mathrm{Ex}_R(A, M)$ and that $M \mapsto \mathrm{Ex}_R(A, M)$ is an A-linear functor from the category of A-modules to itself.

Proposition 58.6. *Let $R \to A \to B$ be ring homomorphisms and let N be a B-module. Then*

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Der}_A(B,N) \arrow[r] & \mathrm{Der}_R(B,N) \arrow[r] & \mathrm{Der}_R(A,N) \arrow[dll, rounded corners, "\gamma"] \\
& \mathrm{Ex}_A(B,N) \arrow[r] & \mathrm{Ex}_R(B,N) \arrow[r] & \mathrm{Ex}_R(A,N)
\end{tikzcd}$$

is an exact sequence of R-modules where γ is given by $\gamma(\partial) = D := \mathrm{D}_B N$ with A-algebra structure $A \to D$ given by $a \mapsto \varepsilon a + \partial a$.

Proposition 58.7. *Let I be an ideal of R and set $\overline{R} = R/I$. Then for every $\overline{R}$-module N there exists an isomorphism, functorial in N*
$$\Phi\colon \mathrm{Hom}_{\overline{R}}(I/I^2, N) \simeq \mathrm{Ex}_R(\overline{R}, N).$$

Proof. Observe that R/I^2 is an R-extension of $\overline{R}$ by I/I^2. For any $\overline{R}$-module homomorphism $\varphi\colon I/I^2 \to N$ we obtain by functoriality of $\mathrm{Ex}_R(\overline{R}, -)$ an element $\Phi(\varphi) \in \mathrm{Ex}_R(\overline{R}, N)$. Conversely, if E is an R-extension of $\overline{R}$ by N, then we attach the R-linear map $\varphi\colon I \to R \to E$. Then $\pi\varphi = 0$ and we may consider φ as an R-linear map $I \to N$ which induces an $\overline{R}$-linear map $I/I^2 \to N$ because N is an ideal of square zero in E. This defines an inverse to Φ. $\square$

58.3 Non-associative Construction

Let B be a commutative ring. We set $B[\mathrm{d}]$ to be the non-associative algebra obtained by adjoining a formal variable d to be B such that

1. $\mathrm{d}^2 = 0$ and $\mathrm{d}b = b\mathrm{d}$ for all $b \in B$;
2. $\mathrm{d}(b_1 + b_2) = \mathrm{d}b_1 + \mathrm{d}b_2$ for all $b_1, b_2 \in B$;
3. $[b_1, b_2, \mathrm{d}] = b_1(b_2\mathrm{d})$ for all $b_1, b_2 \in B$, where $[\cdot,\cdot,\cdot]$ is the associator of $B[\mathrm{d}]$.

In particular, (3) is equivalent to the Leibniz law:
$$\mathrm{d}(b_1 b_2) = (\mathrm{d}b_1)b_2 + b_1(\mathrm{d}b_2).$$

Note that the Leibniz law implies $\mathrm{d}(1) = 0$, and thus additivity of d implies $\mathrm{d}(\mathbb{Z}) = 0$. Thus we have

$$B[\mathrm{d}] = B + \Omega_{B/\mathbb{Z}}.$$

Now suppose that B is an A-algebra.

Lemma 58.3. *Let B be an A-algebra such that B is an integral domain. Suppose b is integral over A, say*

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0, \tag{220}$$

where $n \geq 2$ is minimal. If n is a unit in A, then $\mathrm{d}b = 0$. In particular, we have $\Omega_{A[b]/A} = 0$.

Proof. Applying $(1/n)\mathrm{d}$ to both sides of (220) gives us

$$(b^{n-1} + (n-1)(a_{n-1}/n)b^{n-2} + \cdots + (a_1/n))\mathrm{d}b = 0.$$

Thus if $\mathrm{d}b \neq 0$, then we must have

$$b^{n-1} + (n-1)(a_{n-1}/n)b^{n-2} + \cdots + (a_1/n) = 0.$$

However this contradicts minimality of n, so we must have $\mathrm{d}b = 0$. □

58.4 The Naive Cotangent Complex

Let A be an R-algebra. Denote by $R[A]$ to be the polynomial ring whose variables are the elements $a \in A$. Let's denote $x_a \in R[A]$ to be the variable corresponding to $a \in A$. Thus $R[A]$ is a free R-module on the monomials $x_{a_1} \cdots x_{a_n}$ where $a_1, \dots, a_n$ ranges over all unordered sequences of elements of A. There is a canonical surjection $R[A] \twoheadrightarrow A$ given by $x_a \mapsto a$ whose kernel we denote $I \subseteq R[A]$.

Proposition 58.8. *I is generated by elements of the form*

$$\begin{aligned} f_{\boldsymbol{a}} &= x_{a_1+a_2} - x_{a_1} - x_{a_2} \\ g_{\boldsymbol{a}} &= x_{a_1 a_2} - x_{a_1}x_{a_2} \\ h_r &= x_r - r, \end{aligned}$$

where $a_1, a_2 \in A$ and $r \in R$.

Proof. Clearly we have $\langle \{ f_{\boldsymbol{a}}, g_{\boldsymbol{a}}, h_r \} \rangle \subseteq I$. For the reverse inclusion, let $f = r_1 x^{\alpha_1} + \cdots + r_m x^{\alpha_m} \in I$ where $x^{\alpha_i} = x_{a_{i,1}} \cdots x_{a_{i,k_i}}$. Then using the relations above, we can express f as

$$f = x_a + g,$$

where $g \in \langle \{ f_{\boldsymbol{a}}, g_{\boldsymbol{a}}, h_r \} \rangle$ and $a = \sum_{i=1}^n r_i(a_{i,1} \cdots a_{i,k_i})$. This implies $x_a \in I$ which implies $x_a = 0$. It follows that $I \subseteq \langle \{ f_{\boldsymbol{a}}, g_{\boldsymbol{a}}, h_r \} \rangle$. □

Now observe that there is a canonical map

$$I/I^2 \to A \otimes_{R[A]} \Omega_{R[A]/R},$$

given by $\overline{f} \mapsto 1 \otimes \mathrm{d}f$ for all $f \in I$, whose cokernel is canonically isomorphic to $\Omega_{A/R}$. Furthermore, observe that $\Omega_{R[A]/R} \otimes_{R[A]} A$ is a free A-module on the generators $\mathrm{d}x_a$.

Definition 58.5. The **naive cotangent complex** $\mathrm{NL}_{A/R}$ is the chain complex

$$\mathrm{NL}_{A/R} = (I/I^2 \to A \otimes_{R[A]} \Omega_{R[A]/R})$$

where I/I^2 sits in homological degree 1 and $\Omega_{R[A]/R} \otimes_{R[A]} A$ sits in homological degree 0. We will denote $\mathrm{H}_1(\mathrm{L}_{A/R}) = \mathrm{H}_1(\mathrm{NL}_{A/R})$ the homology in degree 1.

Remark 100. There exists a canonical simplicial R-algebra P whose terms are polynomial algebras and which comes equipped with a canonical homotopy equivalence $P \xrightarrow{\simeq} A$. The cotangent complex $\mathrm{L}_{A/R}$ of A over R is defined as the chain complex associated to the cosimplicial module $A \otimes_R \Omega_{P/R}$. The naive cotangent complex as defined above is canonically isomorphic to $\tau_{\leq 1}\mathrm{L}_{A/R}$. In particular, it is indeed the case that $\mathrm{H}_1(\mathrm{NL}_{A/R}) = \mathrm{H}_1(\mathrm{L}_{A/R})$ so our definition is compatible with the one using the cotangent complex. Moreover we also have $\mathrm{H}_0(\mathrm{L}_{A/R}) = \mathrm{H}_0(\mathrm{NL}_{A/R}) = \Omega_{A/R}$.

58.5 Smooth Ring Maps

Definition 58.6. A ring map $R \to A$ is **smooth** if it is of finite presentation (meaning there exists integers $m, n \in \mathbb{N}$ and a sequence of polynomials $\boldsymbol{f} = f_1, \ldots, f_m$ in $R[x_1, \ldots, x_n] = R[\boldsymbol{x}]$ such that $A \cong R[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle$ as R-algebras) and the naive cotangent complex $\mathrm{NL}_{A/R}$ is quasi-isomorphic to a finite projective A-module placed in homological degree 0.

In particular, if $R \to A$ is smooth, then the module $\Omega_{A/R}$ is a finite projective A-module. Moreover, the naive cotangent complex of any presentation has the same structure. Thus for any surjection $\alpha \colon R[\boldsymbol{x}] \to A$ with kernel I the map

$$I/I^2 \to A \otimes_{R[\boldsymbol{x}]} \Omega_{R[\boldsymbol{x}]/R} \simeq \bigoplus_{i=1}^{n} A\mathrm{d}x_i$$

is a split injection. In other words, we have

$$\bigoplus_{i=1}^{n} A\mathrm{d}x_i \cong I/I^2 \oplus \Omega_{A/R}$$

as A-modules. This implies that I/I^2 is a finite projective A-module too!

Remark 101. Let $A \to B$ be a ring map of finite presentation. If for some presentation α of B over A the naive cotangent complex $\mathrm{NL}(\alpha)$ is quasi-isomorphic to a finite projective B-module placed in homological degree 0, then this holds for any presentation.

Example 58.12. Suppose that A is a ring and that $B = A[x,y]/f$ for some nonzero $f \in A[x,y]$. In this case there is an exact sequence

$$B \longrightarrow B\mathrm{d}x \oplus B\mathrm{d}y \longrightarrow \Omega_{B/A} \longrightarrow 0 \tag{221}$$

$$B \to B\mathrm{d}x \oplus B\mathrm{d}y \to \Omega_{B/A} \to 0,$$

where the first map sends 1 to $\partial_x f \mathrm{d}x + \partial_y f \mathrm{d}y$. We conclude that $\Omega_{B/A}$ is locally free of rank 1 if the partial derivatives of f generate the unit ideal in B. In this case B is smooth of relative dimension 1 over A. But it can happen that $\Omega_{B/A}$ is locally free of rank 2, namely if both partial derivatives of f are zero. For example if for a prime p we have $p = 0$ in A and $f = x^p + y^p$ then this happens. Here $A \to B$ is a relative global complete intersection of relative dimension 1 which is not smooth. Hence, in order to check that a ring map is smooth it is not sufficient to check whether the module of differentials is free.

Lemma 58.4. *Let $A \to B$ be a smooth ring map. Any localization B_t where $t \in B$ is smooth over A. If $s \in A$ map to an invertible element of B, then $A_s \to B$ is smooth.*

Proof. The naive cotangent complex of B_t over A is the base change of the naive cotangent complex of B over A. The assumption is that the naive cotangent complex of B/A is $\Omega_{B/A}$ and that this is a finite projective B-module. Hence so is its base change. Thus B_t is smooth over A. □

Lemma 58.5. *(smoothness is preserved under base change) Let $A \to B$ be a smooth ring map and let $A \to A'$ be any ring map. Then the base change $A' \to B' := A' \otimes_A B$ is smooth.*

Proof. Let $\alpha \colon A[\boldsymbol{x}] \to B$ be a presentation with kernel I. Let $\alpha' \colon A'[\boldsymbol{x}] \to A' \otimes_A B$ be the induced presentation with kernel I'. Since

$$0 \longrightarrow I \longrightarrow A[\boldsymbol{x}] \longrightarrow B \longrightarrow 0$$

is exact, the sequence

$$A' \otimes_A I \longrightarrow A'[\boldsymbol{x}] \longrightarrow A' \otimes_A B \longrightarrow 0$$

is exact. Thus $A' \otimes_A I \to I'$ is surjective. Since $A \to B$ is smooth, we have a short exact sequence

$$0 \longrightarrow I/I^2 \longrightarrow \Omega_{A[\boldsymbol{x}]/A} \otimes_{A[\boldsymbol{x}]} B \longrightarrow \Omega_{B/A} \longrightarrow 0$$

and the B-module $\Omega_{B/A}$ is finite projective. In particular, I/I^2 is a direct summand of $\Omega_{A[\boldsymbol{x}]/A} \otimes_{A[\boldsymbol{x}]} B$. Consider the commutative diagram

$$\begin{tikzcd}
A' \otimes_A (I/I^2) \arrow[r] \arrow[d] & A' \otimes_A (\Omega_{A[\boldsymbol{x}]/A} \otimes_{A[\boldsymbol{x}]} B) \arrow[d] \\
I'/(I')^2 \arrow[r] & \Omega_{A'[\boldsymbol{x}]/A'} \otimes_{A'[\boldsymbol{x}]} (A' \otimes_A B)
\end{tikzcd}$$

Since the right vertical map is an isomorphism we see that the left vertical map is injective and surjective by what was said above. Thus we conclude that $\mathrm{NL}(\alpha')$ is quasi-isomorphic to $\Omega_{B'/A'} \simeq B' \otimes_A \Omega_{B/A}$. And this is finite projective since it is the base change of a finte projective module.

□

Definition 58.7. Let A be a ring and set $B = A[x_1, \dots, x_n]/\langle f_1, \dots, f_m \rangle = A[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle$ where $0 \leq m \leq n$. We say B is a **standard smooth algebra** over A if the polynomial

$$g = \det \begin{pmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_m} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_m & \cdots & \partial_{x_m} f_m \end{pmatrix} \in A[\boldsymbol{x}]$$

is a unit B.

Example 58.13. Let $R = \mathbb{Z}[x,y]$ and let $S = \mathbb{Z}[x,y]/f$ where $f = xy - 1$. The ideal generated by the maximal minors of $\mathrm{J}_f = \begin{pmatrix} y & x \end{pmatrix}$ is the unit ideal in S, so S is a smooth $\mathbb{Z}$-algebra. Note that we can also express S as a localization, namely $S \simeq \mathbb{Z}[x, 1/x]$. Consider the complex $\Omega_{S/\mathbb{Z}}$ whose underlying graded module is

$$\Omega^i_{S/\mathbb{Z}} = \begin{cases} S & \text{if } i = 0 \\ S\mathrm{d}x & \text{if } i = 1 \\ 0 & \text{else} \end{cases}$$

and whose differential $\mathrm{d} \colon S \to S\mathrm{d}x$ is defined by $\mathrm{d}(t^n) = nt^{n-1}\mathrm{d}t$ for all $n \in \mathbb{Z}$. Thus if $\sum c_n t^n \in S$, where $c_n \in \mathbb{Z}$, then we have

$$\mathrm{d}\left(\sum_{n \in \mathbb{Z}} c_n t^n \right) = \sum_{n \in \mathbb{Z}} n c_n t^{n-1} \mathrm{d}t.$$

In particular, $\omega = t^{-1}\mathrm{d}t$ defines a class in $\mathrm{H}^1_{\mathrm{dR}}(X)$ where we set $X = \mathbb{G}_m = \operatorname{Spec} S$. On the other hand, let F be the minimal R-free resolution of S. Thus as a graded R-module, F has the form

$$F_i = \begin{cases} R & \text{if } i = 0 \\ Re & \text{if } i = 1 \\ 0 & \text{else} \end{cases}$$

and the differential of F is defined by $\mathrm{d}(e) = f$. Thus if $r_1 + r_2 e \in F$ where $r_1, r_2 \in R$, then $\mathrm{d}(r_1 + r_2 e) = r_2 f$. Let us denote $F_S = F \otimes_R S$, so F_S is an S-complex whose underlying graded S-module is

$$F_{S,i} \simeq \begin{cases} S & \text{if } i = 0 \\ Se & \text{if } i = 1 \\ 0 & \text{else} \end{cases}$$

In this case, we have $\mathrm{H}_1(F_S) = \mathrm{Tor}^R_1(S,S) = S$ and $\mathrm{H}_0(F_S) = S$. We have

$$\begin{aligned} \widetilde{F}_{-2} &= \mathbb{Z}\mathrm{d}x\mathrm{d}y \\ \widetilde{F}_{-1} &= \mathbb{Z}[x,y]\mathrm{d}x + \mathbb{Z}[y]\mathrm{d}y + e\mathbb{Z}\mathrm{d}x\mathrm{d}y \\ \widetilde{F}_0 &= \mathbb{Z}[x,y] + e\mathbb{Z}[x,y]\mathrm{d}x + e\mathbb{Z}[y]\mathrm{d}y \\ \widetilde{F}_1 &= e\mathbb{Z}[x,y] \end{aligned}$$

Next observe that=

$$\begin{aligned} \mathrm{d}(e\mathrm{d}x\mathrm{d}y) &= -\mathrm{d}x\mathrm{d}y \\ \mathrm{d}(y\mathrm{d}x) &= -\mathrm{d}x\mathrm{d}y \\ \mathrm{d}(1) &= 0 \\ \mathrm{d}(e\mathrm{d}x) &= xy\mathrm{d}x - \mathrm{d}x \\ \mathrm{d}(e\mathrm{d}y) &= -y^2\mathrm{d}x - \mathrm{d}y \\ \mathrm{d}(ey\mathrm{d}x) &= (xy-1)y\mathrm{d}x + e\mathrm{d}x\mathrm{d}y \\ \mathrm{d}(ex\mathrm{d}x) &= (xy-1)x\mathrm{d}x \\ \mathrm{d}(exy) &= (xy-1)xy \\ \mathrm{d}(ey) &= (xy-1)y - e\mathrm{d}y \\ \mathrm{d}(ex) &= (xy-1)x - e\mathrm{d}x \\ \mathrm{d}e &= xy - 1 \end{aligned}$$

Thus we have $[1] = [(xy)^n]$ for all $n \geq 1$. Similarly we have $0 = [\mathrm{d}x] = [(xy)^n \mathrm{d}x]$ and $0 = [\mathrm{d}y] = [(xy)^n \mathrm{d}y]$ for all $n \geq 1$. We also see that

$$[xy\mathrm{d}x] = [\mathrm{d}x] = [-y^2\mathrm{d}x]$$

in $\mathrm{H}_{-1}(\widetilde{F})$ for all $n \geq 0$. Next observe that $\mathrm{d}(e\mathrm{d}x\mathrm{d}y - y\mathrm{d}x) = 0$, but note that

$$[e\mathrm{d}x\mathrm{d}y - y\mathrm{d}x] = [((-xy+1)y - y)\mathrm{d}x] = [-xy^2\mathrm{d}x] = [-x\mathrm{d}x],$$

and this should be a nontrivial element in $\mathrm{H}_{-1}(\widetilde{F})$ (it should remind you of $t^{-1}\mathrm{d}t$). Therefore

$$\mathrm{H}_i(\widetilde{F}) = \begin{cases} 0 & \text{if } i = -2 \\ \mathbb{Z} & \text{if } i = -1 \\ \mathbb{Z} & \text{if } i = 0 \\ 0 & \text{if } i = 1 \end{cases}$$

Example 58.14. Let $\Bbbk$ be a field of characteristic $\neq 2$ and let $A = \Bbbk[\boldsymbol{x}]/\boldsymbol{f} = \Bbbk[x_1, x_2, x_3]/\langle f_1, f_2 \rangle$ where $f_1 = x_1^2 + x_2^2 + x_3^2 - 1$ and $f_2 = x_1x_2x_3$. Then

$$\mathrm{J}_{\boldsymbol{f}} = \begin{pmatrix} 2x_1 & 2x_2 & 2x_3 \\ x_2x_3 & x_1x_3 & x_1x_2 \end{pmatrix}.$$

In particular, if $p = (1,0,0)$, then $\mathrm{J}_{\boldsymbol{f}}(p) = \left(\begin{smallmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ has rank 1.

Proposition 58.9. *Let R be a noetherian ring and let A be a smooth R-algebra. Then A is flat as an R-module.*

Proof. Let S be a localization of a □

Proof. Recall that A is a flat R-module if and only $A_{\mathfrak{p}}$ is a flat $R_{\mathfrak{p}}$-module for all primes $\mathfrak{p}$ of R. Thus we may assume that $R = (R, \mathfrak{m}, \Bbbk)$ is local. Then since □

Proposition 58.10. *Let $A \to B$ be a local homomorphism of local noetherian rings. Then the following are equivalent:*

1. *B is a formally smooth A-algebra in the $\mathfrak{m}_B$-adic topology;*
2. *B is a flat A-module and the $\Bbbk_A$-algebra $\Bbbk_A \otimes_A B$ is geometrically regular.*

58.6 Étale Ring Maps

Definition 58.8. Let $\varphi\colon A \to B$ be a ring map. We say φ is **étale** if it is of finite presentation and the naive cotangent complex $\mathrm{NL}_{B/A}$ is quasi-isomorphic to zero. Given a prime $\mathfrak{q}$ of B we say that φ is **étale at** $\mathfrak{q}$ if there exists a $t \in B \backslash \mathfrak{q}$ such that $A \to B_t$ is étale.

In particular, we see that $\Omega_{B/A} = 0$ if B is étale over A. If φ is smooth, then φ is étale if and only if $\Omega_{B/A} = 0$.

Lemma 58.6. *Any étale ring map is standard smooth. More precisely, if $A \to B$ is étale, then there exists a presentation $B = A[x_1, \ldots, x_n]/\langle f_1, \ldots, f_n \rangle = A[\boldsymbol{x}]/\langle \boldsymbol{f} \rangle$ such that the image of $\deg \mathrm{J}_{\boldsymbol{f}}$ is invertible in B.*

Proof. Let $A \to B$ be étale. Choose a presentation $B = A[\boldsymbol{x}]/I$. As $A \to B$ is étale we know that

$$\mathrm{d}\colon I/I^2 \to \bigoplus_{i=1}^{n} B\mathrm{d}x_i$$

is an isomorphism, in particular I/I^2 is a free B-module. Thus we may assume (after possibly changing the presentation) that $I = \langle f_1, \ldots, f_m \rangle$ such that the classes $\overline{f}_i$ form a basis of I/I^2. It follows immediately from the fact that the displayed map above is an isomorphism, that $m = n$, and that $\deg \mathrm{J}_{\boldsymbol{f}}$ is invertible in B. □

58.7 Tangent Vector Fields and Infinitesimal Morphisms

Proposition 58.11. *Let $\varphi\colon A \to A'$ be a map of R-algebras and let $\delta\colon A \to A'$ be a map of abelian groups such that $\delta(A)^2 = 0$. Then $\varphi + \delta$ is a homomorphism of R-algebras if and only if δ is an R-linear derivation in the sense that*

$$\delta(a_1a_2) = \delta(a_1)\varphi(a_2) + \varphi(a_1)\delta(a_2)$$

for all $a_1, a_2 \in A$.

Proof. We have

$$\begin{aligned}(\varphi+\delta)(a_1)\cdot(\varphi+\delta)(a_2) &= (\varphi a_1+\delta a_1)(\varphi a_2+\delta a_2)\\ &= (\varphi a_1)(\varphi a_2)+(\varphi a_1)(\delta a_2)+(\delta a_1)(\varphi a_2)+(\delta a_1)(\delta a_2)\\ &= (\varphi a_1)(\varphi a_2)+(\varphi a_1)(\delta a_2)+(\delta a_1)(\varphi a_2)\\ &= \varphi(a_1a_2)+(\varphi a_1)(\delta a_2)+(\delta a_1)(\varphi a_2)\\ &= \varphi(a_1a_2)+\delta(a_1a_2)-\delta(a_1a_2)+(\varphi a_1)(\delta a_2)+(\delta a_1)(\varphi a_2)\\ &= (\varphi+\delta)(a_1a_2)-\delta(a_1a_2)+(\varphi a_1)(\delta a_2)+(\delta a_1)(\varphi a_2).\end{aligned}$$

□

Proposition 58.12. *Let $R \to A \to B$ be a rings with $\pi\colon A \to B$ an epimorphism and set $I = \ker \pi$. Then in the conormal sequence*

$$I/I^2 \longrightarrow B \otimes_A \Omega_{A/R} \longrightarrow \Omega_{B/R} \longrightarrow 0 \tag{222}$$

the map $\mathrm{d}\colon I/I^2 \to B \otimes_A \Omega_{A/R}$ is a split injection if and only if there is a map of R-algebras $\tau\colon B \to A/I^2$ splitting the projection map $A/I^2 \twoheadrightarrow A/I = B$.

59 Étale morphisms

Definition 59.1. Let A and B be local noetherian rings and let $\varphi\colon A \to B$ be a local ring homomorphism.

1. We say φ is an **unramified homomorphism of local rings** if
   (a) $\mathfrak{m}_A B = \mathfrak{m}_B$, or equivalently, if the fiber of B over $\mathfrak{m}_A$ is $\Bbbk_A$.
   (b) $\Bbbk_B$ is a finite separable extension of $\Bbbk_A$,
   (c) B is essentially of finite type over A, meaning B is the localization of a finite type A-algebra at a prime: thus it has the form
   $$B \cong A[t_1,\dots,t_n]_S/I_S = A[\boldsymbol{t}]_S/I_S,$$
   where I is an ideal of $A[\boldsymbol{t}]$ and where S is a multiplicatively closed subset of $A[\boldsymbol{t}]$.
2. We say φ is an **étale homomorphism of local rings** if it is flat and an unramified homomorphism of local rings.

Example 59.1. Let $A = \Bbbk[x]_{\langle x\rangle}$ and $B = \Bbbk[\sqrt{x}]_{\langle\sqrt{x}\rangle}$. Then the inclusion map $A \to B$ is not unramified since $\langle x\rangle B \neq \langle\sqrt{x}\rangle$.

Example 59.2. Let $\Bbbk'/\Bbbk$ be a non-separable or non-finte field extension, let $A = \Bbbk[x]_{\langle x\rangle}$ and let $B = \Bbbk'[x]_{\langle x\rangle}$. Then the inclusion map $A \to B$ is not unramified since $\Bbbk'/\Bbbk$ is not a finite separable field extension.

Example 59.3. Let $A = \Bbbk[x]_{\langle x\rangle}$ and let $B = \Bbbk[x^{1/p^\infty}]_{\langle x^{1/p^\infty}\rangle}$. Then $A \to B$ is not unramified since B is not essentially of finite type over A.

59.1 Formally Smooth / Unramified / Étale

Let A be an R-algebra equipped with the $\mathfrak{a}$-adic topology where $\mathfrak{a}$ is an ideal of A. Note that if $\mathfrak{a} = 0$, then A has the discrete topology (and so continuous maps out of A are the same thing as just functions out of A).

Definition 59.2. We say A is an **$\mathfrak{a}$-smooth** / **$\mathfrak{a}$-unramified** / **$\mathfrak{a}$-étale** R-algebra if it satisfies the following lifting property: for every continuous R-algebra homorphism $\varphi\colon A \to B/N$, where B is an R-algebra and N is a proper ideal of B such that $N^2 = 0$ and B/N is given the discrete topology, there exists at *least* / at *most* / *exactly* one R-algebra homomorphism $\widetilde{\varphi}\colon A \to B$ which makes lifts φ with respect to π, that is, $\pi \circ \widetilde{\varphi} = \varphi$. In other words, there exists at *least* / at *most* / *exactly* one R-algebra homomorphism $\widetilde{\varphi}\colon A \to B$ which makes the following diagram commute:

$$\begin{tikzcd} & B \arrow[d, "\pi"] \\ A \arrow[ur, dashed, "\widetilde{\varphi}"] \arrow[r, "\varphi"'] & B/N \end{tikzcd} \tag{223}$$

If $\mathfrak{a} = 0$, then we say **formally smooth / unramified / étale** instead.

Remark 102. Note that φ being continuous is equivalent to saying $\varphi(\mathfrak{a}^n) = 0$ for some n. Thus if $\widetilde{\varphi}\colon A \to B$ is a lift of φ, then we must have $\widetilde{\varphi}(\mathfrak{a}^n) \subseteq N$.

Remark 103. Note that φ being continuous means that for each $a \in A$ and $\beta \in B/N$ such that $\varphi(a) = \beta$, we have $\varphi(a + \mathfrak{a}^n) = \beta$ for some $n \geq 1$ where initially n depends on a and β, but in fact there exists a minimal n that works for all such a and β. Indeed, letting $a = 0 = \beta$ we see that $\varphi(\mathfrak{a}^n) = 0$ for some $n \in \mathbb{N}$. Choose n minimal such that $\varphi(\mathfrak{a}^n) = 0$. Then for any $a \in A \backslash \mathfrak{a}$ such that $\varphi(a) = 0$, we have $\varphi(a + \mathfrak{a}^n) = 0$ where n is minimal in this case too. Thus $\varphi^{-1}(0)$ is covered by disjoint translates of the open ball $\mathrm{B}_n(0) := \mathfrak{a}^n$:

$$\varphi^{-1}(0) = \bigcup_a \mathrm{B}_n(a)$$

where we set $\mathrm{B}_n(a) = a + \mathfrak{a}^n$ where a runs through a set of coset representatives of $A/\mathfrak{a}$ such that $\varphi(a) = 0$. Similarly, if $\varphi(a) = \beta$ where $\beta \neq 0$, then $\varphi(a + \mathfrak{a}^n) = \beta$ where n again is minimal. Thus $\varphi\colon A \to B/N$ factors through an R-algebra homomorphism $\overline{\varphi}\colon A/\mathfrak{a}^n \to B/N$ for some $n \geq 1$. Conversely, if φ factors through an R-algebra homomorphism of the form $\overline{\varphi}\colon A/\mathfrak{a}^n \to B/N$ for some $n \geq 1$, then $\varphi\colon A \to B/N$ is continuous.

Remark 104. Choose $n \geq 1$ minimal such that $\varphi\colon A \to B/N$ factors through $\overline{\varphi}\colon A/\mathfrak{a}^n \to B/N$. If $\widetilde{\overline{\varphi}}\colon A/\mathfrak{a}^n \to B$ is a lift of $\overline{\varphi}\colon A/\mathfrak{a}^n \to B/N$ with respect to $\pi\colon B \to B/N$, then $\widetilde{\overline{\varphi}} \circ \rho\colon A \to B$ is a lift of $\varphi\colon A \to B/N$ with respect to $\pi\colon B \to B/N$, where ρ is the canonical quotient map $\rho\colon A \to A/\mathfrak{a}^n$. Conversely, suppose that $\widetilde{\varphi}\colon A \to B$ is a lift of $\varphi\colon A \to B/N$ with respect to $\pi\colon B \to B/N$. Then $\widetilde{\varphi}(\mathfrak{a}^n) \subseteq N$, but we need not have $\widetilde{\varphi}(\mathfrak{a}^n) = 0$ (that is, $\widetilde{\varphi}$ need not factor through $A/\mathfrak{a}^n$).

Example 59.4. Let $A = \mathbb{k}[x,y]/\langle xy \rangle$, let $B = \mathbb{k}[\varepsilon]/\langle \varepsilon^3 \rangle$, and let $N = \langle \varepsilon^2 \rangle$. Let $\varphi\colon A \to B/N \simeq \mathbb{k}[\varepsilon]/\langle \varepsilon^2 \rangle$ be the $\mathbb{k}$-algebra homomorphism such that $\varphi(x) = \varepsilon = \varphi(y)$. Then a lift $\widetilde{\varphi}\colon A \to B$ of φ must have the form

$$\begin{aligned} \widetilde{\varphi}(x) &= \varepsilon + c\varepsilon^2 \\ \widetilde{\varphi}(y) &= \varepsilon + d\varepsilon^2, \end{aligned}$$

where $c, d \in \mathbb{k}$. However since $xy = 0$, we must also have $0 = (\varepsilon + c\varepsilon^2)(\varepsilon + d\varepsilon^2) = \varepsilon^2$ which doesn't hold in B. Therefore there cannot be an infinitesimal lift and so A is not a formally smooth $\mathbb{k}$-algebra.

60 Category Theory

ZFC stands for Zermelo-Frankel + Axiom of Choice. There are $9 + 1$ axioms in ZFC. We also consider NGB (Von Neumann-Gödel-Bernays).

60.1 Definition of a Category

Definition 60.1. A **category** $\mathcal{C}$ consists of:

- A class $\mathrm{Ob}(\mathcal{C})$ of **objects**. If $x \in \mathrm{Ob}(\mathcal{C})$, we simply write $x \in \mathcal{C}$.
- Given $x, y \in \mathcal{C}$, there's a class $\mathrm{Mor}_{\mathcal{C}}(x, y)$ of **morphisms**, whose elements are called **morphisms** or **arrows** from x to y. If $f \in \mathrm{Mor}_{\mathcal{C}}(x, y)$, we write $f\colon x \to y$.
- Given $f\colon x \to y$ and $g\colon y \to z$, there is a morphism called their **composite** and is denoted $g \circ f\colon x \to z$. To clean notation, we sometimes denote the composite as gf.

$$\begin{tikzcd} & y \arrow[dr, "g"] & \\ x \arrow[ur, "f"] \arrow[rr, "g\circ f"'] & & z \end{tikzcd}$$

- Composition is associative: $(h \circ g) \circ f = h \circ (g \circ f)$ if either side is well-defined.

$$\begin{tikzcd} \bullet \arrow[r, "g"] \arrow[dr, "h\circ f"] & \bullet \arrow[d, "h"] \\ \bullet \arrow[u, "f"] \arrow[ur, "g\circ f"] \arrow[r, "h\circ(g\circ f)=(h\circ g)\circ f"'] & \bullet \end{tikzcd}$$

- For any $x \in \mathcal{C}$, there is an **identity morphism** $1_x\colon x \to x$

$$\begin{tikzcd} x \arrow[loop above, "1_x"] \end{tikzcd}$$

- We have the **left and right unity laws**:

$$1_x \circ f = f \text{ for any } f\colon y \to x$$

$$g \circ 1_x = g \text{ for any } g\colon x \to y$$

60.1.1 Functors exactness

Proposition 60.1. *Let $\mathcal{F}$ and $\mathcal{G}$ be two functors from the category of R-modules to itself, let $\tau\colon \mathcal{F} \to \mathcal{G}$ be a natural isomorphism, and let*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3$$

be exact at M_2. Then

$$\mathcal{F}(M_1) \xrightarrow{\mathcal{F}(\varphi_1)} \mathcal{F}(M_2) \xrightarrow{\mathcal{F}(\varphi_1)} \mathcal{F}(M_3) \tag{224}$$

is exact at $\mathcal{F}(M_2)$ if and only if

$$\mathcal{G}(M_1) \xrightarrow{\mathcal{G}(\varphi_1)} \mathcal{G}(M_2) \xrightarrow{\mathcal{G}(\varphi_1)} \mathcal{G}(M_3)$$

is exact at $\mathcal{G}(M_2)$.

Proof. The natural transformation $\tau\colon \mathcal{F} \to \mathcal{G}$ gives us the commutative diagram

$$\begin{tikzcd} \mathcal{F}(M_1) \arrow[r, "\mathcal{F}(\varphi_1)"] \arrow[d, "\tau_{M_1}"] & \mathcal{F}(M_2) \arrow[r, "\mathcal{F}(\varphi_1)"] \arrow[d, "\tau_{M_2}"] & \mathcal{F}(M_3) \arrow[d, "\tau_{M_3}"] \\ \mathcal{G}(M_1) \arrow[r, "\mathcal{G}(\varphi_1)"] & \mathcal{G}(M_2) \arrow[r, "\mathcal{G}(\varphi_1)"] & \mathcal{G}(M_3) \end{tikzcd}$$

The proposition follows trivially from the 3×3 lemma. $\square$

60.2 Colimits

Definition 60.2. Let X be a set. A **preorder** on X is a binary relation that is reflexive and transitive.

Definition 60.3. Let $(I, \leq)$ be a preordered set. A system (M_i, μ_{ij}) of R-modules over I consists of a family of R-modules $\{M_i\}_{i \in I}$ indexed by I and a family of R-module maps $\{\mu_{ij} \colon M_i \to M_j\}_{i \leq j}$ such that for all $i \leq j \leq k$,

$$\mu_{ii} = 1_{M_i} \quad \text{and} \quad \mu_{ik} = \mu_{jk}\mu_{ij}.$$

We say (M, μ_{ij}) is a **directed system** if I is a directed set.

Lemma 60.1. *Let (M_i, μ_{ij}) be a system of R-modules over the preordered set I. The colimit of the system (M_i, μ_{ij}) is the quotient R-modules*

$$\bigoplus_{i \in I} M_i / \langle \{ (\iota_i(u_i) - \iota_j(\mu_{ij}(u_i)) \mid u_i \in M_i \text{ and } i \in I \} \rangle,$$

where $\iota_i \colon M_i \to \bigoplus_{i \in I} M_i$ is the natural inclusion. We denote the colimit $M = \mathrm{colim}_i M_i$. We denote $\pi \colon \bigoplus_{i \in I} M_i \to M$ the projection map and $\phi_i = \pi \circ \iota_i \colon M_i \to M$.

Proof. Note that $\phi_i = \phi_j \circ \mu_{ij}$ in the above construction. Indeed, let $u_i \in M_i$. Then

$$\begin{aligned}
(\phi_j \mu_{ij})(u_i) &= (\pi \iota_j \mu_{ij})(u_i) \\
&= \pi(\iota_j(\mu_{ij}(u_i))) \\
&= \pi(\iota_i(u_i)) \\
&= (\pi \iota_i)(u_i) \\
&= \varphi_i(u_i).
\end{aligned}$$

To show the pair (M, ϕ_i) is the colimit we have to show it satisfies the universal property: for any other such pair (Y, ψ_i) with $\psi_i \colon M_i \to Y$ and $\psi_i = \psi_j \circ \mu_{ij}$, there is a unique R-module homomorphism $g \colon M \to Y$ such that the following diagram commutes:

$$\begin{tikzcd}
M_i \arrow[rr, "\mu_{ij}"] \arrow[dr, "\phi_i"] \arrow[ddr, bend right, "\psi_i"'] & & M_j \arrow[dl, "\phi_j"'] \arrow[ddl, bend left, "\psi_j"] \\
& M \arrow[d, "g"] & \\
& Y &
\end{tikzcd}$$

and this is clear because we can define g by taking the map ψ_i on the sumand M_i in the direct sum $\bigoplus M_i$. $\square$

Lemma 60.2. *Let (M_i, μ_{ij}) be a system of R-modules over the preordered set I. Assume that I is directed. The colimit of the system (M_i, μ_{ij}) is canonically isomorphic to the module M defined as follows:*

1. *as a set let*
$$M = \left(\coprod_{i \in I} M_i \right) / \sim$$
where for $u \in M_i$ and $u' \in M_{i'}$ we have
$$u \sim u' \text{ if and only if } \mu_{ij}(u) = \mu_{i'j}(u') \text{ for some } j \geq i, i'$$

2. *as an abelian group for $u \in M_i$ and $u' \in M_{i'}$ we define the sum of the classes of u and u' in M to be the class of $\mu_{ij}(u) + \mu_{i'j}(u')$ where $j \in I$ is any index with $i \leq j$ and $i' \leq j$, and*

3. *as an R-module define $u \in M_i$ and $a \in R$ the product of a and the class of u in M to be the class of au in M.*

The canonical maps $\phi_i \colon M_i \to M$ are induced by the canonical maps $M_i \to \coprod_{i \in I} M_i$.

Part VI
Homological Algebra

61 Introduction

Homological Algebra is a subject in Mathematics whose origins can be traced back to Topology. Homological Algebra is a very diverse subject, so we will not attempt to give an all encompassing description of what Homological Algebra is, rather we give a partial description instead:

> Homological is the study of R-complexes and their homology.

Here R is understood to be a commutative ring with identity[7]. Whenever we write, "let M be an R-module" or "let (A, d) be an R-complex", then it is understood that R is a ring.

61.1 Notation and Conventions

Unless otherwise specified, let K be a field and let R be a commutative ring with identity.

61.1.1 Category Theory

In this document, we consider the following categories:

- The category of all sets and functions, denoted **Set**;
- The category of all rings and ring homomorphisms, denoted **Ring**;
- The category of all R-modules and R-linear maps, denoted $\mathbf{Mod}_R$;
- The category of all graded R-modules and graded R-linear maps, denoted $\mathbf{Grad}_R$;
- The category of all R-algebras R-algebra homorphisms, denoted $\mathbf{Alg}_R$;
- The category of all R-complexes and chain maps, denoted $\mathbf{Comp}_R$;
- The category of all R-complexes and homotopy classes of chain maps, denoted $\mathbf{HComp}_R$
- The category of all DG R-algebras DG algebra homomorphisms, denoted $\mathbf{DG}_R$.

62 Graded Rings and Modules

62.1 Graded Rings

Definition 62.1. Let H be an additive semigroup with identity 0. An H-**graded ring** R is a ring together with a direct sum decomposition

$$R = \bigoplus_{h \in H} R_h,$$

where the R_h are abelian groups which satisfy the property that if $r_{h_1} \in R_{h_1}$ and $r_{h_2} \in R_{h_2}$, then $r_{h_1} r_{h_2} \in R_{h_1+h_2}$. The R_h are called **homogeneous components of** R and the elements of R_h are called **homogeneous elements of degree** h. If r is a homogeneous element in R, then unless otherwise specified, we denote the degree of r by $\deg r$. When we say "let R be a graded ring", then it is understood that the homogeneous components of R are denoted R_h.

Proposition 62.1. *Let R be an H-graded ring. Then R_0 is a ring.*

Proof. First note that $1 \in R_0$ since if $r \in R_i$, the $1 \cdot r = r \in R_i$. If $r, s \in R_0$, then also $rs \in R_0$. It follows that R_0 is an abelian group equipped with a multiplication map with identity $1 \in R_0$. This multiplication map satisfies all of the properties which are required for R_0 to be a ring since it inherits these properties from R. $\square$

[7] Unless otherwise specified, all rings discussed in this document are assumed to be commutative and unital.

We are mostly interested in the case where $H = \mathbb{N}^n$ or $H = \mathbb{N}$[8]. Whenever we write, "let R be an H-graded ring", then it is understood that H is an additive semigroup with identity 0. If we omit H and simply write "let R be a graded ring", then it is understood that R is an $\mathbb{N}$-graded ring.

It is wrong to think of an H-grading of R as a map $|\cdot|: R\backslash\{0\} \to H$ be a map such that

$$|rs| = |r| + |s|$$

whenever $rs \neq 0$. Indeed, usually there are many nonzero elements $r \in R$ where $|r|$ is not defined. What we can say however is that for each $r \in R$ there exists nonzero elements $r_{h_1}, \dots r_{h_n}$, where $r_{h_k} \in R_{h_k}$ for all $1 \leq k \leq n$ and $h_i \neq h_j$ for all $1 \leq i < j \leq n$, such that r can be expressed *uniquely* as

$$r = r_{h_1} + \cdots + r_{h_n}. \tag{225}$$

The qualifier "uniquely" here means that if we have another expression for r, say

$$r = r_{h'_1} + \cdots + r_{h'_{n'}}$$

where $r_{h'_{k'}} \in R_{h'_{k'}} \backslash \{0\}$ for all $1 \leq k' \leq n'$ and $h'_{i'} \neq h'_{j'}$ for all $1 \leq i' < j' \leq n'$, then we must have $n = n'$ and, after reordering if necessary, we must have $r_{h_k} = r_{h'_k}$ for all $1 \leq k \leq n$. We call (225) the **decomposition of r into its homogeneous parts**.

62.1.1 Trivially Graded Ring

Example 62.1. Let R be any ring, then $R_0 := R$ and $R_i := 0$ for all $i > 0$ defines a trivial structure of a graded ring for R. This grading is called the **trivial grading** and we say R is a **trivially graded ring**. Whenever we introduce a ring without specifying any grading, then we assume R is equipped with the trivial grading unless otherwise specified.

62.1.2 A Ring Equipped with Two Gradings

Sometimes we speak of a graded ring as a **ring equipped with an H-grading**. If R is a ring, then it may possible to equip R with two gradings. Here is an example of this:

Example 62.2. Let R be a ring and let $\boldsymbol{x} = x_1, \dots, x_n$ be a list of indeterminates. Then $R[\boldsymbol{x}]$ is both an $\mathbb{N}$-graded ring and an $\mathbb{N}^n$-graded ring. The homogeneous component in degree i in the $\mathbb{N}$-grading is given by

$$R[\boldsymbol{x}]_i = \sum_{|\boldsymbol{\alpha}|=i} R\boldsymbol{x}^{\boldsymbol{\alpha}}.$$

The homogeneous component in degree $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ in the $\mathbb{N}^n$-grading is given by

$$R[\boldsymbol{x}]_{\boldsymbol{\alpha}} = R\boldsymbol{x}^{\boldsymbol{\alpha}}.$$

62.2 Graded R-Modules

Let R be an H-graded ring. An ***H*-graded** R-module M is an R-module together with a direct sum decomposition

$$M = \bigoplus_{h \in H} M_h$$

into abelian groups M_h which satisfies the condition that if $r_{h_1} \in R_{h_1}$ and $u_{h_2} \in M_{h_2}$, then $r_{h_1} u_{h_2} \in M_{h_1+h_2}$ for all $h_1, h_2 \in H$. The u_h are called **homogeneous components** of M and the elements of M_h are called **homogeneous elements** of **degree** h. If u is a homogeneous element in M, then unless otherwise specified, we denote the degree of u by $\deg u$. Whenever we write "let M be an H-graded R-module", then it is assumed that R is an H-graded ring. In the usual case, R will be an $\mathbb{N}$-graded ring and M will be a $\mathbb{Z}$-graded R-module. In this case, we will just say "let M be a graded R-module".

62.2.1 Twist of Graded Module

Definition 62.2. Let M be an H-graded R-module. For each $h \in H$, we define the ***h*th twist of** M, denoted $M(h)$, to be the H-graded R-module whose h'th homogeneous component is given by $M(h)_{h'} := M_{h+h'}$ for all $i \in \mathbb{Z}$.

[8] Our convention is that $\mathbb{N} = \{0, 1, 2, \dots\}$.

62.3 Graded R-Submodules

Lemma 62.1. *Let M be a graded R-module and $N \subset M$ be a submodule. The following conditions are equivalent:*

1. *N is graded R-module whose homogeneous components are $M_i \cap N$.*
2. *N can be generated by homogeneous elements.*

Proof. We first show that 1 implies 2. Let $x \in N$. Since N is graded with homogeneous components $M_i \cap N$, there exists homogeneous elements $x_{i_k} \in M_{i_k} \cap N$ for $1 \leq k \leq n$ such that

$$x = x_{i_1} + \cdots + x_{i_n}.$$

In particular, N can be generated by homogeneous elements.

Now we show that 2 implies 1. Let $\{y_\alpha\}$ be a set of homogeneous generators for N and let $x \in N$. Since $N \subset M$, we can uniquely decompose x as a sum of homogeneous elements, $x = \sum x_i$, where each $x_i \in M$. We need to show that each $x_i \in N$. To do this, note that $x = \sum r_\alpha y_\alpha$ where r_α belongs to R. If we take ith homogeneous components, we find that

$$x_i = \sum (r_\alpha)_{i - \deg y_\alpha} y_\alpha,$$

where $(r_\alpha)_{i-\deg y_\alpha}$ refers to the homogeneous component of r_α concentrated in the degree $i - \deg y_\alpha$. From this it is easy to see that each x_i is a linear combination of the y_α and consequently lies in N. □

Definition 62.3. A submodule $N \subset M$ satisfying the equivalent conditions of Lemma (62.1) is called a **graded submodule**. A graded submodule of a graded ring is called a **homogeneous ideal**.

Example 62.3. Consider the graded ring $R = k[x,y,z]_{(5,6,15)}$. Then the ideal $I = \langle y^5 - z^2, x^3 - z, x^6 - y^5 \rangle$ is a homogeneous ideal in R.

Remark 105. Let R be a graded ring and let I be a homogeneous ideal in R. Then the quotient ring R/I has an induced structure as a graded ring, where the ith homogeneous component of R/I is

$$(R/I)_i := (R_i + I)/I \cong R_i/(I \cap R_i)$$

62.3.1 Criterion for Homogoneous Ideal to be Prime

Proposition 62.2. *Let $\mathfrak{p} \subset R$ be a homogeneous ideal. In order that $\mathfrak{p}$ be prime, it is necessary and sufficient that whenever x, y are homogeneous elements such that $xy \in \mathfrak{p}$, then at least one of $x, y \in \mathfrak{p}$.*

Proof. Necessity is immediate. For sufficiency, suppose $a, b \in R$ and $ab \in \mathfrak{p}$. We must prove that one of these is $\mathfrak{p}$. Write

$$a = a_{i_1} + \cdots + a_{i_m} \quad \text{and} \quad b = b_{j_1} + \cdots + b_{j_n}$$

as a decomposition into homogeneous components where a_{k_m} and a_{k_n} are nonzero and of the highest degree.

We will prove that one of $a, b \in \mathfrak{p}$ by induction on $m + n$. When $m + n = 2$, then it is just the condition of the lemma. Suppose it is true for smaller values of $m + n$. Then ab has highest homogeneous component $a_{i_m} b_{j_n}$, which must be in $\mathfrak{p}$ by homogeneity. Thus one of a_{i_m}, b_{j_n} belongs to $\mathfrak{p}$, say for definiteness it is a_{i_m}. Then we have

$$(a - a_{i_m})b \equiv ab \equiv 0 \bmod \mathfrak{p}$$

so that $(a - a_{i_m})b \in \mathfrak{p}$. But the resolutions of $a - a_{i_m}$ and b have a smaller $m + n$ value: $a - a_{i_m}$ can be expressed with $m - 1$ terms. By the inductive hypothesis, it follows that one of these is in $\mathfrak{p}$, and since $a_{i_m} \in \mathfrak{p}$, we find that one of $a, b \in \mathfrak{p}$. □

62.4 Homomorphisms of Graded R-Modules

Definition 62.4. Let M and N be graded R-modules. A homomorphism $\varphi\colon M \to N$ is called **graded of degree j** if $\varphi(M_i) \subset N_{i+j}$ for all $i \in \mathbb{Z}$. If φ is graded of degree zero then we will simply say φ is **graded**.

Example 62.4. Consider the graded ring $R = k[X, Y, Z, W]$. Then the matrix

$$U := \begin{pmatrix} X + Y + Z & W^2 - X^2 & X^3 \\ 1 & X & XY + Z^2 \end{pmatrix}$$

defines a graded homomorphism $U\colon R(-1) \oplus R(-2) \oplus R(-3) \to R \oplus R(-1)$.

Example 62.5. Let R be a graded ring and let

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}$$

be an $n \times m$ matrix with entries $a_{ij} \in R_{\pi(i,j)}$ where $\pi(i,j) \in \mathbb{N}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. Can we realize $A\colon R^m \to R^n$ as the matrix representation of a graded homomorphism between free R-modules? This answer is no. Indeed, consider the free R-modules F and F' generated by e_1, e_2 and e'_1, e'_2 respectively. Let $\varphi\colon F \to G$ be the unique R-linear map such that

$$\begin{aligned} \varphi(e_1) &= a_{11}e'_1 + a_{21}e'_2 \\ \varphi(e_2) &= a_{12}e'_1 + a_{22}e'_2 \end{aligned}$$

where $a_{11} \in R_1$, $a_{12} \in R_2$, $a_{21} \in R_3$, and $a_{22} \in R_5$. Then φ has matrix representation with respect to these bases as

$$[\varphi] = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

but this is not graded. Indeed, the system of equations

$$\begin{aligned} \varphi(e_1) &= a_{11}e'_1 + a_{21}e'_2 \\ \varphi(e_2) &= a_{12}e'_1 + a_{22}e'_2 \end{aligned}$$

gives us the system of equations

$$\begin{aligned} \deg(e_1) &= 1 + \deg(e'_1) \\ \deg(e_1) &= 2 + \deg(e'_2) \\ \deg(e_2) &= 3 + \deg(e'_1) \\ \deg(e_2) &= 5 + \deg(e'_2), \end{aligned}$$

but not such solution exists.

Definition 62.5. Let R and S be graded rings. A ring homomorphism $\varphi\colon R \to S$ is said to be **graded** if it respects the grading. Thus if $a \in R_i$, then $\varphi(a) \in S_i$.

Example 62.6. Let $\varphi\colon K[x,y,z]_{(1,2,3)} \to K[x,y,z]$ be the unique ring homomorphism map such that $\varphi(x) = x$, $\varphi(y) = y^2$, and $\varphi(z) = z^3$. Then φ is a graded ring isomorphism onto its image $K[x,y^2,z^3]$. Indeed, the inverse $\psi\colon K[x,y^2,z^3] \to K[x,y,z]_{(1,2,3)}$ is the unique ring homomorphism such that $\psi(x) = x$, $\psi(y^2) = y$, and $\psi(z^3) = z$.

62.5 Category of all Graded R-Modules

62.5.1 Products in the Category of Graded R-Modules

Let Λ be a set and let M_λ be a graded R-module for all $\lambda \in \Lambda$. For each $\lambda \in \Lambda$ denote the homogeneous component of M_λ in degree i by $M_{\lambda,i}$. If Λ is finite, then

$$\begin{aligned} \prod_{\lambda \in \Lambda} M_\lambda &= \prod_{\lambda \in \Lambda} \bigoplus_{i \in \mathbb{Z}} M_{\lambda,i} \\ &\cong \bigoplus_{i \in \mathbb{Z}} \prod_{\lambda \in \Lambda} M_{\lambda,i}. \end{aligned}$$

Therefore, if Λ is finite, we may view $\prod_\lambda M_\lambda$ as a graded R-module whose homogeneous component in degree i is $\prod_\lambda M_{\lambda,i}$. On the other hand, if Λ is infinite, then we only have an injective map

$$\bigoplus_{i \in \mathbb{Z}} \prod_{\lambda \in \Lambda} M_{\lambda,i} \to \prod_{\lambda \in \Lambda} \bigoplus_{i \in \mathbb{Z}} M_{\lambda,i}.$$

In particular, $\prod_\lambda M_\lambda$ is not the correct product in $\mathbf{Grad}_R$. The correct product is **graded product**, given by the graded R-module

$$\prod^{\star}_{\lambda \in \Lambda} M_\lambda := \bigoplus_{i \in \mathbb{Z}} \prod_{\lambda \in \Lambda} M_{\lambda,i}$$

together with its projection maps $\pi_\lambda \colon \prod_\lambda^\star M_\lambda \to M_\lambda$ for all $\lambda \in \Lambda$. A homogeneous element of degree i in $\prod_\lambda^\star M_\lambda$ is a sequence of the form $(u_{\lambda,i})_\lambda$ where $u_{\lambda,i} \in M_{\lambda,i}$ for all $\lambda \in \Lambda$. Thus any element in $\prod_\lambda^\star M_\lambda$ can be expressed as a finite sum of the form

$$(u_{\lambda,i_1} + u_{\lambda,i_2} + \cdots + u_{\lambda,i_n})$$

where we often assume without loss of generality that $i_1 < i_2 < \cdots < i_n$.

Let us check that this is in fact the correct product in $\mathbf{Grad}_R$. To show that the pair $(\prod_\lambda^\star M_\lambda, \pi_\lambda)$ is the correct product we have to show it satisfies the universal property: for any other such pair (M, ψ_λ), where M is a graded R-module and $\psi_\lambda \colon M \to M_\lambda$ are graded R-linear maps, there is a unique graded R-linear map $\psi \colon M \to \prod_\lambda^\star M_\lambda$ such that $\pi_\lambda \psi = \psi_\lambda$ for all $\lambda \in \Lambda$. So let (M, ψ_λ) be such a pair. We define $\psi \colon M \to \prod_\lambda^\star M_\lambda$ by

$$\psi(u) = (\psi_\lambda(u))$$

for $u \in M_i$. Clearly ψ is a graded R-linear map since ψ_λ is a graded R-linear map for each $\lambda \in \Lambda$. Moreover, for all $u \in M_i$, we have

$$\begin{aligned}(\pi_\lambda \psi)(u) &= \pi_\lambda(\psi(u)) \\ &= \pi_\lambda((\psi_\lambda(u)) \\ &= \psi_\lambda(u).\end{aligned}$$

This implies $\pi_\lambda \psi = \psi_\lambda$. This establishes existence of ψ. For uniqueness, suppose $\widetilde{\psi} \colon M \to \prod_\lambda^\star M_\lambda$ is another such map. Then for all $u \in M_i$, we have

$$\begin{aligned}\widetilde{\psi}(u) = \psi(u) &\iff \pi_\lambda(\widetilde{\psi}(u)) = \pi_\lambda(\psi(u)) \text{ for all } \lambda \in \Lambda \\ &\iff (\pi_\lambda \widetilde{\psi})(u) = (\pi_\lambda \psi)(u) \text{ for all } \lambda \in \Lambda \\ &\iff \psi_\lambda(u) = \psi_\lambda(u) \text{ for all } \lambda \in \Lambda.\end{aligned}$$

It follows that $\widetilde{\psi} = \psi$.

62.5.2 Inverse Systems and Inverse Limits in the Category Graded R-Modules

Definition 62.6. Let $(\Lambda, \leq)$ be a preordered set (i.e. $\leq$ is reflexive and transitive). An **inverse system** $(M_\lambda, \varphi_{\lambda\mu})$ of graded R-modules and graded R-linear maps over Λ consists of a family of graded R-modules $\{M_\lambda\}$ indexed by Λ and a family of graded R-linear maps $\{\varphi_{\lambda\mu} \colon M_\mu \to M_\lambda\}_{\lambda \leq \mu}$ such that for all $\lambda \leq \mu \leq \kappa$,

$$\varphi_{\lambda\lambda} = 1_{M_\lambda} \quad \text{and} \quad \varphi_{\lambda\kappa} = \varphi_{\lambda\mu}\varphi_{\mu\kappa}.$$

We say the pair (M, ψ_λ) is **compatible** with the inverse system $(M_\lambda, \varphi_{\lambda\mu})$ if

$$\varphi_{\lambda\mu}\psi_\mu = \psi_\lambda$$

for all $\lambda \leq \mu$.

Suppose $(M_\lambda, \varphi_{\lambda\mu})$ and $(M'_\lambda, \varphi'_{\lambda\mu})$ are two direct systems over a partially ordered set $(\Lambda, \leq)$. A **morphism** $\psi \colon (M_\lambda, \varphi_{\lambda\mu}) \to (M'_\lambda, \varphi'_{\lambda\mu})$ of inverse systesms consists of a collection of graded R-linear maps $\psi_\lambda \colon M_\lambda \to M'_\lambda$ indexed by Λ such that for all $\lambda \leq \mu$ we have

$$\varphi'_{\lambda\mu}\psi_\mu = \psi_\lambda\varphi_{\lambda\mu}.$$

Proposition 62.3. *Let $(M_\lambda, \varphi_{\lambda\mu})$ be an inverse system of graded R-modules and graded R-linear maps over a preordered set $(\Lambda, \leq)$. The inverse limit of this system, denoted $\overset{\star}{\varprojlim} M_\lambda$, is (up to unique isomorphism) given by the graded R-module*

$$\overset{\star}{\varprojlim} M_\lambda = \left\{ (u_\lambda) \in \prod_{\lambda \in \Lambda}^{\star} M_\lambda \mid \varphi_{\lambda\mu}(u_\mu) = u_\lambda \textit{ for all } \lambda \leq \mu \right\}$$

together with the projection maps

$$\pi_\lambda \colon \overset{\star}{\varprojlim} M_\lambda \to M_\lambda$$

for all $\lambda \in \Lambda$. In particular, the homogeneous component of degree i in $\overset{\star}{\varprojlim} M_\lambda$ is given by

$$(\overset{\star}{\varprojlim} M_\lambda)_i = \varprojlim M_{\lambda,i}.$$

Remark 106. We put a $\star$ above $\varprojlim$ to remind ourselves that this is the inverse limit in the category of all graded R-modules. In the category of all R-modules, the inverse limit is denoted by $\varprojlim M_\lambda$. If Λ is finite, then $\lim M_\lambda$ already has a natural interpretation of a graded R-module.

Proof. We need to show that $\overset{\star}{\varprojlim} M_\lambda$ satisfies the universal mapping property. Let (M, ψ_λ) be compatible with respect to the invserse system $(M_\lambda, \varphi_{\lambda\mu})$, so $\varphi_{\lambda\mu}\psi_\mu = \psi_\lambda$ for all $\lambda \leq \mu$. By the universal mapping property of the graded product, there exists a unique graded R-linear map $\psi\colon M \to \prod_\Lambda^\star M_\lambda$ such that $\pi_\lambda \psi = \psi_\lambda$ for all $\lambda \in \Lambda$. In fact, this map lands in $\overset{\star}{\varprojlim} M_\lambda$ since

$$\begin{aligned} \varphi_{\lambda\mu}\pi_\mu\psi(u) &= \varphi_{\lambda\mu}\psi_\mu(u) \\ &= \psi_\lambda(u) \\ &= \pi_\lambda\psi(u) \end{aligned}$$

for all $u \in M$. This establishes existence and uniqueness, and thus $\overset{\star}{\varprojlim} M_\lambda$ satisfies the universal mapping property. $\square$

62.5.3 Pullbacks in the Category of Graded R-Modules

Here is an interesting example of a limit in the case where Λ is finite. Let $\psi\colon N \to M$ and $\varphi\colon P \to M$ be graded R-linear maps. The **pullback of** $\psi\colon N \to M$ **and** $\varphi\colon P \twoheadrightarrow M$ is defined to be graded R-module

$$N \times_M P = \{(u, v) \in N \times P \mid \psi(u) = \varphi(v)\}$$

endowed with the projection maps

$$\pi_1\colon N \times_M P \to N \quad \text{and} \quad \pi_2\colon N \times_M P \to P.$$

One can check that the pullback satisfies the universal mapping property of the system

$$\begin{tikzcd} & P \arrow[d, "\varphi"] \\ N \arrow[r, "\psi"'] & M \end{tikzcd}$$

Thus there exists a *unique* isomorphism from $N \times_M P$ to the limit of this system which makes everything commute.

62.5.4 Pullbacks Preserves Surjective Maps

Proposition 62.4. *Let $\varphi_{13}\colon M_3 \to M_1$ and $\varphi_{12}\colon M_2 \to M_1$ be graded R-linear maps. Consider their pullback*

$$\begin{tikzcd} M_3 \times_{M_1} M_2 \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & M_2 \arrow[d, "\varphi_{12}"] \\ M_3 \arrow[r, "\varphi_{13}"'] & M_1 \end{tikzcd}$$

1. *If both φ_{12} and φ_{13} are injective, then both π_1 and π_2 are injective.*
2. *If φ_{12} is surjective, then π_1 is surjective. Similarly, if φ_{13} is surjective, then π_2 is surjective.*

Proof. 1. Suppose both φ_{12} and φ_{13} are injective. We want to show that π_1 is injective. Let $(u_3, u_2) \in \ker \pi_1$. So $(u_3, u_2) \in M_3 \times_{M_1} M_2$, which means $\varphi_{13}(u_3) = \varphi_{12}(u_2)$, and $\pi_1(u_3, u_2) = 0$, which means $u_3 = 0$. Thus

$$\begin{aligned} \varphi_{12}(u_2) &= \varphi_{13}(u_3) \\ &= \varphi_{13}(0) \\ &= 0. \end{aligned}$$

Since φ_{12} is injective, this implies $u_2 = 0$, which implies $\varphi_{13}(u_3) = 0$. Since φ_{12} is injective, this implies $u_3 = 0$.

2. Suppose φ_{12} is surjective. We want to show that π_1 is surjective. Let $u_3 \in M_3$. Using the fact that φ_{12} is surjective, we choose a lift of $\varphi_{13}(u_3)$ with respect to φ_{12}, say $u_2 \in M_2$. So $\varphi_{12}(u_2) = \varphi_{13}(u_3)$, but this means $(u_3, u_2) \in M_3 \times_{M_1} M_2$, which implies π_1 is surjective since $\pi_1(u_3, u_2) = u_3$. The proof that φ_{13} surjective implies π_2 surjective follows in a similar manner.

$\square$

62.5.5 Coproducts in the Category of Graded R-Modules

Let Λ be a set and let M_λ be a graded R-module for all $\lambda \in \Lambda$. For each $\lambda \in \Lambda$ denote the homogeneous component of M_λ in degree i by $M_{\lambda,i}$. Then observe that

$$\begin{aligned}\bigoplus_{\lambda\in\Lambda} M_\lambda &= \bigoplus_{\lambda\in\Lambda}\bigoplus_{i\in\mathbb{Z}} M_{\lambda,i} \\ &\cong \bigoplus_{i\in\mathbb{Z}}\bigoplus_{\lambda\in\Lambda} M_{\lambda,i}.\end{aligned}$$

Therefore $\bigoplus_\lambda M_\lambda$ has a natural interpretation as a graded R-module with the homogeneous component in degree i being given by $\bigoplus_\lambda M_{\lambda,i}$. One can check that $\bigoplus_\lambda M_\lambda$ together with the inclusion maps $\iota_\lambda \colon M_\lambda \to \bigoplus_\lambda M_\lambda$ is the correct coproduct in $\mathbf{Grad}_R$.

62.5.6 Direct Systems and Direct Limits in the Category of Graded R-Modules

Definition 62.7. A directed set $(\Lambda, \leq)$ is a nonempty set Λ equipped with a binary relation $\leq$ on Λ such that

1. $\leq$ is a preorder, meaning
   (a) it is reflexive: $\lambda \leq \mu$ and $\mu \leq \lambda$ implies $\lambda = \mu$ for all $\lambda, \mu \in \Lambda$.
   (b) it is transitive: if $\lambda \leq \mu$ and $\mu \leq \kappa$, then $\lambda \leq \kappa$ for all $\lambda, \mu, \kappa, \in \Lambda$.
2. $\leq$ is directed, meaning for all $\lambda, \mu \in \Lambda$, there exists $\kappa \in \Lambda$ such that $\lambda \leq \kappa$ and $\mu \leq \kappa$.

Definition 62.8. Let $(\Lambda, \leq)$ be a preordered set (i.e. $\leq$ is reflexive and transitive). A **direct system** $(M_\lambda, \varphi_{\lambda\mu})$ of graded R-modules and graded R-linear maps over Λ consists of a family of graded R-modules $\{M_\lambda\}$ indexed by Λ and a family of graded R-linear maps $\{\varphi_{\lambda\mu} \colon M_\lambda \to M_\mu\}_{\lambda\leq\mu}$ such that for all $\lambda \leq \mu \leq \kappa$,

$$\varphi_{\lambda\lambda} = 1_{M_\lambda} \quad \text{and} \quad \varphi_{\lambda\kappa} = \varphi_{\mu\kappa}\varphi_{\lambda\mu}.$$

If $(\Lambda, \leq)$ is also directed set, then we say $(M_\lambda, \varphi_{\lambda\mu})$ is a **directed system**. If M is an R-module and $\{\psi_\lambda \colon M_\lambda \to M\}$ is a collection of R-linear maps indexed over Λ, then we say the pair (M, ψ_λ) is **compatible** with the direct system $(M_\lambda, \varphi_{\lambda\mu})$ if

$$\psi_\mu\varphi_{\lambda\mu} = \psi_\lambda$$

for all $\lambda \leq \mu$. The **direct limit** (or the **colimit)** of the direct system $(M_\lambda, \varphi_{\lambda\mu})$ is the pair $(\varinjlim M_\lambda, \bar{\iota}_\lambda)$ which is universally compatible with the direct system $(M_\lambda, \varphi_{\lambda\mu})$ in the following sense: for all pairs (M, ψ_λ) which are compatible with the direct system $(M_\lambda, \varphi_{\lambda\mu})$, there exists a unique graded R-linear map $\psi\colon \varinjlim M_\lambda \to M_\lambda$ such that

$$\psi\bar{\iota}_\lambda = \psi_\lambda$$

for all $\lambda \in \Lambda$. This universal mapping property characterizes $(\varinjlim M_\lambda, \bar{\iota}_\lambda)$ up to a unique isomorphism. Often we denote the colimit by $\varinjlim M_\lambda$ instead of $(\varinjlim M_\lambda, \bar{\iota}_\lambda)$.

Proposition 62.5. *Let $(M_\lambda, \varphi_{\lambda\mu})$ be a direct system of graded R-modules and graded R-linear maps over a preordered set $(\Lambda, \leq)$. The **direct limit** of this system, denoted $\varinjlim M_\lambda$, is (up to unique isomorphism) given by the graded R-module*

$$\varinjlim M_\lambda := \bigoplus_{\lambda\in\Lambda} M_\lambda / \langle\{(\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_\lambda) \mid u_\lambda \in M_\lambda \text{ and } \lambda \leq \mu\}\rangle$$

together with the inclusion maps

$$\bar{\iota}_\lambda \colon M_\lambda \to \varinjlim M_\lambda$$

for all $\lambda \in \Lambda$, where $\bar{\iota}_\lambda$ is the composite of the inclusion map $\iota_\lambda \colon M_\lambda \to \bigoplus_{\lambda\in\Lambda} M_\lambda$ together with the quotient map $\bigoplus_{\lambda\in\Lambda} M_\lambda \to \varinjlim M_\lambda$. The homogeneous component of degree $i \in \mathbb{Z}$ of $\varinjlim M_\lambda$ is given by

$$(\varinjlim M_\lambda)_i = \varinjlim M_{\lambda,i}.$$

Proof. First observe that the submodule

$$\langle\{(\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_\lambda) \mid u_\lambda \in M_\lambda \text{ and } \lambda \leq \mu\}\rangle$$

of $\bigoplus_\lambda M_\lambda$ is generated by homogeneous elements. Indeed, for any $(\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_\lambda)$, we express u_λ into its homogeneous parts, say

$$u_\lambda = u_{\lambda,i_1} + \cdots + u_{\lambda,i_n},$$

then since $\iota_\lambda - \iota_\mu \varphi_{\lambda\mu}$ is a graded R-linear map, we have

$$\begin{aligned}(\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_\lambda) &= (\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_{\lambda,i_1} + \cdots + u_{\lambda,i_n}) \\ &= (\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_{\lambda,i_1}) + (\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_{\lambda,i_n}),\end{aligned}$$

where each $(\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_{\lambda,i_m})$ is homogeneous. Thus any such $(\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_\lambda)$ can be expressed as a sum of finitely many homogeneous terms. It follows that $\varinjlim M_\lambda$ has a natural graded R-module structure.

We need to show that $\varinjlim M_\lambda$ satisfies the universal mapping property. Let (M, ψ_λ) be compatible with respect to the direct system $(M_\lambda, \varphi_{\lambda\mu})$, so $\psi_\mu\varphi_{\lambda\mu} = \psi_\lambda$ for all $\lambda \leq \mu$. By the universal mapping property of the coproduct, there exists a unique graded R-linear map $\psi \colon \bigoplus_\lambda M_\lambda \to M$ such that $\psi\iota_\lambda = \psi_\lambda$ for all $\lambda \in \Lambda$. In fact, since

$$\begin{aligned}\psi(\iota_\lambda - \iota_\mu\varphi_{\lambda\mu})(u_\lambda) &= \psi\iota_\lambda(u_\lambda) - \psi\iota_\mu\varphi_{\lambda\mu}(u_\lambda) \\ &= \psi_\lambda(u_\lambda) - \psi_\mu\varphi_{\lambda\mu}(u_\lambda) \\ &= \psi_\lambda(u_\lambda) - \psi_\lambda(u_\lambda) \\ &= 0\end{aligned}$$

for all $u_\lambda \in M_\lambda$ and $\lambda \in \Lambda$, the universal mapping property of quotients implies there exists a unique graded R-linear map $\overline{\psi} \colon \varinjlim M_\lambda \to M$ such that

$$\overline{\psi}\overline{\iota}_\lambda = \psi\iota_\lambda = \psi_\lambda.$$

This shows that $\varinjlim M_\lambda$ satisfies the universal mapping property. □

To simplify notation, we often write $\overline{u}_\lambda$ instead of $\overline{\iota}(u_\lambda)$ whenever $u_\lambda \in M_\lambda$.

Suppose $(M_\lambda, \varphi_{\lambda\mu})$ and $(M'_\lambda, \varphi'_{\lambda\mu})$ are two direct systems over a partially ordered set $(\Lambda, \leq)$. A **morphism** $\psi \colon (M_\lambda, \varphi_{\lambda\mu}) \to (M'_\lambda, \varphi'_{\lambda\mu})$ of direct systems consists of a collection of graded R-linear maps $\psi_\lambda \colon M_\lambda \to M'_\lambda$ indexed by Λ such that for all $\lambda \leq \mu$ we have

$$\varphi'_{\lambda\mu}\psi_\lambda = \psi_\mu\varphi_{\lambda\mu}.$$

The morphism ψ induces a graded R-linear map $\varinjlim \psi_\lambda \colon \varinjlim M_\lambda \to \varinjlim M'_\lambda$ uniquely determined by

$$\varinjlim \psi_\lambda(\overline{u}_\lambda) = \overline{\psi_\lambda(u_\lambda)}$$

for all $u_\lambda \in M_\lambda$ for all $\lambda \in \Lambda$.

Proposition 62.6. *Let $(M_\lambda, \varphi_{\lambda\mu})$ be a directed system of graded R-modules and graded R-linear maps over a directed set $(\Lambda, \leq)$.*

1. *Each element of $\varinjlim M_\lambda$ has the form $\overline{u}_\lambda$ for some $u_\lambda \in M_\lambda$.*
2. *$\overline{u}_\lambda = 0$ if and only if $\varphi_{\lambda\mu}(u_\lambda) = 0$ for some $\lambda \leq \mu$.*

Proof. 1. An element in $\varinjlim M_\lambda$ has the form $\sum_{i=1}^n \overline{u}_{\lambda_i}$ where $\lambda_1, \dots, \lambda_n \in \Lambda$ and $u_{\lambda_i} \in M_{\lambda_i}$ for all $1 \leq i \leq n$. Since Λ is directed, there exists a $\lambda \in \Lambda$ such that $\lambda_i \leq \lambda$ for all $1 \leq i \leq n$. Then we have

$$\begin{aligned}\sum_{i=1}^n \overline{u}_{\lambda_i} &= \sum_{i=1}^n \overline{\varphi_{\lambda_i,\lambda}(u_{\lambda_i})} \\ &= \overline{\sum_{i=1}^n \varphi_{\lambda_i,\lambda}(u_{\lambda_i})} \\ &= \overline{u}_\lambda,\end{aligned}$$

where $\overline{u}_\lambda = \sum_{i=1}^n \varphi_{\lambda_i,\lambda}(u_{\lambda_i})$. Each $\varphi_{\lambda_i,\lambda}(u_{\lambda_i})$ lands in M_λ, so $u_\lambda \in M_\lambda$.

2. If $\varphi_{\lambda\mu}(u_\lambda) = 0$ for some $\lambda \leq \mu$, then $\overline{u}_\lambda = \overline{\varphi_{\lambda\mu}(u_\lambda)} = 0$. Conversely, suppose $\overline{u}_\lambda = 0$. Then we have

$$\iota_\lambda(u_\lambda) = \sum_{i=1}^n \iota_{\lambda_i}(u_{\lambda_i}) - \sum_{i=1}^n \iota_{\mu_i}\varphi_{\lambda_i,\mu_i}(u_{\lambda_i}) \tag{226}$$

for some $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in \Lambda$ and $u_{\lambda_i} \in M_{\lambda_i}$ for all $1 \leq i \leq n$, where we may assume that $\lambda_i \neq \mu_i$ since otherwise we have $\iota_{\lambda_i} - \iota_{\mu_i}\varphi_{\lambda_i,\mu_i} = 0$. Since $u_\lambda \in M_\lambda$, we may assume that $u_{\lambda_i} \in M_\lambda$ for each $1 \leq i \leq n$. In particular, this implies

$$u_\lambda = \sum_{i=1}^n u_{\lambda_i} \quad \text{and} \quad \sum_{i=1}^n \varphi_{\lambda,\mu_i}(u_{\lambda_i}) = 0.$$

Now if $\mu_i = \mu = \mu_j$ for each $1 \le i, j \le n$, then clearly we have

$$\begin{aligned}
\varphi_{\lambda,\mu}(u_\lambda) &= \varphi_{\lambda,\mu}\left(\sum_{i=1}^{n} u_{\lambda_i}\right) \\
&= \sum_{i=1}^{n} \varphi_{\lambda,\mu}(u_{\lambda_i}) \\
&= 0.
\end{aligned}$$

Otherwise, choose $\mu \in \Lambda$ such that $\mu_i \le \mu$ for all $1 \le i \le n$. Then it's easy to see that we still have $\varphi_{\lambda,\mu}(u_\lambda) = 0$. □

62.5.7 Taking Directed Limits is an Exact Functor

Proposition 62.7. *Let*

$$0 \longrightarrow (M_\lambda, \varphi_\lambda) \xrightarrow{\psi} (M'_\lambda, \varphi'_\lambda) \xrightarrow{\psi'} (M''_\lambda, \varphi''_\lambda) \longrightarrow 0$$

be a short exact sequence of directed systems of graded R-modules and graded R-linear maps. Then

$$0 \longrightarrow \varinjlim M_\lambda \xrightarrow{\varinjlim \psi_\lambda} \varinjlim M'_\lambda \xrightarrow{\varinjlim \psi'_\lambda} \varinjlim M_\lambda \longrightarrow 0$$

is a short exact sequence of graded R-modules and graded R-linear maps.

Proof. We first show $\varinjlim \psi_\lambda$ is injective. Let $\overline{u}_\lambda \in \varinjlim M_\lambda$ and suppose $\overline{\psi_\lambda u_\lambda} = 0$. Then there exists $\mu \ge \lambda$ such that

$$\begin{aligned}
0 &= \varphi'_{\lambda\mu}\psi_\lambda u_\lambda \\
&= \psi_\mu \varphi_{\lambda\mu} u_\lambda.
\end{aligned}$$

Since ψ_λ is injective, we have $\varphi_{\lambda\mu}u_\lambda = 0$, which implies $\overline{u}_\lambda = 0$. So $\varinjlim \psi_\lambda$ is injective.

Next we show exactness at $\varinjlim M'_\lambda$. Let $\overline{u'}_\lambda \in \varinjlim M'_\lambda$ and suppose $\overline{\psi'_\lambda u'_\lambda} = 0$. Then there exists $\mu \ge \lambda$ such that

$$\begin{aligned}
0 &= \varphi''_{\lambda\mu}\psi'_\lambda u'_\lambda \\
&= \psi'_\mu \varphi'_{\lambda\mu} u'_\lambda.
\end{aligned}$$

This implies $\varphi'_{\lambda\mu}u'_\lambda = \psi_\mu u_\mu$ for some $u_\mu \in M_\mu$, by exactness at $(M'_\lambda, \varphi'_\lambda)$. Thus

$$\begin{aligned}
\overline{u'_\lambda} &= \overline{\varphi'_{\lambda\mu}u'_\lambda} \\
&= \overline{\psi_\mu u_\mu}.
\end{aligned}$$

This implies exactness at $\varinjlim M'_\lambda$. Exactness at $\varinjlim M''_\lambda$ is easy and is left as an exercise. □

62.5.8 Contravariant Hom Converts Direct Limits to Inverse Limits

Proposition 62.8. *Let $(M_\lambda, \varphi_{\lambda\mu})$ be a direct system of graded R-linear module. Then there exists an isomorphism*

62.5.9 Tensor Products

Let M and N be graded R-modules. As R-modules, their tensor product is given by

$$\begin{aligned}
M \otimes_R N &= \left(\bigoplus_{i\in\mathbb{Z}} M_i\right) \otimes \left(\bigoplus_{j\in\mathbb{Z}} N_j\right) \\
&\cong \bigoplus_{i\in\mathbb{Z}}\bigoplus_{j\in\mathbb{Z}} (M_i \otimes N_j) \\
&= \bigoplus_{i\in\mathbb{Z}} \left(\bigoplus_{j\in\mathbb{Z}} M_j \otimes N_{i-j}\right).
\end{aligned}$$

In particular, $M \otimes_R N$ has a natural interpretation as a graded R-module with the homogeneous component in degree i given by

$$(M \otimes_R N)_i = \bigoplus_{j \in \mathbb{Z}} M_j \otimes N_{i-j}.$$

Indeed, if $x \in M_i$, $y \in N_j$, and $a \in R_k$, then

$$a(x \otimes y) = ax \otimes y = x \otimes ay \in (M \otimes_R N)_{i+j+k}.$$

So the grading is preserved upon R-scaling.

62.5.10 Graded Hom

Unlike the case of tensor products, hom does not have a natural interpretation as a graded R-module Instead we consider the graded version of hom: let M and N be graded R-modules. Their **graded hom**, denoted $\mathrm{Hom}_R^\star(M, N)$, is the graded R-module whose homogeneous component in degree i is

$$\mathrm{Hom}_R^\star(M, N)_i = \{\text{graded homomorphisms } \alpha\colon M \to N \text{ of degree } i\}.$$

Observe that we have a natural inclusion of R-modules

$$\mathrm{Hom}_R^\star(M, N) \subseteq \mathrm{Hom}_R(M, N).$$

In particular, many properties which $\mathrm{Hom}_R(M, N)$ satisfies are inherited by $\mathrm{Hom}_R^\star(M, N)$.

62.5.11 Graded Hom Properties

Proposition 62.9. *Let M be a graded R-module, let Λ be a set, and let N_λ be a graded R-module for each $\lambda \in \Lambda$. Then we have natural isomorphisms*

$$\mathrm{Hom}_R^\star\left(M, \prod_{\lambda\in\Lambda}^{\star} N_\lambda\right) \cong \prod_{\lambda\in\Lambda}^{\star} \mathrm{Hom}_R^\star(M, N_\lambda) \quad \textit{and} \quad \mathrm{Hom}_R^\star\left(\bigoplus_{\lambda\in\Lambda} M_\lambda, -\right) \cong \prod_{\lambda\in\Lambda}^{\star} \mathrm{Hom}_R^\star(M_\lambda, -)$$

Proof. Let $i \in \mathbb{Z}$. Define a map $\Psi\colon \mathrm{Hom}_R^\star\left(M, \prod_{\lambda\in\Lambda} N^\lambda\right)_i \to \prod_{\lambda\in\Lambda} \mathrm{Hom}_R^\star\left(M, N^\lambda\right)_i$ by

$$\Psi(\varphi) = (\pi_\lambda \varphi)_{\lambda\in\Lambda}$$

for all $\varphi \in \mathrm{Hom}_R^\star\left(M, \prod_{\lambda\in\Lambda} N^\lambda\right)_i$, where $\pi_\lambda\colon \prod_{\lambda\in\Lambda} N^\lambda \to N^\lambda$ is the projection to the λth coordinate. We claim that Ψ is a graded isomorphism.

We first check that it is R-linear. Let $a, b \in R$ and $\varphi, \psi \in \mathrm{Hom}_R\left(M, \prod_{i\in I} N_i\right)$. Then

$$\begin{aligned}
\Psi(a\varphi + b\psi) &= (\pi_i \circ (a\varphi + b\psi)) \\
&= (a(\pi_i \circ \varphi) + b(\pi_i \circ \psi)) \\
&= a(\pi_i \circ \varphi) + b(\pi_i \circ \psi) \\
&= a\Psi(\varphi) + b\Psi(\psi).
\end{aligned}$$

Thus Ψ is R-linear. To show that Ψ is an isomorphism, we construct its inverse. Let $(\varphi_i) \in \prod_{i\in I} \mathrm{Hom}_R(M, N_i)$. Define $\Phi((\varphi_i))\colon M \to \prod_{i\in I} N_i$ by

$$\Phi((\varphi_i))(x) := (\varphi_i(x))$$

for all $x \in M$. Then clearly Φ and Ψ are inverse to each other. Indeed, let $\varphi \in \mathrm{Hom}_R\left(M, \prod_{i\in I} N_i\right)$. Then

$$\begin{aligned}
\Phi(\Psi(\varphi))(x) &= \Phi((\pi_i \circ \varphi))(x) \\
&= ((\pi_i \circ \varphi)(x)) \\
&= \varphi(x)
\end{aligned}$$

for all $x \in M$. Thus $\Phi(\Psi(\varphi)) = \varphi$. Conversely, let $(\varphi_i) \in \prod_{i\in I} \mathrm{Hom}_R(M, N_i)$. Then

$$\begin{aligned}
\Psi(\Phi(\varphi_i)) &= (\pi_i \circ \Phi(\varphi_i)) \\
&= (\pi_i \circ \varphi)) \\
&= \varphi(x)
\end{aligned}$$

Finally, note that Ψ is graded since π_λ is graded of degree 0 for all $\lambda \in \Lambda$. $\square$

In fact we can generalize the above proposition as follows:

Proposition 62.10. *Let $(\Lambda, \leq)$ be a preordered set, let $(M_\lambda, \phi_{\lambda\mu})$ be a direct system of graded R-modules and graded R-linear maps over Λ and let $(N_\lambda, \varphi_{\lambda\mu})$ be an inverse system of graded R-modules and graded R-linear maps over Λ. Then we have natural isomorphisms*

$$\mathrm{Hom}^\star_R(M, \overset{\star}{\varprojlim} N_\lambda) \cong \overset{\star}{\varprojlim} \mathrm{Hom}^\star_R(M, N_\lambda) \quad \text{and} \quad \mathrm{Hom}^\star_R(\overset{\star}{\varprojlim} M_\lambda, N) \cong \varinjlim \mathrm{Hom}^\star_R(M_\lambda, N)$$

Proof. Let $i \in \mathbb{Z}$. Define a map $\Psi \colon \mathrm{Hom}^\star_R(M, \overset{\star}{\varprojlim} N_\lambda)_i \to \overset{\star}{\varprojlim} \mathrm{Hom}^\star_R(M, N_\lambda)_i$ by

$$\Psi(\varphi) = (\pi_\lambda \varphi)$$

for all $\varphi \in \mathrm{Hom}^\star_R(M, \overset{\star}{\varprojlim} N_\lambda)_i$, where π_λ is the projection to the λth coordinate. Observe that Ψ lands in $\overset{\star}{\varprojlim} \mathrm{Hom}^\star_R(M, N_\lambda)_i$ since $\pi_\mu \varphi = \varphi_{\lambda\mu} \pi_\lambda \varphi$ for all $\lambda \leq \mu$. We claim that Ψ is a graded isomorphism.

We first check that it is R-linear. Let $a, b \in R$ and $\varphi, \psi \in \mathrm{Hom}_R\left(M, \prod_{i \in I} N_i\right)$. Then

$$\begin{aligned}
\Psi(a\varphi + b\psi) &= (\pi_i \circ (a\varphi + b\psi)) \\
&= (a(\pi_i \circ \varphi) + b(\pi_i \circ \psi)) \\
&= a(\pi_i \circ \varphi) + b(\pi_i \circ \psi) \\
&= a\Psi(\varphi) + b\Psi(\psi).
\end{aligned}$$

Thus Ψ is R-linear. To show that Ψ is an isomorphism, we construct its inverse. Let $(\varphi_i) \in \prod_{i \in I} \mathrm{Hom}_R(M, N_i)$. Define $\Phi((\varphi_i)) \colon M \to \prod_{i \in I} N_i$ by

$$\Phi((\varphi_i))(x) := (\varphi_i(x))$$

for all $x \in M$. Then clearly Φ and Ψ are inverse to each other. Indeed, let $\varphi \in \mathrm{Hom}_R\left(M, \prod_{i \in I} N_i\right)$. Then

$$\begin{aligned}
\Phi(\Psi(\varphi))(x) &= \Phi((\pi_i \circ \varphi))(x) \\
&= ((\pi_i \circ \varphi)(x)) \\
&= \varphi(x)
\end{aligned}$$

for all $x \in M$. Thus $\Phi(\Psi(\varphi)) = \varphi$. Conversely, let $(\varphi_i) \in \prod_{i \in I} \mathrm{Hom}_R(M, N_i)$. Then

$$\begin{aligned}
\Psi(\Phi(\varphi_i)) &= (\pi_i \circ \Phi(\varphi_i)) \\
&= (\pi_i \circ \varphi)) \\
&= \varphi(x)
\end{aligned}$$

Finally, note that Ψ is graded since π_λ is graded of degree 0 for all $\lambda \in \Lambda$. $\square$

62.5.12 Left Exactness of $\mathrm{Hom}^\star_R(M, -)$ and $\mathrm{Hom}^\star_R(-, N)$

Let M and N be graded R-modules. Recall that both $\mathrm{Hom}_R(M, -)$ and $\mathrm{Hom}_R(-, N)$ are left exact functors from the category of R-modules to itself. The graded version of these functors are

$$\mathrm{Hom}^\star_R(M, -) \colon \mathrm{Grad}_R \to \mathrm{Grad}_R \quad \text{and} \quad \mathrm{Hom}^\star_R(-, N) \colon \mathrm{Grad}_R \to \mathrm{Grad}_R.$$

We want to check that they are also left exact functors. Let's focus on $\mathrm{Hom}^\star_R(-, N)$ first:

Proposition 62.11. *The sequence of graded R-modules and graded homomorphisms*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0 \tag{227}$$

is exact if and only if for all R-modules N the induced sequence

$$0 \longrightarrow \mathrm{Hom}^\star_R(M_3, N) \xrightarrow{\varphi_2^*} \mathrm{Hom}^\star_R(M_2, N) \xrightarrow{\varphi_1^*} \mathrm{Hom}^\star_R(M_1, N) \tag{228}$$

is exact.

Proof. Suppose that (320) is exact and let N be any R-module. Exactness at $\mathrm{Hom}^\star_R(M_3, N)$ follows from the fact that φ_2^* is injective (which follows from the fact that $\mathrm{Hom}_R(-, N)$ is left exact). Next we show exactness at $\mathrm{Hom}^\star_R(M_2, N)$. Let $\psi_2 \colon M_2 \to N$ be a graded homomorphism of degree i such that $\psi_2 \varphi_1 = 0$. By left exactness of $\mathrm{Hom}_R(-, N)$, there exists a $\psi_3 \in \mathrm{Hom}_R(M, N)$ such that $\psi_2 = \psi_3 \varphi_2$. Since φ_2 is surjective, ψ_3 is graded of degree i. Thus $\psi_3 \in \mathrm{Hom}^\star_R(M, N)$. Thus we have exactness at $\mathrm{Hom}^\star_R(M_2, N)$. $\square$

62.5.13 Projective Objects and Injective Objects in $\mathbf{Grad}_R$

$\mathrm{Hom}^\star_R(\bigoplus_\lambda P_\lambda, B) \cong \prod_\lambda \mathrm{Hom}^\star_R(P_\lambda, B)$ and $\mathrm{Hom}^\star_R(A, \prod^\star_\lambda E_\lambda) \cong \prod^\star_\lambda \mathrm{Hom}^\star_R(A, E_\lambda)$.

62.6 Noetherian Graded Rings and Modules

62.6.1 The Irrelevant Ideal

Definition 62.9. Let R be a graded ring. The **irrelevant ideal of** R is defined to be

$$R_+ := \bigoplus_{i>0} R_i.$$

It is straightforward to check that R_+ is in fact an ideal of R and that $R/R_+ \cong R_0$.

62.6.2 Noetherian Graded Rings

The following lemma will be used many times without mention.

Lemma 62.2. *Let R be a ring and let $S \subseteq R$. Suppose the ideal $\langle S \rangle$ generated by S is finitely generated. Then we can choose the generators to be in S.*

Proof. Since $\langle S \rangle$ is finitely generated, there are $x_1, \dots, x_n \in \langle S \rangle$ such that $\langle S \rangle = \langle x_1, \dots, x_n \rangle$. In particular we have

$$x_i = \sum_{j=1}^{n_i} r_{ji} s_{ji}$$

where for each $1 \leq i \leq n$ we have $n_i \in \mathbb{N}$, and for each $1 \leq j \leq n_i$ we have $r_{ji} \in R$ and $s_{ji} \in S$. In particular, this means

$$\langle S \rangle = \langle s_{ji} \mid 1 \leq i \leq n \text{ and } 1 \leq j \leq n_i \rangle.$$

□

Definition 62.10. A **Noetherian** graded ring is a graded ring whose underlying ring is Noetherian.

Proposition 62.12. *Let R be a graded ring. Suppose $R_+ = \langle \{x_\lambda\}_{\lambda \in \Lambda} \rangle$. Then the R_0-algebra map*

$$\varphi \colon R_0[\{X_\lambda\}] \to R$$

given by $\varphi(X_\lambda) = x_\lambda$ for all $\lambda \in \Lambda$ is surjective. In other words, if a subset $S \subset R_+$ generates the irrelevant ideal R_+ as an R-ideal, then it generates R as an R_0-algebra.

Proof. It suffices to show that $R_k \subset \operatorname{im} \varphi$ for all $k \in \mathbb{N}$. We prove this by induction on k. The base case $k = 0$ is trivial. Now suppose it is true for all $i < k$ for some $k > 0$ and let $a \in R_k$. Since $R = R_0 \oplus R_+$, we have a unique decomposition

$$a = a_0 + x$$

where $a_0 \in R_0$ and $x \in R_+$. Since $R_+ = \langle \{x_\lambda\} \rangle$ and $x \in R_+$, there exists $x_{\lambda_1}, \dots, x_{\lambda_n} \in \{x_\lambda\}$ and $a_m \in R_{k - \deg x_{\lambda_m}}$ for all $1 \leq m \leq n$ such that

$$x = a_1 x_{\lambda_1} + \cdots + a_n x_{\lambda_n}.$$

Choose $A_m \in R_0[\{X_\lambda\}]$ such that $\varphi(A_m) = a_m$ for all $0 \leq m \leq n$ (we can do this by induction). Then

$$\begin{aligned} a &= a_0 + a_1 x_{\lambda_1} + \cdots + a_n x_{\lambda_n} \\ &= \varphi(A_0) + \varphi(A_1)\varphi(X_{\lambda_1}) + \cdots + \varphi(A_n)\varphi(X_{\lambda_n}) \\ &= \varphi(A_0 + A_1 X_{\lambda_1} + \cdots + A_n X_{\lambda_n}). \end{aligned}$$

This implies $R_k \subset \operatorname{im} \varphi$. Therefore φ is surjective. □

Proposition 62.13. *Let R be a graded ring. Then R is Noetherian if and only if R_0 is Noetherian and R is finitely-generated as an R_0-algebra.*

Proof. Suppose R_0 is Noetherian and R is finitely-generated as an R_0-algebra. Then there exists an $n \geq 0$ and a surjection

$$R_0[X_1, \dots, X_n] \to R.$$

where $R_0[X_1, \dots, X_n]$ is a polynomial algebra over Noetherian ring, and hence Noetherian, which implies that R is Noetherian, as it is a quotient of a Noetherian ring.

Now suppose R is Noetherian. Since $R_0 \cong R/R_+$, we see that R_0 must be Noetherian since it is the quotient of a Noetherian ring. Since R is Noetherian, the irrelevant ideal R_+ is finitely-generated, say by $x_1, \ldots, x_n \in R_+$. Since R is graded, we have a surjective R_0-algebra map

$$R_0[X_1, \ldots, X_n] \to R$$

sending $X_i \mapsto x_i$ for all $1 \leq i \leq n$. It follows that R is a finitely-generated R_0-algebra. $\square$

62.7 Localization of Graded Rings

Definition 62.11. If $S \subset R$ is a multiplicative subset of a graded ring R consisting of homogeneous elements, then $S^{-1}R$ is a $\mathbb{Z}$-graded ring: we let the homogeneous elements of degree n be of the form r/s where $r \in R_{n+\deg s}$. We write $R_{(S)}$ for the subring of elements of degree zero; there is thus a map $R_0 \to R_{(S)}$.

If S consists of the powers of a homogeneous element f, we write $R_{(f)}$ for R_S. If $\mathfrak{p}$ is a homogeneous ideal and S is the set of homogeneous elements of R not in $\mathfrak{p}$, we write $R_{(\mathfrak{p})}$ for $R_{(S)}$.

More generally if M is a graded R-module, then we define $M_{(S)}$ to be the submodule of $S^{-1}M$ consisting of elements of degree zero. When S consists of powers of a homogeneous element $f \in R$, then we write $M_{(f)}$ instead of $M_{(S)}$. We similarly define $M_{(\mathfrak{p})}$ for a homogeneous prime ideal $\mathfrak{p}$.

62.8 Graded R-Algebras

An R-algebra A is an R-module equipped with an R-linear map $A \otimes_R A \to A$, denoted $a \otimes b \mapsto ab$. This means that for all $r \in R$ and $a, b \in A$, we have

$$r(ab) = (ra)b = a(rb),$$

and for all $a, b, c \in A$, we have

$$(a+b)c = ab + ac \quad \text{and} \quad a(b+c) = ab + ac.$$

We say the R-algebra is **associative** when for all $a, b, c \in A$, we have

$$(ab)c = a(bc).$$

We say the R-algebra is **unital** when there exists an element $e \in A$ such that for all $a \in A$, we have

$$ae = a = ea.$$

Unless otherwise specified, all R-algebras discussed are assumed to be associative and unital, so they are genuinely rings (perhaps not commutative) and being an R-algebra just means they have a little extra structure related to scaling by R. If A is an R-algebra, then can view R as sitting inside A via the map $\varphi \colon R \to A$, given by

$$\varphi(r) = 1 \cdot r$$

for all $r \in R$, though this map need not be injective.

Definition 62.12. An H-**graded** R-**algebra** A is an R-algebra which is also H-graded as a ring. So there is a direct sum decomposition

$$A = \bigoplus_{h \in H} A_h,$$

where the A_h are abelian groups which satisfy the property that if $a_{h_1} \in A_{h_1}$ and $a_{h_2} \in A_{h_2}$, then $a_{h_1} a_{h_2} \in A_{h_1+h_2}$. If R is also an H-graded ring, then we also require A to be an H-graded left R-module. This means that if $r_{h_1} \in R_{h_1}$ and $a_{h_2} \in A_{h_2}$, then $r_{h_1} a_{h_2} \in A_{h_1+h_2}$.

62.8.1 Examples of Graded R-Algebras

Example 62.7. Let R be a graded ring and let $\boldsymbol{x} = x_1, \ldots, x_n$. The polynomial ring $R[\boldsymbol{x}]$ over R is both an $\mathbb{N}$-graded R-algebra and an $\mathbb{N}^n$-graded R-algebra. The homogeneous component in degree i with respect to the $\mathbb{N}$-grading is given by

$$R[\boldsymbol{x}]_i = \sum_{\boldsymbol{\alpha}} R_{i-|\boldsymbol{\alpha}|} \boldsymbol{x}^{\boldsymbol{\alpha}}.$$

The homogeneous component in degree $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ with respect to the $\mathbb{N}^n$-grading is given by

More generally, let $\boldsymbol{w} := (w_1, \dots, w_n)$ be an n-tuple of positive integers. We define the **weighted degree of a monomial** of a monomial $\boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, denoted $\deg_w(\boldsymbol{x}^{\boldsymbol{\alpha}})$, by the formula

$$\deg_w(\boldsymbol{x}^{\boldsymbol{\alpha}}) := \langle \boldsymbol{w}, \boldsymbol{\alpha} \rangle := \sum_{\lambda=1}^{n} w_\lambda \alpha_\lambda.$$

The **weighted polynomial ring with respect to the weighted vector** $\boldsymbol{w}$, denoted $R[\boldsymbol{x}]^{\boldsymbol{w}}$, is the polynomial ring $R[\boldsymbol{x}]$ equipped with the **weighted grading**: the homogeneous component in degree i is given by

$$R[\boldsymbol{x}]_i^{\boldsymbol{w}} = \sum_{\boldsymbol{\alpha}} R_{i - \langle \boldsymbol{w}, \boldsymbol{\alpha} \rangle} \boldsymbol{x}^{\boldsymbol{\alpha}}.$$

Example 62.8. Let K be a field, let $R = K[x,y]/\langle xy \rangle$, and let $A = R[z,w]$. View R as a graded K-algebra with $|x| = 1$ and $|y| = 2$ and view A as a graded R-algebra with $|z| = 1$ and $|w| = 3$. Then the homogeneous components of A start out as

$$\begin{aligned}
A_0 &= K \\
A_1 &= K\overline{x} + Kz \\
A_2 &= K\overline{x}^2 + K\overline{x}z + K\overline{y} \\
A_3 &= K\overline{x}^3 + K\overline{x}^2 z + K\overline{xy} + K\overline{x}z^2 + K\overline{y}z + Kw \\
&\vdots
\end{aligned}$$

Example 62.9. Let R be a ring and let Q be an ideal in R. The **blowup algebra of** Q **in** R is defined by

$$B_Q(R) := R + tQ + t^2Q^2 + t^3Q^3 + \cdots \cong \bigoplus_{i=0}^{\infty} Q^i.$$

Elements in $B_Q(R)$ have the form

$$t^{i_1} x_{i_1} + \cdots + t^{i_m} x_{i_m}$$

where $0 \leq i_1 < \cdots < i_m$ and $x_{i_\lambda} \in Q^{i_\lambda}$ for all $1 \leq \lambda \leq m$. The t^{i_λ} part keeps track of what degree we are in. We define multiplaction on elements of the form $t^i x$ and $t^j y$ by

$$(t^i x)(t^j y) = t^{i+j} xy,$$

and we extend this to all of $B_Q(R)$ in the obvious way. This gives $B_Q(R)$ the structure of a graded R-algebra.

If Q is finitely generated, say $Q = \langle a_1, \dots, a_n \rangle$, then there is a unique R-algebra homomorphism

$$\varphi\colon R[u_1, \dots, u_n] \to B_Q(R),$$

such that $\varphi(u_\lambda) = ta_\lambda$ for all $1 \leq \lambda \leq n$.

62.8.2 Graded Associative R-Algebras

Let R be a ring and let $\boldsymbol{x} = x_1, \dots, x_n$ be a list of indeterminates. We denote by $R\langle \boldsymbol{x} \rangle$ to be the **free** R**-algebra generated by** $\boldsymbol{x}$. A basis of $R\langle \boldsymbol{x} \rangle$ as an R-module consists of **words**:

$$\boldsymbol{x}^{\boldsymbol{\alpha}_1} \cdots \boldsymbol{x}^{\boldsymbol{\alpha}_k}$$

where $k \in \mathbb{N}$ and $\boldsymbol{\alpha}_j \in \mathbb{N}^n$ for all $1 \leq j \leq k$. For example, in $R\langle x_1, x_2, x_3 \rangle$, we have

$$\boldsymbol{x}^{\boldsymbol{\alpha}_1} \boldsymbol{x}^{\boldsymbol{\alpha}_2} \boldsymbol{x}^{\boldsymbol{\alpha}_3} = x_3^2 x_1^3 x_2 x_3 x_2,$$

where

$$\begin{aligned}
\boldsymbol{\alpha}_1 &= (0,0,2) \\
\boldsymbol{\alpha}_2 &= (3,2,1) \\
\boldsymbol{\alpha}_3 &= (0,1,0).
\end{aligned}$$

The set of all words is denoted $\mathrm{W}(\boldsymbol{x})$. Words of the form $\boldsymbol{x}^{\boldsymbol{\alpha}}$ are called **standard words** and form a subset of the set of all words. A **standard polynomial** in $R\langle \boldsymbol{x} \rangle$ is a finite linear combination of standard words.

Example 62.10. Let R be a graded ring, let $\boldsymbol{x} = x_1, \dots, x_n$ be a list of indeterminates, and let $\boldsymbol{w} := (w_1, \dots, w_n)$ be an n-tuple of positive integers. We define $R\langle \boldsymbol{x} \rangle^{\boldsymbol{w}}$ to be the graded R-algebra whose homogeneous component in degree i is given by

$$R\langle \boldsymbol{x} \rangle_i^{\boldsymbol{w}} = \sum_{\boldsymbol{x}^{\boldsymbol{\alpha}_1} \cdots \boldsymbol{x}^{\boldsymbol{\alpha}_k} \in \mathrm{W}(\boldsymbol{x})} R_{i - \sum_{j=1}^{k} \langle \boldsymbol{w}, \boldsymbol{\alpha}_j \rangle} \boldsymbol{x}^{\boldsymbol{\alpha}_1} \cdots \boldsymbol{x}^{\boldsymbol{\alpha}_k}.$$

62.8.3 Graded Commutative R-Algebras

Definition 62.13. Let A be a $\mathbb{Z}$-graded R-algebra. We say A is **graded-commutative** if for all $a \in A_i$ and $b \in A_j$, we have

$$ab = (-1)^{ij} ba. \tag{229}$$

We say A is **strictly graded-commutative** if, an addition to (229), we also have $a^2 = 0$ for all odd degree elements $a \in A$.

Remark 107. Cohomology rings are a natural source of graded-commutative rings.

Every finitely-presented R-algebra A is isomorphic to $R\langle \boldsymbol{x} \rangle / I$ where $\boldsymbol{x} = x_1, \dots, x_n$ and where I is a two-sided ideal in $R\langle \boldsymbol{x} \rangle$. For our purposes we will be interested in the following finitely-presented R-algebra.

Definition 62.14. Let R be a ring, let $\boldsymbol{x} = x_1, \dots, x_n$ be indeterminates, and let $\boldsymbol{w} = (w_1, \dots, w_n)$ be their respective weights. Set

$$J = \langle \{ fg - (-1)^{ij} gf \mid f \in R\langle \boldsymbol{x} \rangle_i^{\boldsymbol{w}} \text{ and } g \in R\langle \boldsymbol{x} \rangle_j^{\boldsymbol{w}} \} \cup \{ f^2 \mid f \in R\langle \boldsymbol{x} \rangle_i^{\boldsymbol{w}} \text{ where } i \text{ is odd} \rangle.$$

We define the **free graded-(strictly)-commutative R-algebra generated by $\boldsymbol{x}$ with respect to the weighted vector $\boldsymbol{w}$**, denoted $R\lceil \boldsymbol{x} \rceil_{\boldsymbol{w}}$, to be the graded R-algebra

$$R\lceil \boldsymbol{x} \rceil^{\boldsymbol{w}} := R\langle \boldsymbol{x} \rangle^{\boldsymbol{w}} / J.$$

Since $x_\lambda x_\mu - (-1)^{w_\lambda w_\mu} x_\mu x_\lambda \in J$ for all $1 \leq \lambda < \mu \leq n$, we see that every $\overline{f} \in R\lceil \boldsymbol{x} \rceil^{\boldsymbol{w}}$ can be represented by a standard polynomial $f \in R\langle \boldsymbol{x} \rangle^{\boldsymbol{w}}$. We typically dispense with the overline notation and just write $f \in R\lceil \boldsymbol{x} \rceil^{\boldsymbol{w}}$. In particular, any $f \in R\lceil \boldsymbol{x} \rceil^{\boldsymbol{w}}$ can be expressed as

$$f = \sum_{\boldsymbol{\alpha}} r_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$$

where the sum ranges over all $\boldsymbol{\alpha} \in \mathbb{N}^n$ with $r_{\boldsymbol{\alpha}} = 0$ for almost all $\boldsymbol{\alpha} \in \mathbb{N}^n$.

62.9 Hilbert Function and Dimension

The Hilbert function of a graded module associates to an integer i the dimension of the ith graded part of the given module. For sufficiently large i, the values of this function are given by a polynomial, the Hilbert polynomial.

Definition 62.15. Let R be a Noetherian graded K-algebra and let M be a finitely-generated graded R-module. The **Hilbert function** $H_M \colon \mathbb{Z} \to \mathbb{Z}$ of M is defined by

$$H_M(i) := \dim_K(M_i)$$

Lemma 62.3. *Let R be a Noetherian graded ring and let $i \in \mathbb{Z}$. Then R_i is a finitely-generated R_0-module.*

Proof. The ideal $\langle R_i \rangle$ is finitely-generated since R is Noetherian. Choose generators in $\langle R_i \rangle$ such that each generator belongs to R_i, say $x_1, \dots, x_n \in R_i$. In particular, $\langle R_i \rangle$ is a graded ideal with $\langle R_i \rangle_0 = R_i$. It follows that

$$R_i = R_0 x_1 + \cdots + R_0 x_n,$$

and so R_i is a finitely-generated R_0-module. □

Corollary 63. *Let R be a Noetherian graded ring and let M be a finitely-generated graded R-module. Then M_i is a finitely-generated R_0-module for all $i \in \mathbb{Z}$. Moreover, there exists $k \in \mathbb{Z}$ such that $M_j = 0$ for all $j < \mathbb{Z}$.*

Proof. Choose homogeneous generators of M, say $u_1, \dots, u_n$, and let $i \in \mathbb{Z}$. Then

$$M_i = R_{i - \deg(u_1)} u_1 + \cdots + R_{i - \deg(u_n)} u_n.$$

This implies that M_i is a finitely-generated R_0-module since the R_i's are finitely generated R_0-modules by Lemma (62.3).

For the moreover part, let

$$k = \min\{\deg(u_i) \mid 1 \leq i \leq n\}.$$

Then $M_j = 0$ for all $j < k$ since $R_i = 0$ for all $i < 0$. □

62.10 Semigroup Ordering

Definition 62.16. Let H be an additive semigroup with identity 0. A **semigroup ordering** on H is a partial ordering $>$ on H such that

1. $>$ is a total ordering, i.e. either $h_1 > h_2$ or $h_2 > h_1$ for all $h_1, h_2 \in H$.
2. $>$ is translate invariant, i.e. $h_1 > h_2$ implies $h_1 + h_3 > h_2 + h_3$ for all $h_1, h_2, h_3 \in H$.

If $>$ is a semigroup ordering on H, then we call the pair $(H, >)$ an **additive ordered semigroup**.

Example 62.11. The integers $\mathbb{Z}$ (or the natural numbers $\mathbb{N}$) equipped with the natural order $>$ forms an additive ordered semigroup.

Example 62.12. For $n > 1$, there are many different semigroup orderings we can equip $\mathbb{N}^n$ (or even $\mathbb{Z}^n$). For example, one of them is call **lexicographical ordering**, which is defined as follows: for $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^n$ where $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$, we say $\boldsymbol{\alpha} >_{\text{lex}} \boldsymbol{\beta}$ if for some $1 \leq i \leq n$ we have

$$\begin{aligned} \alpha_1 &= \beta_1 \\ &\vdots \\ \alpha_{i-1} &= \beta_{i-1} \\ \alpha_i &> \beta_i \end{aligned}$$

Theorem 62.4. *Let $(H, >)$ be an additive ordered semigroup, let R be an H-graded ring, and let M be an H-graded R-module. Then every associated prime of M is a homogeneous ideal. Furthermore, ever associated prime of M is the annihilator of a homogeneous element.*

Proof. If $\mathfrak{p}$ is an associated prime of M, it is the annihilator of a nonzero element

$$u = u_{j_1} + \cdots + u_{j_t} \in M,$$

where the u_{j_ν} are nonzero homogeneous elements of degrees $j_1 < \cdots < j_t$. Choose u such that t is as small as possible. Suppose that

$$a = a_{i_1} + \cdots + a_{i_s}$$

kills u, where for every ν, a_{i_ν} has degree i_ν, and $i_1 < \cdots < i_s$. We shall show that every a_{i_ν} kills u, which proves that $\mathfrak{p}$ is homogeneous. It suffices to show that a_{i_1} kills u (since $a - a_{i_1}$ kills u and we can proceed by induction). Since $au = 0$, the unique least degree term $a_{i_1} u_{j_1} = 0$. Therefore

$$u' = a_{i_1} u = a_{i_1} u_{j_2} + \cdots + a_{i_1} u_{j_t}.$$

If this element is nonzero, its annihilator is still $\mathfrak{p}$, since $Ru \cong R/\mathfrak{p}$ and every nonzero element has annihilator $\mathfrak{p}$. Since $a_{i_1} u_{j_\nu}$ is homogeneous of degree $i_1 + j_\nu$, or else is 0, u' has fewer nonzero homogeneous components than u does, contradicting our choice of u.

For the second part of the theorem, suppose $\mathfrak{p} = 0 : u$ is an associated prime of M. Express u in terms of its homogeneous components as

$$u = u_1 + \cdots + u_n.$$

Then note that $\mathfrak{p} = 0 : u \supseteq \bigcap_{i=1}^n 0 : u_i$. Since $\mathfrak{p}$ is prime, we must have $\mathfrak{p} \supseteq 0 : u_i$ for some i. However $0 : u_i \supseteq \mathfrak{p}$ since $au = 0$ implies $au_i = 0$. □

Corollary 64. *If I is a homogeneous ideal of a Noetherian ring R graded by a semigroup H equipped with a semigroup ordering $>$, then every minimal prime of I is homogeneous.*

Proof. This is immediate, since the minimal primes of I are among the associated primes of R/I. □

Proposition 62.14. *Let $(H, >)$ be an additive ordered semigroup, let R be a H-graded ring, and let I be a homogeneous ideal. Then $\sqrt{I}$ is homogeneous.*

Proof. Let

$$f_{i_1} + \cdots + f_{i_k} \in \sqrt{I}$$

with $i_1 < \cdots < i_k$ and each f_{i_j} nonzero of degree i_j. We need to show that every $f_{i_j} \in \sqrt{I}$. If any of the components are in $\sqrt{I}$, we may subtract them off, giving a similar sum whose terms are the homogeneous components not in $\sqrt{I}$. Therefore it suffices to show that $f_{i_1} \in \sqrt{I}$. But

$$\left(f_{i_1} + \cdots + f_{i_k}\right)^N \in I$$

for some $N > 0$. When we expand, there is a unique term formally of least degree, namely $f_{i_1}^N$, and therefore this term is in I, since I is homogeneous. But this means that $f_{i_1} \in \sqrt{I}$, as required. □

Corollary 65. *Let R be a finitely-generated graded K-algebra and let $\mathfrak{m} = \bigoplus_{i=1}^{\infty} R_i$ be the homogeneous maximal ideal of R. Then*

$$\dim R = \operatorname{ht} \mathfrak{m} = \dim R_{\mathfrak{m}}.$$

Proof. The dimension of R will be equal to the dimension of $R/\mathfrak{p}$ for one of the minimal primes $\mathfrak{p}$ of R. Since $\mathfrak{p}$ is minimal, it is an associated prime and therefore is homogeneous. Hence, $\mathfrak{p} \subseteq \mathfrak{m}$. The domain $R/\mathfrak{p}$ is finitely-generated over K, and therefore its dimension is equal to the height of every maximal ideal including, in particular, $\mathfrak{m}/\mathfrak{p}$. Thus,

$$\begin{aligned} \dim R &= \dim R/\mathfrak{p} \\ &= \dim (R/\mathfrak{p})_{\mathfrak{m}} \\ &\leq \dim R_{\mathfrak{m}} \\ &\leq \dim R, \end{aligned}$$

and so equality holds throughout, as required. □

63 Homological Algebra

Throughout this section, let R be a ring (trivially graded).

63.1 R-Complexes

63.1.1 R-Complexes and Chain Maps

Definition 63.1. An **R-complex** (A, d) is a graded R-module A equipped with graded R-linear map $\mathrm{d}\colon A \to A$ of degree -1 such that $\mathrm{d}^2 = 0$. Any such map d which satisfies these properties is called an **R-linear differential**. If we denote the ith homogeneous component of A as A_i and if we denote $\mathrm{d}_i = \mathrm{d}|_{A_i}$, then we may view an R-complex as a sequence of R-modules A_i and R-linear maps $\mathrm{d}_i\colon A_i \to A_{i-1}$ as below

$$\cdots \longrightarrow A_{i+1} \xrightarrow{\mathrm{d}_{i+1}} A_i \xrightarrow{\mathrm{d}_i} A_{i-1} \longrightarrow \cdots \tag{230}$$

such that $\mathrm{d}_i \mathrm{d}_{i+1} = 0$ for all $i \in \mathbb{Z}$. An element in $\ker \mathrm{d}$ is called a **cycle** of (A, d) and an element in $\operatorname{im} \mathrm{d}$ is called a **boundary** of (A, d).

A **chain map** $\varphi\colon (A, \mathrm{d}) \to (A', \mathrm{d}')$ between R-complexes (A, d) and (A', d') is a graded R-linear map $\varphi\colon A \to A'$ of degree 0 which commutes with the differentials:

$$\mathrm{d}'\varphi = \varphi \mathrm{d}.$$

If we denote $\varphi_i = \varphi|_{A_i}$, then we may view φ as a sequence of R-linear maps $\varphi_i\colon A_i \to A'_i$ as below

$$\begin{tikzcd} \cdots \arrow[r] & A_{i+1} \arrow[r, "\mathrm{d}_{i+1}"] \arrow[d, "\varphi_{i+1}"] & A_i \arrow[r, "\mathrm{d}_i"] \arrow[d, "\varphi_i"] & A_{i-1} \arrow[r] \arrow[d, "\varphi_{i-1}"] & \cdots \\ \cdots \arrow[r] & A'_{i+1} \arrow[r, "\mathrm{d}'_{i+1}"] & A'_i \arrow[r, "\mathrm{d}'_i"] & A'_{i-1} \arrow[r] & \cdots \end{tikzcd}$$

such that $\mathrm{d}'_i \varphi_i = \varphi_{i-1} \mathrm{d}'_i$ for all $i \in \mathbb{Z}$. It is easy to check that the identity map $1_{(A,\mathrm{d})}\colon (A, \mathrm{d}) \to (A, \mathrm{d})$ from an R-complex (A, d) to itself is a chain map. It is also easy to check that the composition of two chain maps is a chain map. We obtain the category $\mathbf{Comp}_R$, whose objects are R-complexes and whose morphisms chain maps.

Remark 108. To simplify notation, we often write A instead of (A, d) if the differential is understood from context. For instance, we may introduce an R-complex as "(A, d)" but later refer to it as "A", but we also may introduce an R-complex as "A" with the differential understood to be denoted "d_A". In that case, we will denote $\mathrm{d}_{A,i} = (\mathrm{d}_A)|_{A_i}$. Also a chain map is always understood to be a map between R-complexes. For instance, if we write "let $\varphi\colon A \to A'$ be a chain map" without first introducing A or A', then it is understood that A and A' are R-complexes.

63.1.2 Homology

Let (A, d) be an R-complex. The condition $\mathrm{d}^2 = 0$ is equivalent to the condition $\ker \mathrm{d} \supseteq \operatorname{im} \mathrm{d}$. Since d is graded, we see that both $\ker \mathrm{d}$ and $\operatorname{im} \mathrm{d}$ are graded submodules of A. Therefore we have

$$\ker \mathrm{d} = \bigoplus_{i \in \mathbb{Z}} \ker \mathrm{d}_i \quad \text{and} \quad \operatorname{im} \mathrm{d} = \bigoplus_{i \in \mathbb{Z}} \operatorname{im} \mathrm{d}_i,$$

and for each $i \in \mathbb{Z}$, we have $\ker \mathrm{d}_i \supseteq \operatorname{im} \mathrm{d}_{i+1}$. Therefore $\ker \mathrm{d}/\operatorname{im} \mathrm{d}$ is a graded R-module. With this in mind, we are justified in making the following definitions:

Definition 63.2. Let (A, d) be an R-complex.

1. We say A is **exact** if $\ker \mathrm{d} = \operatorname{im} \mathrm{d}$ and we say A is **exact at** A_i if $\ker \mathrm{d}_i = \operatorname{im} \mathrm{d}_i$.

2. The **homology** of A is defined to be the graded R-module

$$\mathrm{H}(A, \mathrm{d}) := \ker \mathrm{d}/\operatorname{im} \mathrm{d}.$$

   The ith homogeneous component of $\mathrm{H}(A, \mathrm{d})$ is denoted

$$\mathrm{H}_i(A, \mathrm{d}) := \ker \mathrm{d}_i/\operatorname{im} \mathrm{d}_i.$$

Remark 109. If the differential d is clear from context, then we will simplify our notation by denoting the homology of A as $\mathrm{H}(A)$ rather than $\mathrm{H}(A, \mathrm{d})$.

63.1.3 Positive, Negative, and Bounded Complexes

Definition 63.3. Let A be an R-complex.

1. We say A is **positive** if $A_i = 0$ for all $i < 0$.

2. We say A is **bounded below** if $A_i = 0$ for $i \ll 0$. In other words, if A_i is eventually 0, that is, if there exists $n \in \mathbb{Z}$ such that $A_i = 0$ for all $i < n$.

3. We say A is **homologically bounded below** if $\mathrm{H}_i(A) = 0$ for $i \ll 0$.

Similarly,

1. We say A is **negative** if $A_i = 0$ for all $i > 0$.

2. We say A is **bounded above** if $A_i = 0$ for $i \gg 0$.

3. We say A is **homologically bounded above** if $\mathrm{H}_i(A) = 0$ for $i \gg 0$.

If A is both bounded below and bounded above, then we will say A is **bounded**. Similarly, if A is both homologically bounded above and homologically bounded below, then we will say A is **homologically bounded**.

63.1.4 Supremum and Infimum

Definition 63.4. Let A be an R-complex. We define its **supremum** to be

$$\sup A := \begin{cases} -\infty & \text{if } A \text{ is exact} \\ \sup\{i \in \mathbb{Z} \mid \mathrm{H}_i(A) \neq 0\} & \text{if } A \text{ is not exact and is homologically bounded above} \\ \infty & \text{if } A \text{ is not homologically bounded above.} \end{cases}$$

Similarly, we define its **infimum** to be

$$\inf A := \begin{cases} \infty & \text{if } A \text{ is exact} \\ \inf\{i \in \mathbb{Z} \mid \mathrm{H}_i(A) \neq 0\} & \text{if } A \text{ is not exact and is homologically bounded below} \\ -\infty & \text{if } A \text{ is not homologically bounded below.} \end{cases}$$

The **amplitude** of A is defined to be

$$\operatorname{amp} A := \begin{cases} -\infty & \text{if } A \text{ is exact} \\ \infty & \text{if } A \text{ is homologically bounded above but not homologically bounded below} \\ \sup A - \inf A & \text{if } A \text{ is not exact and homologically bounded} \\ \infty & \text{if } A \text{ is homologically bounded below but not homologically bounded above} \\ \infty & \text{if } A \text{ is not homologically bounded above or below.} \end{cases}$$

63.2 Category of R-Complexes

The set of all R-complexes together with the set of all chain maps forms a category, which we denote $\mathbf{Comp}_R$. Similarly, the set of all graded R-modules together with the set of all graded homomorphisms (of degree 0) forms a category, which we denote $\mathbf{Grad}_R$.

63.2.1 Homology Considered as a Functor

We've already seen that if (A, d) is an R-complex, then $\mathrm{H}(A)$ is a graded R-module. We would like to extend this observation to get a functor $\mathrm{H}\colon \mathbf{Comp}_R \to \mathbf{Grad}_R$. This will follow from the following three propositions:

Proposition 63.1. *Let $\varphi\colon (A, \mathrm{d}) \to (A', \mathrm{d}')$ be a chain map. Then φ induces a graded homomorphism $\mathrm{H}(\varphi)\colon \mathrm{H}(A) \to \mathrm{H}(A')$, where*

$$\mathrm{H}(\varphi)(\overline{a}) = \overline{\varphi(a)} \tag{231}$$

for all $\overline{a} \in \mathrm{H}(A)$.

Proof. First let us check that the target of each element in $\mathrm{H}(A)$ under $\mathrm{H}(\varphi)$ lands in $\mathrm{H}(A')$. Let $\overline{a} \in \mathrm{H}(A)$ (so $\mathrm{d}(a) = 0$). Then $\overline{\varphi(a)} \in \mathrm{H}(A')$ since

$$\begin{aligned} \mathrm{d}'(\varphi(a)) &= \varphi(\mathrm{d}(a)) \\ &= 0. \end{aligned}$$

Next let us check that that $\mathrm{H}(\varphi)$ is well-defined. Let $a + \mathrm{d}(b)$ be another representative of the coset class $\overline{a} \in \mathrm{H}(A)$. Then

$$\begin{aligned} \mathrm{H}(\varphi)(\overline{a + \mathrm{d}(b)}) &= \overline{\varphi(a + \mathrm{d}(b))} \\ &= \overline{\varphi(a) + \varphi(\mathrm{d}(b))} \\ &= \overline{\varphi(a)} + \overline{\varphi(\mathrm{d}(b))} \\ &= \overline{\varphi(a)} + \overline{\mathrm{d}'(\varphi(b))} \\ &= \overline{\varphi(a)} \\ &= \mathrm{H}(\varphi)(\overline{a}). \end{aligned}$$

Thus $\mathrm{H}(\varphi)$ is well-defined.

So far we have shown that $\mathrm{H}(\varphi)$ is a function. To see that $\mathrm{H}(\varphi)$ is an R-module homomorphism, let $r, s \in R$ and $a, b \in A$. Then

$$\begin{aligned} \mathrm{H}(\varphi)(\overline{ra + sb}) &= \overline{\varphi(ra + sb)} \\ &= \overline{r\varphi(a) + s\varphi(b)} \\ &= r\overline{\varphi(a)} + s\overline{\varphi(b)} \\ &= r\mathrm{H}(\varphi)(\overline{a}) + s\mathrm{H}(\varphi)(\overline{b}). \end{aligned}$$

Finally, to see that $\mathrm{H}(\varphi)$ is graded, let $\overline{a}_i \in \mathrm{H}_i(A)$ (so $a_i \in A_i$). Then

$$\begin{aligned} \mathrm{H}(\varphi)(\overline{a}_i) &= \overline{\varphi(a_i)} \\ &\in \mathrm{H}_i(A') \end{aligned}$$

since φ is graded. □

Proposition 63.2. *Let $\varphi\colon (A, \mathrm{d}) \to (A', \mathrm{d}')$ and $\varphi'\colon (A', \mathrm{d}') \to (A'', \mathrm{d}'')$ be two chain maps. Then*

$$\mathrm{H}(\varphi' \circ \varphi) = \mathrm{H}(\varphi') \circ \mathrm{H}(\varphi).$$

Proof. Let $\overline{a} \in \mathrm{H}(A)$. Then we have

$$\begin{aligned} \mathrm{H}(\varphi' \circ \varphi)(\overline{a}) &= \overline{(\varphi' \circ \varphi)(a)} \\ &= \overline{\varphi'(\varphi(a))} \\ &= \mathrm{H}(\varphi')(\overline{\varphi(a)}) \\ &= \mathrm{H}(\varphi')(\mathrm{H}(\varphi)(\overline{a})) \\ &= (H(\varphi') \circ H(\varphi))(\overline{a}). \end{aligned}$$

□

Proposition 63.3. *Let (A, d) be an R-complex. Then we have*

$$\mathrm{H}(\mathrm{id}_{(A,\mathrm{d})}) = \mathrm{id}_{\mathrm{H}(A)}.$$

In particular, if $\varphi\colon (A,\mathrm{d}) \to (A',\mathrm{d}')$ is a chain map isomorphism, then $\mathrm{H}(\varphi)\colon \mathrm{H}(A) \to \mathrm{H}(A')$ is an isomorphism between graded R-modules $\mathrm{H}(A)$ and $\mathrm{H}(A')$.

Proof. Let $\overline{a} \in \mathrm{H}(A)$. Then

$$\begin{aligned} \mathrm{H}(\mathrm{id}_{(A,\mathrm{d})})(\overline{a}) &= \overline{\mathrm{id}_{(A,\mathrm{d})}(a)} \\ &= \overline{a} \\ &= \mathrm{id}_{\mathrm{H}(A)}(\overline{a}). \end{aligned}$$

For the latter statement, let $\varphi\colon (A,\mathrm{d}) \to (A',\mathrm{d}')$ be a chain map isomorphism and let $\psi\colon (A',\mathrm{d}') \to (A,\mathrm{d})$ be its inverse. Then

$$\begin{aligned} \mathrm{id}_{\mathrm{H}(A)} &= \mathrm{H}(\mathrm{id}_{(A,d)}) \\ &= \mathrm{H}(\psi \circ \varphi) \\ &= \mathrm{H}(\psi) \circ \mathrm{H}(\varphi). \end{aligned}$$

A similar computation gives $\mathrm{H}(\varphi) \circ \mathrm{H}(\psi) = \mathrm{id}_{\mathrm{H}(A')}$. □

63.2.2 $\mathbf{Comp}_R$ is an R-linear category

There is more structure on the categories $\mathbf{Comp}_R$ and $\mathbf{Grad}_R$ which we haven't discussed so far. They are examples of R-linear categories[9]. Moreover, homology can be viewed as an additive functor from $\mathbf{Comp}_R$ to $\mathbf{Grad}_R$.

Proposition 63.4. *$\mathbf{Comp}_R$ is an R-linear category.*

Proof. Let (A, d) and (A', d') be two R-complexes. We define $\mathcal{C}(A, A')$

$$\mathcal{C}(A, A') := \mathrm{Hom}((A,\mathrm{d}),(A',\mathrm{d}')) := \{\varphi\colon (A,\mathrm{d}) \to (A',\mathrm{d}') \mid \varphi \text{ is a chain map}\}.$$

Then $\mathcal{C}(A, A')$ has the structure of an R-module. Indeed, if $\varphi, \psi \in \mathcal{C}(A, A')$ and $r \in R$, then we define addition and scalar multiplication by

$$(\varphi + \psi)(a) := \varphi(a) + \psi(a) \quad \text{and} \quad (r\varphi)(a) = \varphi(ra)$$

for all $a \in A$. Since d is an R-linear map, it is clear that $\varphi + \psi$ and $r\varphi$ are chain maps (that is, they are graded R-linear maps which commute with the differentials).

Moreover, let (A'', d'') be another R-complex. We define composition

$$\circ\colon \mathcal{C}(A', A'') \times \mathcal{C}(A, A') \to \mathcal{C}(A, A''),$$

in the usual way: if $(\varphi', \varphi) \in \mathcal{C}(A', A'') \times \mathcal{C}(A, A')$, then we define $\varphi' \circ \varphi \in \mathcal{C}(A, A'')$ by

$$(\varphi' \circ \varphi)(a) = \varphi'(\varphi(a))$$

for all $a \in A$. Again one checks that $\varphi' \circ \varphi$ is indeed a chain map. Observe that composition is an R-bilinear map. For instance, let $\varphi', \psi' \in \mathcal{C}(A', A'')$ and $\varphi \in \mathcal{C}(A, A')$. Then

$$\begin{aligned} ((\varphi' + \psi') \circ \varphi)(a) &= (\varphi' + \psi')(\varphi(a)) \\ &= \varphi'(\varphi(a)) + \psi'(\varphi(a)) \\ &= (\varphi' \circ \varphi)(a) + (\psi' \circ \varphi)(a) \end{aligned}$$

for all $a \in A$. Thus $(\varphi' + \psi') \circ \varphi = \varphi' \circ \varphi + \psi' \circ \varphi$. A similar proof gives the other properties of R-bilinearity. □

Remark 110. To clean notation, we often drop the $\circ$ symbol when denoting composotin. For instance, we often write $\varphi\psi$ rather than $\varphi \circ \psi$.

[9]See Appendix for definition of R-linear categories.

63.2.3 The inclusion functor from $\mathbf{Grad}_R$ to $\mathbf{Comp}_R$ is fully faithful

Every graded R-module M can be view as an R-complex with differential $\mathrm{d} = 0$. In fact, we obtain a functor

$$\iota\colon \mathbf{Grad}_R \to \mathbf{Comp}_R,$$

where the graded R-module M is mapped to the trivially R-complex $(M, 0)$, and where graded homomorphisms $\varphi\colon M \to M'$ is mapped to the chain map $\varphi\colon (M, 0) \to (M, 0')$ of trivially R-complexes. Clearly φ is in fact chain map since these are trivial R-complexes. The functor ι is full and faithful. It is left-adjoint to the forgetful functor

$$\rho\colon \mathbf{Comp}_R \to \mathbf{Grad}_R$$

where ρ maps the R-complex (M, d) to the graded R-module M, and where ρ maps the chain map $\varphi\colon (M, \mathrm{d}) \to (M', \mathrm{d}')$ to the graded homomorphism $\varphi\colon M \to M'$. Then ρ is still faithful, but it is not full since there may be many graded homomorphism $M \to M'$ which do not come from forgetting a chain map $(M, \mathrm{d}) \to (M', \mathrm{d}')$.

63.2.4 The homology functor from $\mathbf{Comp}_R$ to $\mathbf{Grad}_R$

There is another functor which goes from $\mathbf{Comp}_R$ to $\mathbf{Grad}_R$ which is called the **homology functor**. It is denoted

$$\mathrm{H}\colon \mathbf{Comp}_R \to \mathbf{Grad}_R,$$

and is given by mapping an R-complex (M, d) to the graded R-module $\mathrm{H}(M, \mathrm{d})$, and by mapping the chain map $\varphi\colon (M, \mathrm{d}) \to (M', \mathrm{d}')$ to the graded R-linear map $\mathrm{H}(\varphi)\colon \mathrm{H}(M, \mathrm{d}) \to \mathrm{H}(M', \mathrm{d}')$. Let us show that H is an R-linear functor.

Proposition 63.5. *Let $\varphi, \psi\colon (A, \mathrm{d}) \to (A', \mathrm{d}')$ be two chain maps and let $r, s \in R$. Then*

$$\mathrm{H}(r\varphi + s\psi) = r\mathrm{H}(\varphi) + s\mathrm{H}(\psi)$$

Proof. Let $\overline{a} \in \mathrm{H}(A)$. Then

$$\begin{aligned}
\mathrm{H}(r\varphi + s\psi)(\overline{a}) &= \overline{(r\varphi + s\psi)(a)} \\
&= \overline{r\varphi(a) + s\psi(a)} \\
&= r\overline{\varphi(a)} + s\overline{\psi(a)} \\
&= r\mathrm{H}(\varphi)(a) + s\mathrm{H}(\psi)(a).
\end{aligned}$$

□

63.2.5 Inverse Systems and Inverse Limits in the Category of R-Complexes

Definition 63.5. Let $(\Lambda, \leq)$ be a preordered set (i.e. $\leq$ is reflexive and transitive). An **inverse system** $(A_\lambda, \varphi_{\lambda\mu})$ of R-complexes and chains maps over Λ consists of a family of R-complexes $\{(A_\lambda, \mathrm{d}_\lambda)\}$ indexed by Λ and a family of chian maps $\{\varphi_{\lambda\mu}\colon A_\mu \to A_\lambda\}_{\lambda \leq \mu}$ such that for all $\lambda \leq \mu \leq \kappa$,

$$\varphi_{\lambda\lambda} = 1_{M_\lambda} \quad \text{and} \quad \varphi_{\lambda\kappa} = \varphi_{\lambda\mu}\varphi_{\mu\kappa}.$$

Suppose $(M_\lambda, \varphi_{\lambda\mu})$ and $(M'_\lambda, \varphi'_{\lambda\mu})$ are two direct systems over a partially ordered set $(\Lambda, \leq)$. A **morphism** $\psi\colon (M_\lambda, \varphi_{\lambda\mu}) \to (M'_\lambda, \varphi'_{\lambda\mu})$ of inverse systesms consists of a collection of graded R-linear maps $\psi_\lambda\colon M_\lambda \to M'_\lambda$ indexed by Λ such that for all $\lambda \leq \mu$ we have

$$\varphi'_{\lambda\mu}\psi_\mu = \psi_\lambda\varphi_{\lambda\mu}.$$

Proposition 63.6. *Let $(M_\lambda, \varphi_{\lambda\mu})$ be an inverse system of graded R-modules and graded R-linear maps over a preordered set $(\Lambda, \leq)$. The inverse limit of this system, denoted $\overset{\star}{\varprojlim} M_\lambda$, is (up to unique isomorphism) given by the graded R-module*

$$\overset{\star}{\varprojlim} M_\lambda = \left\{ (u_\lambda) \in \overset{\star}{\prod_{\lambda \in \Lambda}} M_\lambda \mid \varphi_{\lambda\mu}(u_\mu) = u_\lambda \text{ for all } \lambda \leq \mu \right\}$$

together with the projection maps

$$\pi_\lambda\colon \overset{\star}{\varprojlim} M_\lambda \to M_\lambda$$

for all $\lambda \in \Lambda$. In particular, the homogeneous component of degree i in $\overset{\star}{\varprojlim} M_\lambda$ is given by

$$(\overset{\star}{\varprojlim} M_\lambda)_i = \varprojlim M_{\lambda,i}.$$

Remark 111. We put a $\star$ above $\varprojlim$ to remind ourselves that this is the inverse limit in the category of all graded R-modules. In the category of all R-modules, the inverse limit is denoted by $\varprojlim M_\lambda$. If Λ is finite, then $\lim M_\lambda$ already has a natural interpretation of a graded R-module.

Proof. We need to show that $\overset{\star}{\varprojlim} M_\lambda$ satisfies the universal mapping property. Let (M, ψ_λ) be compatible with respect to the invserse system $(M_\lambda, \varphi_{\lambda\mu})$, so $\varphi_{\lambda\mu}\psi_\mu = \psi_\lambda$ for all $\lambda \leq \mu$. By the universal mapping property of the graded product, there exists a unique graded R-linear map $\psi\colon M \to \prod_\lambda^\star M_\lambda$ such that $\pi_\lambda \psi = \psi_\lambda$ for all $\lambda \in \Lambda$. In fact, this map lands in $\overset{\star}{\varprojlim} M_\lambda$ since

$$\begin{aligned} \varphi_{\lambda\mu}\pi_\mu\psi(u) &= \varphi_{\lambda\mu}\psi_\mu(u) \\ &= \psi_\lambda(u) \\ &= \pi_\lambda\psi(u) \end{aligned}$$

for all $u \in M$. □

63.2.6 Homology of Inverse Limit

Let (A^n, φ^{mn}) be an inverse system of R-complexes and chain maps indexed over a preordered set $\mathbb{N}$ and set $A = \varprojlim A^n$. In general, the homology of A is complicated and will not necessarily be related to the induced inverse limit of homologies of A^n. However the following proposition does give us a simple criterion to determine when A is acyclic:

Proposition 63.7. *Suppose that each φ^{mn} is surjective and that each A^n is acyclic. Then A is acyclic.*

Proof. Let $\overline{(a^n)} \in \mathrm{H}A$. So $\mathrm{d}^n(a^n) = 0$ and $\varphi^{mn}(a^n) = a^m$ for all $m \leq n$. In order to show that $\overline{(a^n)} = 0$, we need to construct a sequence (b^n) in $\prod A^n$ such that $\mathrm{d}^n(b^{n+1}) = a^n$ and $\varphi^{mn}(b^n) = b^m$. We will do this by induction on n. In the base case $n = 1$, we use the fact that $\mathrm{H}(A^1) = 0$ to get $b^1 \in A^1$ such that $\mathrm{d}^1(b^1) = a^1$. Now suppose that for some $n \in \mathbb{N}$, we have constructed $b^m \in A^m$ for all $m \leq n$ such that $\varphi^{lm}(b^m) = b^l$ and $\mathrm{d}^m(b^m) = a^m$ for all $l \leq m \leq n$. Using the fact that $\mathrm{H}(A^{n+1}) = 0$, we first choose $\widetilde{b}^{n+1} \in A^{n+1}$ such that $\mathrm{d}\widetilde{b}^{n+1} = 0$. Note that $\varphi^{n,n+1}(\widetilde{b}^{n+1}) - b^n \in Z^n$, so using the fact that A^n is acyclic, there exists a $c^n \in A^n$ such that

$$\varphi^{n,n+1}(\widetilde{b}^{n+1}) - b^n = \mathrm{d}^n c^n.$$

Finally, using the fact that $\varphi^{n,n+1}$ restricts to a surjective map $Z^{n+1} \twoheadrightarrow Z^n$, there exists $c^{n+1} \in A^{n+1}$ such that $\varphi^{n,n+1}(c^{n+1}) = c^n$. Finally, setting $b^{n+1} = \widetilde{b}^{n+1} + \mathrm{d}^{n+1}c^{n+1}$, we see that $\mathrm{d}b^{n+1} = a^{n+1}$ and $\varphi^{n,n+1}b^{n+1} = b^n$ as desired. □

63.2.7 Homology commutes with coproducts

Proposition 63.8. *Let λ be an index set and let $(A_\lambda, \mathrm{d}_\lambda)$ be an R-complex for each $\lambda \in \Lambda$. Then*

$$\mathrm{H}\left(\bigoplus_{\lambda\in\Lambda} A_\lambda\right) \cong \bigoplus_{\lambda\in\Lambda} \mathrm{H}(A_\lambda).$$

63.2.8 Homology commutes with graded limits

Proposition 63.9. *Let λ be an index set and let $(A_\lambda, \mathrm{d}_\lambda)$ be an R-complex for each $\lambda \in \Lambda$. Then*

$$\mathrm{H}\left(\bigoplus_{\lambda\in\Lambda} A_\lambda\right) \cong \bigoplus_{\lambda\in\Lambda} \mathrm{H}(A_\lambda).$$

63.3 Homotopy

Definition 63.6. Let φ and ψ be two chain maps between R-complexes (A, d) and (A', d'). We say φ is **homotopic to** ψ if there exists a graded homomorphism $h\colon A \to A'$ of degree 1 such that

$$\varphi - \psi = \mathrm{d}'h + h\mathrm{d}.$$

We call h a **homotopy from** φ **to** ψ. If $\psi = 0$, then we say φ is **null-homotopic**.

63.3.1 Homotopy is an equivalence relation

Proposition 63.10. *Let $\mathcal{C}(A, A')$ denote the set of all chain maps between R-complexes (A, d) and (A', d'). Homotopy gives an equivalence relation on $\mathcal{C}(A, A')$: for two elements $\varphi, \psi \in \mathcal{C}(A, A')$, write $\varphi \sim \psi$ if φ is homotopic to ψ. Then $\sim$ is an equivalence relation.*

Proof. First we show reflexivity. Let $\varphi \in \mathcal{C}(A, A')$. Then the zero map $h = 0$ gives a homotopy from φ to itself.

Next we show symmetry. Let $\varphi, \psi \in \mathcal{C}(A, A')$ and suppose $\varphi \sim \psi$. Choose a homotopy h from φ to ψ. Then $-h$ is a homotopy from ψ to φ.

Finally we show transitivity. Let $\varphi, \psi, \omega \in \mathcal{C}(A, A')$ and suppose $\varphi \sim \psi$ and $\psi \sim \omega$. Choose a homotopy h from φ to ψ and a homotopy h' from ψ to ω. Then

$$\varphi - \psi = \mathrm{d}'h + h\mathrm{d} \qquad \text{and} \qquad \psi - \omega = \mathrm{d}'h' + h'\mathrm{d}.$$

Adding these together gives us

$$\begin{aligned} \varphi - \omega &= \mathrm{d}'h + h\mathrm{d} + \mathrm{d}'h' + h'\mathrm{d} \\ &= \mathrm{d}'(h + h') + (h + h')\mathrm{d}. \end{aligned}$$

Therefore $h + h'$ is a homotopy from φ to ω. □

63.3.2 Homotopy induces the same map on homology

Proposition 63.11. *Let φ and ψ be chain maps of chain complexes (A, d) and (A', d'). If φ is homotopic to ψ, then $\mathrm{H}(\varphi) = \mathrm{H}(\psi)$.*

Proof. Showing $\mathrm{H}(\varphi) = \mathrm{H}(\psi)$ is equivalent to showing $\mathrm{H}(\varphi - \psi) = 0$ since H is additive. Thus, we may assume that φ is null-homotopic and that we are trying to show that $\mathrm{H}(\varphi) = 0$. Let $\overline{a} \in \mathrm{H}(A, d)$. Then $\mathrm{H}(a) = 0$, and so

$$\begin{aligned} \mathrm{H}(\varphi)(\overline{a}) &= \overline{\varphi(a)} \\ &= \overline{(\mathrm{d}'h + h\mathrm{d})(a)} \\ &= \overline{\mathrm{d}'(h(a)) + h(\mathrm{d}(a))} \\ &= \overline{\mathrm{d}'(h(a))} \\ &= 0. \end{aligned}$$

□

63.3.3 The Homotopy Category of R-Complexes

Recall that $\mathbf{Comp}_R$ is an R-linear category. In particular, this means that for each pair of R-complexes A and A' we have an R-module structure on the set of all chain maps between them. This R-module is denoted by $\mathcal{C}(A, A')$. Moreover the composition map

$$\circ \colon \mathcal{C}(A', A'') \times \mathcal{C}(A, A') \to \mathcal{C}(A, A'')$$

is R-bilinear. For any two R-complexes A and A' let us denote

$$[\mathcal{C}(A, A')] := \mathcal{C}(A, A')/\sim,$$

where $\sim$ is the homotopy equivalence relation. We shall write $[\varphi]$ for the equivalence class in $[\mathcal{C}(A, A')]$ with $\varphi \in \mathcal{C}(A, A')$ as one of its representatives. We want to show that the R-module structure on $\mathcal{C}(A, A')$ induces an R-module structure on $[\mathcal{C}(A, A')]$ and that the composition map $\circ$ induces an R-bilinear map

$$[\circ] \colon [\mathcal{C}(A', A'')] \times [\mathcal{C}(A, A')] \to [\mathcal{C}(A, A'')].$$

More generally, we define the **homotopy category** of all R-complexes, denoted $\mathbf{HComp}_R$, to be the category whose objects are R-complexes and whose morphisms are homotopy classes of chain maps. The next theorem will prove that this is in fact a well-defined R-linear category.

Theorem 63.1. $\mathbf{HComp}_R$ *is an R-linear category.*

Proof. Let A and A' be R-complexes. We first show that $[\mathcal{C}(A,A')]$ has an induced R-module structure. Let $[\varphi],[\psi]\in[\mathcal{C}(A,A')]$ and let $r,s\in R$. We set

$$r[\varphi]+s[\psi]:=[r\varphi+s\psi]. \tag{232}$$

Let us check that (232) is in fact well-defined. Suppose $\varphi\sim\widetilde{\varphi}$ and $\psi\sim\widetilde{\psi}$. Choose a homotopy σ from φ to φ' and choose a homotopy τ from ψ to ψ'. Thus

$$\varphi-\widetilde{\varphi}=\sigma\mathrm{d}+\mathrm{d}'\sigma \quad\text{and}\quad \psi-\widetilde{\psi}=\tau\mathrm{d}+\mathrm{d}'\tau.$$

We claim that $r\sigma+s\tau$ is a homotopy from $r\varphi+s\psi$ to $r\widetilde{\varphi}+s\widetilde{\psi}$. Indeed, $\sigma+\tau$ is a graded R-linear map of degree 1 from A to A'. Moreover, we have

$$\begin{aligned} r\varphi+s\psi-(r\widetilde{\varphi}+s\widetilde{\psi}) &= r(\varphi-\widetilde{\varphi})+s(\psi-\widetilde{\psi})\\ &= r(\sigma\mathrm{d}+\mathrm{d}'\sigma)+s(\tau\mathrm{d}+\mathrm{d}'\tau)\\ &= (r\sigma+s\tau)\mathrm{d}+\mathrm{d}'(r\sigma+s\tau). \end{aligned}$$

Thus (232) is well-defined.

Now we will show that composition in $\mathbf{Comp}_R$ induces a well-defined R-bilinear composition operation in $\mathbf{HComp}_R$. Let A, A', and A'' be R-complexes. Let us check that composition map $\circ$ on chain maps induces an R-bilinear composition map on homotopy classes of chain maps:

$$[\circ]\colon[\mathcal{C}(A',A'')]\times[\mathcal{C}(A,A')]\to[\mathcal{C}(A,A'')].$$

Let $([\varphi'],[\varphi])\in[\mathcal{C}(A',A'')]\times[\mathcal{C}(A,A')]$. We define

$$[\circ]([\varphi'],[\varphi])=[\varphi'\varphi]. \tag{233}$$

Let us check that (233) is in fact well-defined. Suppose $\varphi\sim\psi$ and $\varphi'\sim\psi'$. Choose a homotopy h from φ to ψ and choose a homotopy h' from φ' to ψ'. Thus

$$\varphi-\psi=h\mathrm{d}+\mathrm{d}'h \quad\text{and}\quad \varphi'-\psi'=h'\mathrm{d}'+\mathrm{d}''h'.$$

We claim that $\varphi'h+h'\psi$ is a homotopy from $\varphi'\varphi$ to $\psi'\psi$. Indeed, $\varphi'h+h'\psi$ is a graded R-linear map of degree 1 from A to A''. Moreover we have

$$\begin{aligned} (\varphi'h+h'\psi)\mathrm{d}+\mathrm{d}''(\varphi'h+h'\psi) &= \varphi'h\mathrm{d}+h'\psi\mathrm{d}+\mathrm{d}''\varphi'h+\mathrm{d}''h'\psi\\ &= \varphi'h\mathrm{d}+h'\mathrm{d}'\psi+\varphi'\mathrm{d}'h+\mathrm{d}''h'\psi\\ &= \varphi'(\varphi-\psi-\mathrm{d}'h)+(\varphi'-\psi'-\mathrm{d}''h')\psi+\varphi'\mathrm{d}'h+\mathrm{d}''h'\psi\\ &= \varphi'\varphi-\varphi'\psi-\varphi'\mathrm{d}'h+\varphi'\psi-\psi'\psi-\mathrm{d}''h'\psi+\varphi'\mathrm{d}'h+\mathrm{d}''h'\psi\\ &= \varphi'\varphi-\psi'\psi. \end{aligned}$$

Therefore $\varphi'\varphi\sim\psi'\psi$, and so (233) is well-defined. Observe that R-bilinearity and associativity of (233) follows trivially from R-bilinearity and associativity of composition in $\mathbf{Comp}_R$. Also for each R-complex A, the homotopy class of the identity map 1_A serves as the identity morphism for A in $\mathbf{HComp}_R$, which is easily seen to satisfy the left and right unity laws since 1_A satisfies the left and right unity laws in $\mathbf{Comp}_R$. □

63.3.4 Homotopy equivalences

Definition 63.7. Let $\varphi\colon(A,\mathrm{d})\to(A',\mathrm{d}')$ be a chain map. We say φ is a **homotopy equivalence** if there exists a chain map $\varphi'\colon(A',\mathrm{d}')\to(A,\mathrm{d})$ such that $\varphi'\varphi\sim 1_A$ and $\varphi\varphi'\sim 1_{A'}$. In this case, we call φ' a **homotopy inverse** to φ.

Proposition 63.12. *Let $\varphi\colon(A,\mathrm{d})\to(A',\mathrm{d}')$ be an isomorphism of R-complexes with $\varphi'\colon(A',\mathrm{d}')\to(A,\mathrm{d})$ being its inverse. Then both φ is a homotopy equivalence with φ' being a homotopy inverse.*

Proof. Since φ and φ' are inverse to each other, we see that $\varphi'\varphi=1_A$ and $\varphi\varphi'=1_{A'}$. In particular, if we take h to be the zero map, then we have

$$\begin{aligned} h\mathrm{d}+\mathrm{d}'h &= 0\cdot d+\mathrm{d}'\cdot 0\\ &= 0\\ &= \varphi'\varphi-1_A. \end{aligned}$$

Thus $\varphi'\varphi\sim 1_A$. By a similar argument, we also have $\varphi\varphi'\sim 1_{A'}$. □

Remark 112. Note that a chain map $\varphi\colon(A,\mathrm{d})\to(A',\mathrm{d}')$ is a homotopy equivalence if and only if $[\varphi]$ is an isomorphism.

63.4 Quasiisomorphisms

Definition 63.8. Let $\varphi\colon A \to A'$ be a chain map. We say φ is a **quasiisomorphism** if the induced map in homology $\mathrm{H}(\varphi)\colon \mathrm{H}(A) \to \mathrm{H}(A')$ is an isomorphism of graded R-modules.

63.4.1 Homotopy equivalence is a quasiisomorphism

Proposition 63.13. *Let $\varphi\colon (A,\mathrm{d}) \to (A',\mathrm{d}')$ be a homotopy equivalence with homotopy inverse $\varphi'\colon (A',\mathrm{d}') \to (A,\mathrm{d})$. Then both φ and φ' are quasiisomorphisms.*

Proof. Since $\varphi'\varphi \sim 1_A$ and since homology takes homotopic maps to equal maps, we see that

$$\begin{aligned} 1_{\mathrm{H}(A)} &= \mathrm{H}(1_A) \\ &= \mathrm{H}(\varphi'\varphi) \\ &= \mathrm{H}(\varphi')\mathrm{H}(\varphi). \end{aligned}$$

A similarl calculation gives us $\mathrm{H}(\varphi')\mathrm{H}(\varphi) = 1_{\mathrm{H}(A')}$. Therefore $\mathrm{H}(\varphi)\colon \mathrm{H}(A) \to \mathrm{H}(A')$ is an isomorphism of graded R-modules with $\mathrm{H}(\varphi')\colon \mathrm{H}(A') \to \mathrm{H}(A)$ being its inverse. $\square$

Remark 113. The converse is not true. That is, there there are many examples quasiisomorphisms which are not homotopy equivalences.

63.4.2 Quasiisomorphism equivalence relation

Definition 63.9. Let A and A' be R-complexes. We A is **quasiisomorphic** to A', denoted $A \sim_q A'$, if there exists R-complexes $A_0, \dots, A_n$ and $B_1, \dots, B_n$ where $A_0 = A$ and $A_n = A'$, together with quasisomorphisms

$$\sigma_m\colon B_m \to A_{m-1} \quad \text{and} \quad \tau_m\colon B_m \to A_m$$

for each $0 < m \le n$. In terms of arrows, this looks like

$$\begin{tikzcd}[column sep=small] & B_1 \arrow[dl, "\sigma_1"'] \arrow[dr, "\tau_1"] & & \cdots \arrow[dl] \arrow[dr] & & B_n \arrow[dl, "\sigma_n"'] \arrow[dr, "\tau_n"] & \\ A_0 & & A_1 & & A_{n-1} & & A_n \end{tikzcd}$$

One can easily check that being quasiisomorphic is an equivalence relation. It turns out that one can easily simplify this equivalence relation quite a bit. This is described in the following proposition.

Proposition 63.14. *Let A and A' be R-complexes. Then A is quasiisomorphic to A' if and only if there exists a semiprojective R-complex P together with quasiisomorphisms $\pi\colon P \to A$ and $\pi'\colon P \to A$.*

Proof. One direction is clear, so it suffices to prove the other direction. Suppose $A \sim_q A'$. Choose R-complexes $A_0, \dots, A_n$ and $B_1, \dots, B_n$ where $A_0 = A$ and $A_n = A'$, together with quasisomorphisms

$$\sigma_m\colon B_m \to A_{m-1} \quad \text{and} \quad \tau_m\colon B_m \to A_m$$

for each $0 < m \le n$. Choose a semiprojective resolution $\pi_0\colon P \to A_0$ of A_0. Let $\widetilde{\pi}_0\colon P \to B_1$ be a homotopic lift of π_0 with respect to σ_1 and denote $\pi_1 = \tau_1\widetilde{\pi}_0$. We proceed inductively to construct chain maps $\widetilde{\pi}_{m-1}\colon P_m \to B_m$ and $\pi_m\colon P_m \to A_m$ where $\widetilde{\pi}_{m-1}$ is a homotopic lift of π_{m-1} with respect to σ_m and where $\pi_m = \tau_m\widetilde{\pi}_{m-1}$.

We prove by induction on $1 \le m \le n$ that π_m and $\widetilde{\pi}_{m-1}$ are quasiisomorphisms. First we consider the base case $m = 1$. Observe that $\sigma_1\widetilde{\pi}_0 \sim \pi_0$ implies $\mathrm{H}(\sigma_1)\mathrm{H}(\widetilde{\pi}_0) = \mathrm{H}(\pi_0)$. Then $\mathrm{H}(\widetilde{\pi}_0)$ is an isomorphism since both $\mathrm{H}(\sigma_1)$ and $\mathrm{H}(\pi_0)$ are isomorphisms. Therefore $\widetilde{\pi}_0$ is a quasiisomorphism. Similarly, π_1 is a quasiisomorphisms since it is a composition of quasiisomorphisms.

Now suppose we have shown that π_m and $\widetilde{\pi}_{m-1}$ are quasiisomorphisms for some $m < n$. Observe that $\sigma_m\widetilde{\pi}_{m-1} \sim \pi_m$ implies $\mathrm{H}(\sigma_m)\mathrm{H}(\widetilde{\pi}_{m-1}) = \mathrm{H}(\pi_m)$. Then $\mathrm{H}(\widetilde{\pi}_{m-1})$ is an isomorphism since both $\mathrm{H}(\sigma_m)$ and $\mathrm{H}(\pi_m)$ are isomorphisms. Therefore $\widetilde{\pi}_{m-1}$ is a quasiisomorphism. Similarly, π_{m+1} is a quasiisomorphisms since it is a composition of quasiisomorphisms.

Thus we have shown by induction that π_m and $\widetilde{\pi}_{m-1}$ are quasiisomorphisms for all $1 \le m \le n$. In particular, $\pi_n\colon P \to A_n$ is a quasiisomorphism. $\square$

63.5 Exact Sequences of R-Complexes

Definition 63.10. Let (A, d), (A', d'), and (A'', d'') be R-complexes and let $\varphi\colon A' \to A$ and $\psi\colon A \to A''$ be chain maps. Then we say that

$$0 \longrightarrow (A', \mathrm{d}') \xrightarrow{\varphi} (A, \mathrm{d}) \xrightarrow{\psi} (A'', \mathrm{d}'') \longrightarrow 0$$

is a **short exact sequence** of R-complexes if it is a short exact sequence when considered as graded R-modules. More specifically, this means that following diagram is commutative with exact rows:

$$\begin{tikzcd}
 & \vdots \arrow[d, "\mathrm{d}'_{i+2}"] & \vdots \arrow[d, "\mathrm{d}_{i+2}"] & \vdots \arrow[d, "\mathrm{d}''_{i+2}"] & \\
0 \arrow[r] & A'_{i+1} \arrow[r, "\varphi_{i+1}"] \arrow[d, "\mathrm{d}'_{i+1}"] & A_{i+1} \arrow[r, "\psi_{i+1}"] \arrow[d, "\mathrm{d}_{i+1}"] & A''_{i+1} \arrow[r] \arrow[d, "\mathrm{d}''_{i+1}"] & 0 \\
0 \arrow[r] & A'_{i} \arrow[r, "\varphi_{i}"] \arrow[d, "\mathrm{d}'_{i}"] & A_{i} \arrow[r, "\psi_{i}"] \arrow[d, "\mathrm{d}_{i}"] & A''_{i} \arrow[r] \arrow[d, "\mathrm{d}''_{i}"] & 0 \\
0 \arrow[r] & A'_{i-1} \arrow[r, "\varphi_{i-1}"] \arrow[d, "\mathrm{d}'_{i-1}"] & A_{i-1} \arrow[r, "\psi_{i-1}"] \arrow[d, "\mathrm{d}_{i-1}"] & A''_{i-1} \arrow[r] \arrow[d, "\mathrm{d}''_{i-1}"] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

63.5.1 Long exact sequence in homology

Theorem 63.2. *Let*

$$0 \longrightarrow (A', \mathrm{d}') \xrightarrow{\varphi} (A, \mathrm{d}) \xrightarrow{\psi} (A'', \mathrm{d}'') \longrightarrow 0$$

be a short exact sequence of R-complexes. Then there exists a graded homomorphism $\eth\colon \mathrm{H}(A'') \to \mathrm{H}(A')$ of degree -1 such that

$$\begin{tikzcd}
 & \cdots \arrow[r] & \mathrm{H}_{i+1}(A'') \arrow[dll, rounded corners, "\eth_{i+1}"] \\
\mathrm{H}_i(A') \arrow[r, "\mathrm{H}_i(\varphi)"] & \mathrm{H}_i(A) \arrow[r, "\mathrm{H}_i(\psi)"] & \mathrm{H}_i(A'') \arrow[dll, rounded corners, "\eth_{i}"] \\
\mathrm{H}_{i-1}(A') \arrow[r] & \cdots &
\end{tikzcd} \tag{234}$$

is a long exact sequence of R-modules.

Proof. The proof will consists of three steps. The first step is to construct a graded function $\eth\colon \mathrm{H}(A'') \to \mathrm{H}(A')$ of degree -1 (graded here just means $\eth(\mathrm{H}_i(A'')) \subseteq \mathrm{H}_{i-1}(A')$ for all $i \in \mathbb{Z}$). The next step will be to show that $\eth$ is R-linear. The final step will be to show exactness of (245).

Step 1: We construct a graded function $\eth\colon \mathrm{H}(A'') \to \mathrm{H}(A')$ as follows: let $[a''] \in \mathrm{H}_i(A'')$. Choose a representative of the coset $[a'']$, say $a'' \in A''_i$ (so $\mathrm{d}''(a'') = 0$), and choose a lift of a'' in A_i with respect to ψ, say $a \in A_i$ (so $\psi(a) = a''$). We can make such a choice since ψ is surjective. Since

$$\begin{aligned}
\psi(\mathrm{d}(a)) &= \mathrm{d}''(\psi(a)) \\
&= \mathrm{d}''(a'') \\
&= 0,
\end{aligned}$$

it follows by exactness of (63.8.3) that there exists a unique $a' \in A'_{i-1}$ such that $\varphi(a') = \mathrm{d}(a)$. Observe that $\mathrm{d}'(a') = 0$ since φ is injective and since

$$\begin{aligned} \varphi(\mathrm{d}'(a')) &= \mathrm{d}(\varphi(a')) \\ &= \varphi(\mathrm{d}(a)) \\ &= 0. \end{aligned}$$

Thus a' represents an element in $\mathrm{H}_{i-1}(A')$. We define $\eth\colon \mathrm{H}(A'') \to \mathrm{H}(A')$ by

$$\eth[a''] = [a'].$$

We need to verify that $\eth$ is well-defined. There were two choices that we made in constructing $\eth$. The first choice was the choice of a representative of the coset $[a'']$. Let us consider another choice, say $a'' + \mathrm{d}''(b'')$ where $b'' \in A''_{i+1}$ (every representative of the coset $[a'']$ has this form for some $b'' \in A''_{i+1}$). The second choice that we made was the choice of a lift of a'' in A with respect to ψ. This time we have another coset representative of $[a'']$, so let $a + \varphi(b') + \mathrm{d}(b)$ be another choice of a lift of $a'' + \mathrm{d}''(b'')$ with respect to ψ where $b' \in A'_i$ and $b \in A_{i+1}$ (every such choice has this form for some $b' \in A'_i$ and $b \in A_{i+1}$). Now observe that

$$\begin{aligned} \psi\mathrm{d}(a + \varphi(b') + \mathrm{d}(b)) &= \psi\mathrm{d}(a) + \psi\mathrm{d}\varphi(b')) + \psi\mathrm{dd}(b) \\ &= \psi\mathrm{d}(a) + \psi\mathrm{d}\varphi(b')) \\ &= \psi\mathrm{d}(a) + \psi\varphi\mathrm{d}'(b') \\ &= \psi\mathrm{d}(a) \\ &= \mathrm{d}''\psi(a) \\ &= \mathrm{d}''(a'') \\ &= 0. \end{aligned}$$

Hence there exists a unique element in A'_{i-1} which maps to $\mathrm{d}(a + \varphi(b') + \mathrm{d}(b))$ with respect to φ, and since

$$\begin{aligned} \varphi(a' + \mathrm{d}'(b')) &= \varphi(a') + \varphi\mathrm{d}'(b') \\ &= \mathrm{d}(a) + \mathrm{d}\varphi(b') \\ &= \mathrm{d}(a + \varphi(b') + \mathrm{d}(b)), \end{aligned}$$

this unique element must be $a' + \mathrm{d}'(b')$. Therefore

$$\begin{aligned} \eth[a'' + \mathrm{d}''(b'')] &= [a' + \mathrm{d}'(b')] \\ &= [a'] \\ &= \eth[a''], \end{aligned}$$

which implies $\eth$ is well-defined. Moreover, we see that $\eth(\mathrm{H}(A_i)) \subseteq \mathrm{H}(A_{i-1})$, and is hence graded of degree -1. As usualy, we denote $\eth_i := \eth|_{A_i}$ for all $i \in \mathbb{Z}$.

Step 2: Let $i \in \mathbb{Z}$, let $\overline{a''}, \overline{b''} \in H(A'')$, and let $r, s \in R$. Choose a coset representative $\overline{a''}$ and $\overline{b''}$, say $a'' \in A''_i$ and $b'' \in A''_i$. Then $ra'' + sb''$ is a coset representative of $\overline{ra'' + sb''}$ (by linearity of taking quotients). Next, choose lifts of a'' and b'' in A_i under φ, say $a \in A_i$ and $b \in A_i$ respectively. Then $ra + sb$ is a lift of $ra'' + sb''$ in A_i under φ (by linearity of ψ). Finally, let a' and b' be the unique elements in A'_{i-1} such that $\varphi(a') = d(a)$ and $\varphi(b') = d(b)$. Then $ra' + sb'$ is the unique element in A'_{i-1} such that $\varphi(ra' + sb') = d(ra + sb)$ (by linearity of φ). Thus, we have

$$\begin{aligned} \eth(\overline{ra'' + sb''}) &= \overline{ra' + sb'} \\ &= r\overline{a'} + s\overline{b'} \\ &= r\eth(\overline{a''}) + s\eth(\overline{b''}). \end{aligned}$$

Step 3: To prove exactness of (245), it suffices to show exactness at $H_i(A'')$, $H_i(A)$, and $H_i(A')$. First we prove exactness at $H_i(A)$. Let $\overline{a} \in \mathrm{Ker}(H_i(\psi))$ (so $a \in A_i$, $d(a) = 0$, and $\overline{\psi(a)} = \overline{0}$). Lift $\psi(a) \in A''_i$ to an element $a'' \in A'_{i+1}$ under d'' (we can do this since $\overline{\psi(a)} = \overline{0}$). Lift $a'' \in A''_{i+1}$ to an element $b \in A_{i+1}$ under ψ (we can do this since ψ is surjective). Then

$$\begin{aligned} \psi(d(b) - a) &= \psi(d(b)) - \psi(a) \\ &= d''(a'') - \psi(a) \\ &= \psi(a) - \psi(a) \\ &= 0 \end{aligned}$$

implies $d(b) - a \in \operatorname{Ker}(\psi)$. Lift $d(b) - a$ to the unique element $a' \in A'_i$ under φ (we can do this exactness of (63.8.3)). Since φ is injective,

$$\begin{aligned} \varphi(d'(a')) &= d(\varphi(a')) \\ &= d(d(b) - a) \\ &= d(d(b)) - d(a)) \\ &= 0 \end{aligned}$$

implies $d'(a') = 0$. Hence a' represents an element in $H(A')$. Therefore

$$\begin{aligned} H_i(\varphi)(a') &= \overline{\varphi(a')} \\ &= \overline{d(b) - a} \\ &= \overline{a} \end{aligned}$$

implies $\overline{a} \in \operatorname{Im}(H_i(\varphi))$. Thus we have exactness at $H_i(A)$.

Next we show exactness at $H_i(A')$. Let $\overline{a'} \in \operatorname{Ker}(H_i(\varphi))$ (so $a' \in A'_i$, $d(a') = 0$, and $\overline{\varphi(a')} = \overline{0}$). Lift $\varphi(a') \in A_i$ to an element $a \in A'_{i+1}$ under d (we can do this since $\overline{\varphi(a)} = \overline{0}$). Then

$$\begin{aligned} d(\psi(a)) &= \psi(d(a)) \\ &= \psi(\varphi(a')) \\ &= 0. \end{aligned}$$

Hence $\psi(a)$ represents an element in $H_{i+1}(A'')$. By construction, we have $\eth(\overline{\psi(a)}) = \overline{a'}$, which implies $\overline{a'} \in \operatorname{Im}(\eth_{i+1})$. Thus we have exactness at $H_i(A')$.

Finally we show exactness at $H_i(A'')$. Let $\overline{a''} \in \operatorname{Ker}(\eth_i)$ (so $a'' \in A''_i$ and $d(a'') = 0$). Lift a'' to an element $a \in A_i$ under ψ. Lift $d(a)$ to the unique element a' in A'_{i-1} under φ. Lift a' to an element $b' \in A'_{i+1}$ under d (we can do this since $0 = \eth(\overline{a''}) = \overline{a'}$). Then

$$\begin{aligned} d(a - \varphi(b')) &= d(a) - d(\varphi(b')) \\ &= d(a) - \varphi(d(b')) \\ &= d(a) - \varphi(a') \\ &= 0, \end{aligned}$$

and hence $a - \varphi(b')$ represents an element in $H_i(A)$. Moreover, we have

$$\begin{aligned} H_i(\psi)(\overline{a - \varphi(b')}) &= \overline{\psi(a - \varphi(b'))} \\ &= \overline{\psi(a) - \psi(\varphi(b'))} \\ &= \overline{\psi(a)} \\ &= \overline{a''}, \end{aligned}$$

which implies $\overline{a'} \in \operatorname{Im}(H_i(\psi))$. Thus we have exactness at $H_i(A'')$. $\square$

Definition 63.11. Given a short exact sequence of R-complexes as in (63.8.3), we refer to the graded homomorphism $\eth\colon \mathrm{H}(A'') \to \mathrm{H}(A')$ of degree -1 as the **induced connecting map**.

63.5.2 When a Graded R-Linear Map is a Chain Map

Proposition 63.15. *Let (A, d) and (B, ∂) be R-complexes and let $\varphi\colon A \to B$ be a graded R-linear map of the underlying graded modules. Let $\overline{B} = B/\operatorname{im}(\partial\varphi - \varphi\mathrm{d})$ and let $\pi\colon B \to \overline{B}$ be the quotient map. Define $\overline{\partial}\colon \overline{B} \to \overline{B}$ by*

$$\overline{\partial}(\overline{b}) = \overline{\partial(b)}$$

for all $a \in A$ and $\overline{b} \in \overline{B}$. Then $(\overline{B}, \overline{\partial})$ is an R-complex and $\pi\varphi\colon A \to \overline{B}$ is a chain map. Moreover, if φ takes $\operatorname{im}\mathrm{d}$ to $\operatorname{im}\partial$, then we have the following short exact sequence of graded R-modules and graded R-linear maps:

$$0 \longrightarrow \mathrm{H}(B) \xrightarrow{\mathrm{H}(\pi)} \mathrm{H}(\overline{B}) \xrightarrow{\gamma} \operatorname{im}(\partial\varphi - \varphi\mathrm{d})(-1) \longrightarrow 0 \tag{235}$$

where γ is the connecting map coming from a long exact sequence in homology.

Proof. Observe that $\operatorname{im}(\partial\varphi - \varphi\mathrm{d})$ is a graded R-submodule of B since $\partial\varphi - \varphi\mathrm{d}$ is a graded R-linear map of degree -1, therefore the grading on B induces a grading on $\overline{B}$ which makes π into a graded R-linear map. Therefore $\pi\varphi$, being a composite of two graded R-linear maps, is a graded R-linear map. We need to check that $\overline{\partial}$ is well-defined, that is, we need to check that ∂ sends $\operatorname{im}(\partial\varphi - \varphi\mathrm{d})$ to itself. Let $(\partial\varphi - \varphi\mathrm{d})(a) \in \operatorname{im}(\partial\varphi - \varphi\mathrm{d})$ where $a \in A$. Then

$$\begin{aligned}
\partial(\partial\varphi - \varphi\mathrm{d})(a) &= (\partial\partial\varphi - \partial\varphi\mathrm{d})(a) \\
&= -\partial\varphi\mathrm{d}(a) \\
&= (-\partial\varphi\mathrm{d}(a) + \varphi\mathrm{d}\mathrm{d})(a) \\
&= (-\partial\varphi + \varphi\mathrm{d})(\mathrm{d}(a)) \in \operatorname{im}(\partial\varphi - \varphi\mathrm{d}).
\end{aligned}$$

Thus $\overline{\partial}$ is well-defined. Also $\overline{\partial}$ is an R-linear differential since it inherits these properties from ∂. Therefore $(\overline{B}, \overline{\partial})$ is an R-complex.

Now let us check that $\pi\varphi$ is a chain map. To see this, we just need to show it commutes with the differentials. Let $a \in A$. Then we have

$$\begin{aligned}
\overline{\partial}\pi\varphi(a) &= \overline{\partial}(\overline{\varphi(a)}) \\
&= \overline{\partial\varphi(a)} \\
&= \overline{\partial\varphi(a) - (\partial\varphi - \varphi\mathrm{d})(a)} \\
&= \overline{\partial\varphi(a) - \partial\varphi(a) + \varphi\mathrm{d}(a)} \\
&= \overline{\varphi\mathrm{d}(a)} \\
&= \pi\varphi\mathrm{d}(a).
\end{aligned}$$

Thus $\pi\varphi$ is a chain map.

Since ∂ sends $\operatorname{im}(\partial\varphi - \varphi\mathrm{d})$ to itself, it restricts to a differential on $\operatorname{im}(\partial\varphi - \varphi\mathrm{d})$. So we have a short exact sequence of R-complexes

$$0 \longrightarrow \operatorname{im}(\partial\varphi - \varphi\mathrm{d}) \xrightarrow{\iota} B \xrightarrow{\pi} \overline{B} \longrightarrow 0 \tag{236}$$

where ι is the inclusion map. The short exact sequence (236) induces the following long exact sequence in homology

$$\begin{tikzcd}
 & & \cdots \arrow[r] & \mathrm{H}_{i+1}(\overline{B}) \arrow[dlll, rounded corners, "\gamma_{i+1}"'] \\
\mathrm{H}_i(\operatorname{im}(\partial\varphi - \varphi\mathrm{d}) \arrow[r, "\mathrm{H}_i(\iota)"] & \mathrm{H}_i(B) \arrow[r, "\mathrm{H}_i(\pi)"] & \mathrm{H}_i(\overline{B}) \arrow[dll, rounded corners, "\gamma_i"'] & \\
\mathrm{H}_{i-1}(\operatorname{im}(\partial\varphi - \varphi\mathrm{d}) \arrow[r, "\mathrm{H}_{i-1}(\iota)"] & \mathrm{H}_{i-1}(B) \arrow[r] & \cdots &
\end{tikzcd} \tag{237}$$

Let us work out the details of the connecting map γ. Let $[\overline{b}] \in \mathrm{H}_i(\overline{B})$, so $\overline{b} \in \overline{B}_i$ is the coset with $b \in B_i$ as a reprsentative and $[\overline{b}] \in \mathrm{H}_i(\overline{B})$ is the coset with $\overline{b} \in \overline{B}_i$ as a representative. In particular, $\overline{\partial}(\overline{b}) = \overline{0}$, which implies

$$\partial(b) = (\partial\varphi - \varphi\mathrm{d})(a) \tag{238}$$

for some $a \in A$. Then (238) implies that $(\partial\varphi - \varphi\mathrm{d})(a)$ is the unique element in $\operatorname{im}(\partial\varphi - \varphi\mathrm{d})$ which maps to $\partial(b)$ (under the inclusion map). Therefore

$$\gamma_i[\overline{b}] = [(\partial\varphi - \varphi\mathrm{d})(a)].$$

Now suppose φ takes $\operatorname{im}\mathrm{d}$ to $\operatorname{im}\partial$. We claim that ∂ restricts to the zero map on $\operatorname{im}(\partial\varphi - \varphi\mathrm{d})$. Indeed, let $(\partial\varphi - \varphi\mathrm{d})(a) \in \operatorname{im}(\partial\varphi - \varphi\mathrm{d})$ where $a \in A$. Since φ takes $\operatorname{im}\mathrm{d}$ to $\operatorname{im}\partial$, there exists a $b \in B$ such that

$$\varphi\mathrm{d}(a) = \partial(b).$$

Choose such a $b \in B$. Then observe that

$$\begin{aligned}
\partial(\partial\varphi - \varphi\mathrm{d})(a) &= \partial\partial\varphi - \partial\varphi\mathrm{d}(a) \\
&= -\partial\varphi\mathrm{d}(a) \\
&= -\partial\partial(b) \\
&= 0.
\end{aligned}$$

Thus ∂ restricts to the zero map on $\mathrm{im}(\partial\varphi - \varphi\mathrm{d})$. In particular, $\mathrm{H}(\mathrm{im}(\partial\varphi - \varphi\mathrm{d})) \cong \mathrm{im}(\partial\varphi - \varphi\mathrm{d})$.

Next we claim that $\mathrm{H}(\iota)$ is the zero map. Indeed, for any $(\partial\varphi - \varphi\mathrm{d})(a) \in \mathrm{im}(\partial\varphi - \varphi\mathrm{d})$ where $a \in A$, we choose $b \in B$ such that $\varphi\mathrm{d}(a) = \partial(b)$, then we have

$$\begin{aligned}(\partial\varphi - \varphi\mathrm{d})(a) &= \partial\varphi(a) - \varphi\mathrm{d}(a)\\ &= \partial\varphi(a) - \partial b\\ &= \partial(\varphi(a) - b)\\ &\in \mathrm{im}\,\partial.\end{aligned}$$

Therefore $\mathrm{H}(\iota)$ takes the coset in $\mathrm{H}(\mathrm{im}(\partial\varphi - \varphi\mathrm{d}))$ represented by $(\partial\varphi - \varphi\mathrm{d})(a)$ to the coset in $\mathrm{H}(B)$ represented by 0. Thus $\mathrm{H}(\iota)$ is the zero map as claimed.

Combining everything together, we see that the long exact sequence (237) breaks up into short exact sequences

$$0 \longrightarrow \mathrm{H}_i(B) \xrightarrow{\mathrm{H}_i(\pi)} \mathrm{H}_i(\overline{B}) \xrightarrow{\gamma_i} \mathrm{im}(\partial_{i-1}\varphi_{i-1} - \varphi_{i-2}\mathrm{d}_{i-1}) \longrightarrow 0 \tag{239}$$

for all $i \in \mathbb{Z}$. In other words, (236) is a short exact sequence of graded R-modules.

□

63.6 Operations on R-Complexes

63.6.1 Product of R-complexes

63.6.2 Limits

Definition 63.12. Let $(\Lambda, \leq)$ be a preordered set. A system $(M_\lambda, \varphi_{\lambda\mu})$ of R-complexes and chain maps over Λ consists of a family of a family of R-complexes $\{(M_\lambda, \mathrm{d}_\lambda)\}$ indexed by Λ and a family of chain maps $\{\varphi_{\lambda\mu} \colon M_\lambda \to M_\mu\}_{\lambda \leq \mu}$ such that for all $\lambda \leq \mu \leq \kappa$,

$$\varphi_{\lambda\lambda} = 1_{M_\lambda} \quad \text{and} \quad \varphi_{\lambda\kappa} = \varphi_{\mu\kappa}\varphi_{\lambda\mu}.$$

We say $(M_\lambda, \varphi_{\lambda\mu})$ is a **directed system** if Λ is a directed set.

Proposition 63.16. *Let $(M_\lambda, \varphi_{\lambda\mu})$ be a system of R-complexes and chain maps over Λ. The limit of this system, denoted $\lim^\star M_\lambda$, is given by the R-complex $(\lim^\star M_\lambda, \lim^\star \mathrm{d}_\lambda)$ together with together with the projection maps*

$$\pi_\lambda \colon \overset{\star}{\lim} M_\lambda \to M_\lambda$$

for all $\lambda \in \Lambda$, where $\lim^\star M_\lambda$ is the graded R-module given by

$$\overset{\star}{\lim} M_\lambda = \left\{ (u_\lambda) \in \prod_{\lambda \in \Lambda}^{\star} M_\lambda \mid \varphi_{\lambda\kappa}(u_\lambda) = u_\mu \text{ for all } \lambda \leq \mu \right\}$$

and where the differential $\lim^\star \mathrm{d}_\lambda$ is defined pointwise:

$$(\overset{\star}{\lim} \mathrm{d}_\lambda)((u_\lambda)) = (\mathrm{d}_\lambda(u_\lambda))$$

for all $(u_\lambda) \in \lim^\star M_\lambda$.

Proof. We need ot show that $\lim^\star M_\lambda$ satisfies the universal mapping property. Let (M, ψ_λ) be compatible with respect to the system $(M_\lambda, \varphi_{\lambda\mu})$, so

$$\varphi_{\lambda\mu}\psi_\lambda = \psi_\mu$$

for all $\lambda \leq \mu$. By the universal mapping property of the graded limits, there exists a unique graded R-linear map $\psi \colon M \to \lim^\star M_\lambda$ of graded R-linear maps which commutes with all the arrows. It remains to show that ψ commutes with the differentials. Indeed, we have

$$\begin{aligned}(\overset{\star}{\lim} \mathrm{d}_\lambda \psi)(u) &= \overset{\star}{\lim} \mathrm{d}_\lambda((\psi_\lambda(u)))\\ &= (\mathrm{d}_\lambda(\psi_\lambda(u)))\\ &= (\psi_\lambda(\mathrm{d}(u)))\\ &= \psi(\mathrm{d}(u))\\ &= (\psi\mathrm{d})(u).\end{aligned}$$

for all $u \in M$. □

63.6.3 Localization

Let (A, d) be an R-complex and let S be a multiplicatively closed subset of R. The **localization of** (A, d) **with respect to** S is the R_S-complex (A_S, d_S) where A_S is the graded R_S-module whose component in degree i is

$$(A_S)_i = \{a/s \mid a \in A_i \text{ and } s \in S\}.$$

The differential d_S is defined as follows: if $a/s \in (A_S)_i$, then

$$\mathrm{d}_S(a/s) = \mathrm{d}(a)/s.$$

63.6.4 Direct Sum of R-Complexes

Definition 63.13. Let (A, d) and (A', d') be R-complexes. We define their **direct sum** to be the R-complex

$$(A, \mathrm{d}) \oplus_R (A', \mathrm{d}') := (A \oplus A', \mathrm{d} \oplus \mathrm{d}')$$

whose graded R-module $A \oplus A'$ has

$$(A \oplus A')_i = A_i \oplus A'_i$$

as its ith homogeneous component and whose differential $\mathrm{d} \oplus \mathrm{d}'$ is defined by

$$(\mathrm{d} \oplus \mathrm{d}')(a, a') = (\mathrm{d}(a), \mathrm{d}'(a'))$$

for all $(a, a') \in A \oplus A'$.

More generally, suppose $(A_\lambda, \mathrm{d}_\lambda)$ is an R-complex for each λ in some indexing set Λ. We define their **direct sum** to be the R-complex

$$\bigoplus_{\lambda \in \Lambda} (A_\lambda, \mathrm{d}_\lambda) := \left(\bigoplus_{\lambda \in \Lambda} A_\lambda, \bigoplus_{\lambda \in \Lambda} \mathrm{d}_\lambda \right).$$

It is easy to check that

$$\mathrm{H}\left(\bigoplus_{\lambda \in \Lambda} A_\lambda \right) \cong \bigoplus_{\lambda \in \Lambda} \mathrm{H}(A_\lambda).$$

In other words, homology commutes with direct sums.

63.6.5 Shifting an R-complex

We often find ourselves needing to shift the homological degree of an R-complex. To do this, we introduce the following definition:

Definition 63.14. Let A be an R-complex and let $n \in \mathbb{Z}$. We define the nth **shift** of A, denoted $\Sigma^n A$, to be the R-complex whose underlying graded R-module is $A(-n)$ and whose differential, when viewed as a map from A to A, is defined by

$$\mathrm{d}_{\Sigma^n A} = (-1)^n \Sigma^n \mathrm{d}_A \tag{240}$$

where $\Sigma^n \mathrm{d}_A$ is just the map $\mathrm{d}_A \colon A \to A$ but with the grading shifted down by n, that is, given $i \in \mathbb{Z}$, we have

$$\begin{aligned}
(\Sigma^n \mathrm{d}_A)_i &= (\Sigma^n \mathrm{d}_A)|_{A(-n)_i} && \text{(this is just an equality in notation)} \\
&:= \mathrm{d}_A|_{A_{i-n}} \\
&= (\mathrm{d}_A)_{i-n} && \text{(this is just an equality in notation)}
\end{aligned}$$

Technically speaking, the equality (240) is not correct in the category of graded R-modules. Indeed, in the category of graded R-modules, $\mathrm{d}_{\Sigma^n A}$ is a graded map of degree -1 from the graded R-module $\Sigma^n A$ to itself, whereas $(-1)^n \Sigma^n \mathrm{d}_A$ is a graded map of degree -1 from the graded R-module A to itself. The equality (240) only makes sense in the category of R-modules where we forget the grading.

Proposition 63.17. *Let A be an R-complex and let $n \in \mathbb{Z}$. Then*

$$\mathrm{H}(\Sigma^n A) = \mathrm{H}(A)(-n).$$

Proof. Indeed, let $i \in \mathbb{Z}$. Then we have

$$\begin{aligned}
\mathrm{H}_i(\Sigma^n A) &= \ker((\mathrm{d}_{\Sigma^n A})_i) / \operatorname{im}((\mathrm{d}_{\Sigma^n A})_{i+1}) \\
&= \ker((\mathrm{d}_A)_{i-n}) / \operatorname{im}((\mathrm{d}_A)_{i+1-n}) \\
&= \mathrm{H}_{i-n}(A).
\end{aligned}$$

It follows that $\mathrm{H}(\Sigma^n A) = \mathrm{H}(A)(-n)$. □

63.7 The Mapping Cone

Definition 63.15. Let $\varphi\colon A \to B$ be a chain map. The **mapping cone of** φ, denoted $\mathrm{C}(\varphi)$, is the R-complex whose underlying graded R-module is $\mathrm{C}(\varphi) = B \oplus A(-1)$ and whose differential is defined by

$$\mathrm{d}_{\mathrm{C}(\varphi)}(b,a) := (\mathrm{d}_B(b) + \varphi(a), -\mathrm{d}_A(a))$$

for all $(b,a) \in B \oplus A(-1)$.

Remark 114. To see that we are justified in calling $\mathrm{C}(\varphi)$ an R-complex, let us check that $\mathrm{d}_{\mathrm{C}(\varphi)}\mathrm{d}_{\mathrm{C}(\varphi)} = 0$. Let $(b,a) \in C(\varphi)$. Then we have

$$\begin{aligned}
\mathrm{d}_{\mathrm{C}(\varphi)}\mathrm{d}_{\mathrm{C}(\varphi)}(b,a) &= \mathrm{d}_{\mathrm{C}(\varphi)}(\mathrm{d}_B(b) + \varphi(a), -\mathrm{d}_A(a)) \\
&= (\mathrm{d}_B(\mathrm{d}_B(b) + \varphi(a)) + \varphi(-\mathrm{d}_A(a)), -\mathrm{d}_A\mathrm{d}_A(a)) \\
&= (\mathrm{d}_B\varphi(a) - \varphi\mathrm{d}_A(a), 0) \\
&= (0,0).
\end{aligned}$$

63.7.1 Turning a Chain Map Into a Connecting Map

Theorem 63.3. *Let $\varphi\colon A \to B$ be a chain map. Then we have a short exact sequence of R-complexes*

$$0 \longrightarrow B \xrightarrow{\iota} \mathrm{C}(\varphi) \xrightarrow{\pi} \Sigma A \longrightarrow 0 \tag{241}$$

where $\iota\colon B \to \mathrm{C}(\varphi)$ is the inclusion map given by

$$\iota(b) = (b,0)$$

for all $b \in B$, and where $\pi\colon \mathrm{C}(\varphi) \to \Sigma A$ is the projection map given by

$$\pi(b,a) = a$$

for all $(b,a) \in \mathrm{C}(\varphi)$. Moreover the connecting map $\eth\colon \mathrm{H}(\Sigma A) \to \mathrm{H}(B)$ induced by (241) agrees with $\mathrm{H}(\varphi)$.

Proof. It is straightforward to check that (241) is a short exact sequence of R-complexes. Let us show that the connecting map agrees with $\mathrm{H}(\varphi)$. Let $i \in \mathbb{Z}$ and let $\overline{a} \in \mathrm{H}_i(\Sigma A)$. Thus $a \in A_i$ and $\mathrm{d}_A(a) = 0$. Lift $a \in A_i$ to the element $(0,a) \in \mathrm{C}_i(\varphi)$. Now apply $\mathrm{d}_{\mathrm{C}(\varphi)}$ to $(0,a)$ to get $(\varphi(a),0) \in \mathrm{C}_{i-1}(\varphi)$. Then $\varphi(a)$ is the unique element in B_{i-1} which maps to $(\varphi(a),0)$ under d_B. Therefore

$$\begin{aligned}
\eth(\overline{a}) &= \overline{\varphi(a)} \\
&= \mathrm{H}(\varphi)(\overline{a}).
\end{aligned}$$

It follows that $\eth$ and $\mathrm{H}(\varphi)$ agree on all of $\mathrm{H}(A)$. □

Remark 115. In the context of graded R-modules, it would be incorrect to say $\eth = \mathrm{H}(\varphi)$. This is because $\eth$ is graded of degree -1 and $\mathrm{H}(\varphi)$ is graded of degree 0. On the other hand, it would be correct to say $\eth_i = \mathrm{H}_{i-1}(\varphi)$ for all $i \in \mathbb{Z}$.

63.7.2 Quasiisomorphism and Mapping Cone

Corollary 66. *Let $\varphi\colon A \to B$ be a chain map. Then φ is a quasiisomorphism if and only if $\mathrm{C}(\varphi)$ is an exact complex.*

Proof. Suppose $\mathrm{C}(\varphi)$ is an exact complex, so $\mathrm{H}(\mathrm{C}(\varphi)) \cong 0$. Then for each $i \in \mathbb{Z}$, the long exact sequence induced by (241) gives us

$$0 \cong \mathrm{H}_{i+1}(\mathrm{C}(\varphi)) \xrightarrow{\mathrm{H}(\pi)} \mathrm{H}_i(A) \xrightarrow{\mathrm{H}(\varphi)} \mathrm{H}_i(B) \xrightarrow{\mathrm{H}(\iota)} \mathrm{H}_i(\mathrm{C}(\varphi)) \cong 0$$

which implies $\mathrm{H}_i(A) \cong \mathrm{H}_i(B)$ for all $i \in \mathbb{Z}$.

Conversely, suppose φ is a quaisiisomorphism. Then for each $i \in \mathbb{Z}$, the long exact sequence induced by (241) gives us

$$\mathrm{H}_i(A) \cong \mathrm{H}_i(B) \xrightarrow{\mathrm{H}(\iota)} \mathrm{H}_i(\mathrm{C}(\varphi)) \xrightarrow{\mathrm{H}(\pi)} \mathrm{H}_{i-1}(A) \cong \mathrm{H}_{i-1}(B)$$

which implies $\mathrm{H}_i(\mathrm{C}(\varphi)) \cong 0$ for all $i \in \mathbb{Z}$. □

Proposition 63.18. *Let*

$$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0 \tag{242}$$

be a short exact sequence of R-complexes. Then C is quasi-isomorphic to the mapping cone of $\varphi\colon A \to B$. Similarly, A is quasi-isomorphic to the mapping cone of $\psi\colon B \to C$.

Proof. We will just show that C is quasi-isomorphic to the mapping cone of $\varphi\colon A \to B$ since the argument that A is quasi-isomorphic to the mapping cone of $\psi\colon B \to C$ is essentially the same
. Let $B + eA$ be the mapping cone of $\varphi\colon A \to B$. Define $\widetilde{\psi}\colon B + eA \to C$ by $\widetilde{\psi}(b + ea) = \psi(b)$ for all $a \in A$ and $b \in B$. Then $\widetilde{\psi}$ is a chain map since $\psi\varphi = 0$. The kernel of $\widetilde{\psi}$ is given by $\varphi A + eA = \{\varphi a + ea' \mid a, a' \in A\}$. Note that $\varphi A + eA$ is exact: to see this, suppose

$$\begin{aligned} \mathrm{d}(\varphi a + ea') = 0 &\iff \varphi(\mathrm{d}a - a') \text{ and } \mathrm{d}a' = 0 \\ &\iff \mathrm{d}a = a', \end{aligned}$$

where the last if and only if follows from the fact that φ is injective. Thus, taking the long exact sequence in homology of the short exact sequence

$$0 \longrightarrow \varphi A + eA \longrightarrow B + eA \xrightarrow{\widetilde{\psi}} C \longrightarrow 0 \tag{243}$$

and using the fact that $\mathrm{H}(\varphi A + eA) = 0$, we see that $\widetilde{\psi}\colon B + eA \to C$ induces isomorphisms in homology, i.e. $\widetilde{\psi}$ is a quasi-isomorphism. □

63.7.3 Translating Mapping Cone With Isomorphisms

Proposition 63.19. *Suppose we have a commutative diagram of R-complexes*

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "\varphi"'] & B \arrow[d, "\psi"] \\ A' \arrow[r, "\phi'"'] & B' \end{tikzcd}$$

where $\phi\colon A \to B$ and $\phi'\colon A' \to B'$ are isomorphisms. Then we have an isomorphism $\mathrm{C}(\varphi) \cong \mathrm{C}(\psi)$ of R-complexes.

Proof. Define $\phi' \oplus \phi\colon \mathrm{C}(\varphi) \to \mathrm{C}(\psi)$ by

$$(\phi' \oplus \phi)(a', a) = (\phi'(a'), \phi(a))$$

for all $(a', a) \in \mathrm{C}(\varphi)$. Clearly $\phi' \oplus \phi$ is an isomorphism of the underlying graded R-modules. To see that it is an isomorphism of R-complexes, we need to check that it commutes with the differentials. Let $(a', a) \in \mathrm{C}(\varphi)$. We have

$$\begin{aligned} \mathrm{d}_{\mathrm{C}(\psi)}(\phi' \oplus \phi)(a', a) &= \mathrm{d}_{\mathrm{C}(\psi)}(\phi'(a'), \phi(a)) \\ &= (\mathrm{d}_{B'}\phi'(a') + \psi\phi(a), -\mathrm{d}_B\phi(a)) \\ &= (\mathrm{d}_{B'}\phi'(a') + \psi\phi(a), -\mathrm{d}_B\phi(a)) \\ &= (\phi'\mathrm{d}_{A'}(a') + \phi'\varphi(a), -\phi\mathrm{d}_A(a)) \\ &= (\phi' \oplus \phi)(\mathrm{d}_{A'}(a') + \varphi(a), -\mathrm{d}_A(a)) \\ &= (\phi' \oplus \phi)\mathrm{d}_{\mathrm{C}(\varphi)}(a', a). \end{aligned}$$

□

63.7.4 Resolutions by Mapping Cones

Lemma 63.4. *(Lifting Lemma) Let $\varphi\colon M \to M'$ be an R-module homomorphism, let (P, d) be a projective resolution of M, and let (P', d') be a projective resolution of M'. Then there exists a chain map $\varphi\colon (P, d) \to (P', d')$ such that*

$$\begin{tikzcd} H_0(P) \arrow[r, "H_0(\varphi)"] \arrow[d, "\cong"] & H_0(P') \arrow[d, "\cong"] \\ M \arrow[r, "\varphi"] & M' \end{tikzcd}$$

Proof. For each $i > 0$, let $M'_i := \mathrm{Im}(d'_i)$ and let $M_i := \mathrm{Im}(d_i)$. We build a chain map $\varphi\colon (P, d) \to (P', d')$ by constructing R-module homomorphism $\varphi_i\colon P_i \to P'_i$ which commute with the differentials using induction on $i \geq 0$.

First consider the base case $i = 0$. Let $\psi_0\colon P_0 \to P'_0/M'_0$ be the composition

$$P_0 \to P_0/M_1 \cong M \to M' \cong P'_0/M'_1.$$

Since P_0 is projective and since $d'_0\colon P'_0 \to P'_0/M_1$ is a surjective homomorphism, we can lift $\psi_0\colon P_0 \to P'_0/M'_0$ along $d'_0 : P'_0 \to P'_0/M_1$ to a homomorphism $\varphi_0\colon P_0 \to P'_0$ such that $d'_0\varphi_0 = \psi_0$.

Now suppose for some $i > 0$ we have constructedn an R-module homomorphism $\varphi_i\colon P_i \to P'_i$ such that

$$d'_i\varphi_i = \varphi_{i-1}d_i.$$

We need to construct an R-module homomorphism $\varphi_{i+1}\colon P_{i+1} \to P'_{i+1}$ such that

$$d'_{i+1}\varphi_{i+1} = \varphi_i d_{i+1}.$$

First, observe that $\mathrm{Im}(\varphi_i d_{i+1}) \subseteq M'_{i+1}$. Indeed, we have

$$\begin{aligned} d'_i\varphi_i d_{i+1} &= \varphi_{i-1}d_i d_{i+1} \\ &= 0, \end{aligned}$$

Thus, since (P', d') is exact for all $i > 0$, we have

$$\begin{aligned} \mathrm{Im}(\varphi_i d_{i+1}) &\subseteq \mathrm{Ker}(d'_i) \\ &= \mathrm{Im}(d'_{i+1}) \\ &= M'_{i+1}. \end{aligned}$$

Now since P_{i+1} is projective and $d'_{i+1}\colon P_{i+1} \to M_{i+1}$ is surjective, we can lift $\varphi_i d_{i+1} : P_{i+1} \to M'_{i+1}$ along $d'_{i+1} : P'_{i+1} \to M'_{i+1}$ to a homomorphism $\varphi_{i+1}\colon P_{i+1} \to P'_{i+1}$ such that

$$d'_{i+1}\varphi_{i+1} = \varphi_i d_{i+1}.$$

The last part of the lemma, follows from the way φ_0 was constructed.

□

Theorem 63.5. *With the notation as above, the following hold:*

1. *if φ is injective, then $\mathrm{C}(\varphi)$ is a projective resolution of $M'/\mathrm{im}\,\varphi$.*
2. *if φ is surjective, then $\Sigma\mathrm{C}(\varphi)$ is a projective resolution of* $\ker\varphi$.

Proof. First note that the underlying graded R-module of $\mathrm{C}(\varphi)$ is projective since it is a direct sum of projective modules. Now we first consider the case where φ is injective. The short exact sequence

$$0 \longrightarrow P' \xrightarrow{\iota} \mathrm{C}(\varphi) \xrightarrow{\pi} \Sigma P \longrightarrow 0 \tag{244}$$

induces the long exact sequence

$$\begin{tikzcd} & & \cdots \arrow[r] & \mathrm{H}_i(P) \arrow[dll, "\mathrm{H}_i(\varphi)"] \\ \mathrm{H}_i(P') \arrow[r, "\mathrm{H}_i(\iota)"] & \mathrm{H}_i(\mathrm{C}(\varphi)) \arrow[r, "\mathrm{H}_i(\pi)"] & \mathrm{H}_{i-1}(P) \arrow[dll, "\mathrm{H}_{i-1}(\varphi)"] & \\ \mathrm{H}_{i-1}(P') \arrow[r] & \cdots & & \end{tikzcd} \tag{245}$$

This gives us $\mathrm{H}_i(\mathrm{C}(\varphi))$ for all $i > 1$ since $\mathrm{H}_i(P') \cong 0 \cong \mathrm{H}_i(P)$ for all $i \geq 1$. For $i = 1$, we get the exact sequence

$$0 \longrightarrow \mathrm{H}_1(\mathrm{C}(\varphi)) \longrightarrow M \xrightarrow{\varphi} M' \tag{246}$$

Then φ being injective implies $\mathrm{H}_1(\mathrm{C}(\varphi)) \cong 0$. Finally, for $i = 0$, we get the short exact sequence

$$0 \longrightarrow M \xrightarrow{\varphi} M' \longrightarrow \mathrm{H}_0(\mathrm{C}(\varphi)) \longrightarrow 0 \tag{247}$$

This implies $\mathrm{H}_0(\mathrm{C}(\varphi)) \cong M'/\mathrm{im}\,\varphi$.

Now we consider the case where φ is surjective. We still get $\mathrm{H}_i(\mathrm{C}(\varphi))$ for all $i > 1$ since $\mathrm{H}_i(P') \cong 0 \cong \mathrm{H}_i(P)$ for all $i \geq 1$. For $i = 1$, we get again get the exact sequence (246), but this time we conclude that $\mathrm{H}_1(\mathrm{C}(\varphi)) \cong \ker\varphi$ since φ is surjective. Similarly, for $i = 0$, we again get the short exact sequence (247), but this time we conclude $\mathrm{H}_0(\mathrm{C}(\varphi)) \cong 0$ since φ is surjective. □

Example 63.1. Let $S = K[x_1, \dots, x_n]$, let $I_{\mathcal{P}}$ be the permutohedron ideal in S, and let $I_{\mathcal{A}}$ be the associahedron ideal in S. Then there are natural free resolution $F_{\mathcal{P}} \xrightarrow{\tau_{\mathcal{P}}} S/I_{\mathcal{P}}$ and $F_{\mathcal{A}} \xrightarrow{\tau_{\mathcal{A}}} S/I_{\mathcal{A}}$ over S where $F_{\mathcal{P}}$ is supported by the permutohedron and $F_{\mathcal{A}}$ is supported by the associahedron. The inclusion of ideals $I_{\mathcal{A}} \subset I_{\mathcal{P}}$ induces a surjective S-linear map $\varphi\colon S/I_{\mathcal{A}} \to S/I_{\mathcal{P}}$ whose kernel is given by $I_{\mathcal{P}}/I_{\mathcal{A}}$. Lift $\varphi\tau_{\mathcal{A}}$ to a chain map $\widetilde{\varphi}\colon F_{\mathcal{A}} \to F_{\mathcal{P}}$ with respect to $\tau_{\mathcal{P}}$, so $\tau_{\mathcal{P}}\widetilde{\varphi} = \varphi\tau_{\mathcal{A}}$. It follows from Theorem (63.5) that $\Sigma\mathrm{C}(\widetilde{\varphi})$ is a free resolution of $I_{\mathcal{P}}/I_{\mathcal{A}}$ over S.

63.7.5 Split complexes

Definition 63.16. Let (C, d) be an R-complex. We say C is **split** if there exists a graded R-module $s\colon C \to C$ of degree 1 such that $\mathrm{d}s\mathrm{d} = \mathrm{d}$. In this case, we say s **splits** C or is a **splitting map** of C.

Proposition 63.20. *Let (C, d) be a split complex with splitting map $s\colon C \to C$. Then C is isomorphic to the mapping cone of the inclusion map $\iota\colon \mathrm{im}\,\mathrm{d} \to \ker\mathrm{d}$, where $\mathrm{im}\,\mathrm{d}$ and $\ker\mathrm{d}$ are viewed as complexes with the differentials in each case being the zero map.*

Proof. Consider the short exact sequence of graded R-modules:

$$0 \longrightarrow \ker\mathrm{d} \hookrightarrow C \xrightarrow{\mathrm{d}} \Sigma(\mathrm{im}\,\mathrm{d}) \longrightarrow 0 \tag{248}$$

The identity $\mathrm{d}s\mathrm{d} = \mathrm{d}$ says the graded R-module homomorphism $s\colon \Sigma(\mathrm{im}\,\mathrm{d}) \to C$ splits (248) to the right. Therefore the short exact sequence of graded R-modules (248) is isomorphic to the following short exact sequence of graded R-modules

$$0 \longrightarrow \ker\mathrm{d} \hookrightarrow \mathrm{C}(\iota) \xrightarrow{\pi} \Sigma(\mathrm{im}\,\mathrm{d}) \longrightarrow 0 \tag{249}$$

where $\mathrm{C}(\iota) = \ker\mathrm{d} \oplus \Sigma(\mathrm{im}\,\mathrm{d})$. The isomorphism $\theta\colon C \to \mathrm{C}(\iota)$ is given by

$$\theta(c) = (c - s\mathrm{d}(c), \mathrm{d}(c))$$

for all $c \in C$. We claim that $\theta\colon C \to \mathrm{C}(\iota)$ is not just an isomorphism of graded R-modules, but in fact it is an isomorphism of R-complexes. To see this, we just need to show that θ commutes with the differentials: for all $c \in C$ we have

$$\begin{aligned}
\mathrm{d}_{\mathrm{C}(\iota)}\theta(c) &= \mathrm{d}_{\mathrm{C}(\iota)}(c - s\mathrm{d}(c), \mathrm{d}(c)) \\
&= (\mathrm{d}(c - s\mathrm{d}(c)) + \mathrm{d}(c), 0) \\
&= (\mathrm{d}(c), 0) \\
&= \theta\mathrm{d}(c).
\end{aligned}$$

□

63.8 Tensor Products

63.8.1 Definition of tensor product

Definition 63.17. Let (A, d) and (A', d') be two R-complexes. Their **tensor product** is the R-complex $(A \otimes_R A', \mathrm{d}^{\otimes}_{(A,A')})$, where the graded R-module $A \otimes_R A'$ has

$$(A \otimes_R A')_i = \bigoplus_{j \in \mathbb{Z}} A_j \otimes A'_{j-i}$$

as its ith homogeneous component and whose differential is defined on elementary homogeneous tensors (and extended linearly) by

$$\mathrm{d}^{\otimes}_{(A,A')}(a \otimes a') = \mathrm{d}(a) \otimes a' + (-1)^i a \otimes \mathrm{d}'(a')$$

for all $a \in A_i$, $a' \in A_j$ and $i, j \in \mathbb{Z}$.

Proposition 63.21. *The map $\mathrm{d}^{\otimes}_{(A,A')}$ is well-defined and is in fact a differential.*

Proof. First we observe that $\mathrm{d}^{\otimes}_{(A,A')}$ is a well-defined R-linear map because the map $A_i \times A'_j \to A_i \otimes_R A'_j$ given by

$$(a, a') \mapsto \mathrm{d}(a) \otimes a' + (-1)^i a \otimes \mathrm{d}'(a')$$

for all $(a, a') \in A_i \times A'_j$ is R-bilinear for each $i, j \in \mathbb{Z}$. Next we observe that $\mathrm{d}^{\otimes}_{(A,A')}$ is graded of degree -1. Indeed, if $a \otimes a' \in A_j \otimes_R A'_{i-j}$, then

$$\mathrm{d}(a) \otimes a' + (-1)^i a \otimes \mathrm{d}'(a') \in A_{j-1} \otimes_R A'_{i-j} + A_j \otimes_R A_{i-j-1}.$$

Lastly we observe that $\mathrm{d}^{\otimes}_{(A,A')}\mathrm{d}^{\otimes}_{(A,A')} = 0$ since if $a \otimes a' \in (A \otimes_R A')_k$ where $a \in A_i$ and $a' \in A'_j$, then

$$\begin{aligned}
\mathrm{d}^{\otimes}_{(A,A')}\mathrm{d}^{\otimes}_{(A,A')}(a \otimes a') &= \mathrm{d}^{\otimes}_{(A,A')}(\mathrm{d}(a) \otimes a' + (-1)^i a \otimes \mathrm{d}'(a')) \\
&= \mathrm{d}^{\otimes}_{(A,A')}(\mathrm{d}(a) \otimes a') + (-1)^i \mathrm{d}^{\otimes}_{(A,A')}(a \otimes \mathrm{d}'(a')) \\
&= \mathrm{d}\mathrm{d}(a) \otimes a' + (-1)^{i-1}\mathrm{d}(a) \otimes \mathrm{d}'(a') + (-1)^i(\mathrm{d}(a) \otimes \mathrm{d}'(a') + (-1)^i a \otimes \mathrm{d}'\mathrm{d}'(a')) \\
&= (-1)^{i-1}\mathrm{d}(a) \otimes \mathrm{d}'(a') + (-1)^i \mathrm{d}(a) \otimes \mathrm{d}'(a') \\
&= 0.
\end{aligned}$$

□

63.8.2 Commutativity of tensor products

Proposition 63.22. *Let A and B be R-complexes. Then we have an isomorphism of R-complexes*

$$A \otimes_R B \cong B \otimes_R A, \tag{250}$$

which is natural in A and B.

Proof. We define $\tau_{A,B} \colon A \otimes_R B \to B \otimes_R A$ on elementary homogeneous tensors (and extend linearly) by

$$\tau_{A,B}(a \otimes b) = (-1)^{ij} b \otimes a$$

for all $a \otimes b \in A_i \otimes_R B_j$. The map $\tau_{A,B}$ is easily seen to be a well-defined graded R-linear isomorphism. To see that $\tau_{A,B}$ is an isomorphism of R-complexes, we need to show that it commutes with the differentials. That is, we need to show

$$\tau_{A,B}\mathrm{d}^{\otimes}_{(A,B)} = \mathrm{d}^{\otimes}_{(B,A)}\tau_{A,B} \tag{251}$$

It suffices to check (251) on elementary homogeneous tensors, so let $a \otimes b \in A_i \otimes_R B_j$ be such an elementary homogeneous tensor. Then we have

$$\begin{aligned}
\mathrm{d}^{\otimes}_{(B,A)}\tau_{A,B}(a \otimes b) &= (-1)^{ij}\mathrm{d}^{\otimes}_{(B,A)}(b \otimes a) \\
&= (-1)^{ij}\mathrm{d}_B(b) \otimes a + (-1)^{j+ij} b \otimes \mathrm{d}_A(a)) \\
&= (-1)^{i+i(j-1)}\mathrm{d}_B(b) \otimes a + (-1)^{(i-1)j} b \otimes \mathrm{d}_A(a) \\
&= (-1)^{(i-1)j} b \otimes \mathrm{d}_A(a) + (-1)^{i+i(j-1)}\mathrm{d}_B(b) \otimes a \\
&= \tau_{A,B}(\mathrm{d}_A(a) \otimes b + (-1)^i a \otimes \mathrm{d}_B(b)) \\
&= \tau_{A,B}\mathrm{d}^{\otimes}_{(A,B)}(a \otimes b).
\end{aligned}$$

Finally, being natural in A and B means that if $\varphi \colon A \to A'$ and $\psi \colon B \to B'$ are two chain maps, then the following diagram commutes:

$$\begin{array}{ccc}
A \otimes_R B & \xrightarrow{\varphi \otimes_R B} & A' \otimes_R B \\
{\scriptstyle A \otimes_R \psi}\downarrow & & \downarrow{\scriptstyle A' \otimes_R \psi} \\
A \otimes_R B' & \xrightarrow[\varphi \otimes_R B']{} & A' \otimes_R B'
\end{array}$$

We leave it as an exercise for the reader to check that this diagram commutes. □

63.8.3 Associativity of tensor products

Given that the proof of tensor products of R-complexes was nontrivial, we need to be sure that we have associativity of tensor products of R-complexes. The proof in this case turns out to be trivial.

Proposition 63.23. *Let A, A', and A'' be R-complexes. Then we have an isomoprhism of R-complexes*

$$(A \otimes_R A') \otimes_R A'' \cong A \otimes_R (A' \otimes_R A''),$$

which is natural in A, A', and A''.

Proof. Let $\eta_{A,A',A''} \colon (A \otimes_R A') \otimes_R A'' \to A \otimes_R (A' \otimes_R A'')$ to be the unique graded isomorphism such that

$$\eta_{A,A',A''}((a \otimes a') \otimes a'') = a \otimes (a' \otimes a'')$$

for all $a \in A_i$, $a' \in A'_j$, and $a'' \in A''_k$ and for all $i, j, k \in \mathbb{Z}$. To see that $\eta_{A,A',A''}$ is an isomorphism of R-complexes, we need to show that

$$\eta_{A,A',A''} \mathrm{d}^{\otimes}_{((A \otimes_R A'),A'')} = \mathrm{d}^{\otimes}_{(A,(A' \otimes_R A''))} \eta_{A,A',A''} \tag{252}$$

It suffices to check (252) on elementary homogeneous tensors. Let $(a \otimes a') \otimes a'' \in (A_i \otimes_R A_j) \otimes_R A_k$. To simplify the notation in our calculation, we denote $\eta = \eta_{A,A',A''}$. We have

$$\begin{aligned}
\mathrm{d}^{\otimes}_{(A,(A' \otimes_R A''))} \eta((a \otimes a') \otimes a'') &= \mathrm{d}^{\otimes}_{(A,(A' \otimes_R A''))}(a \otimes (a' \otimes a'')) \\
&= \mathrm{d}_A(a) \otimes (a' \otimes a'') + (-1)^i a \otimes \mathrm{d}^{\otimes}_{(A',A'')}(a' \otimes a'') \\
&= \mathrm{d}_A(a) \otimes (a' \otimes a'') + (-1)^i a \otimes (\mathrm{d}_{A'}(a') \otimes a'' + (-1)^j a' \otimes \mathrm{d}_{A''}(a'')) \\
&= \mathrm{d}_A(a) \otimes (a' \otimes a'') + (-1)^i a \otimes (\mathrm{d}_{A'}(a') \otimes a'') + (-1)^{i+j} a \otimes (a' \otimes \mathrm{d}_{A''}(a'')) \\
&= \eta((\mathrm{d}_A(a) \otimes a') \otimes a'') + (-1)^i \eta((a \otimes \mathrm{d}_{A'}(a')) \otimes a'') + (-1)^{i+j} \eta((a \otimes a') \otimes \mathrm{d}_{A''}(a'')) \\
&= \eta((\mathrm{d}_A(a) \otimes a') \otimes a'' + (-1)^i (a \otimes \mathrm{d}_{A'}(a')) \otimes a'' + (-1)^{i+j} (a \otimes a') \otimes \mathrm{d}_{A''}(a'')) \\
&= \eta(\mathrm{d}^{\otimes}_{(A,A')}(a \otimes a') \otimes a'' + (-1)^{i+j} (a \otimes a') \otimes \mathrm{d}_{A''}(a'')) \\
&= \eta \mathrm{d}^{\otimes}_{((A \otimes_R A'),A'')}((a \otimes a') \otimes a'').
\end{aligned}$$

Therefore (252) holds, and thus $\eta_{A,A',A''}$ is an isomorphism of R-complexes.

Naturality in A, A', and A'' means that if $\varphi \colon A \to B$, $\varphi \colon A' \to B'$, and $\varphi \colon A'' \to B''$ are chains maps, then we have a commutative diagram

$$\begin{tikzcd}
(A \otimes_R A')_R \otimes A'' \arrow[r, "\eta_{A,A',A''}"] \arrow[d, "(\varphi \otimes \varphi') \otimes \varphi''"'] & A \otimes_R (A'_R \otimes A'') \arrow[d, "\varphi \otimes (\varphi' \otimes \varphi'')"] \\
(B \otimes_R B')_R \otimes B'' \arrow[r, "\eta_{B,B',B''}"] & (B \otimes_R B')_R \otimes B''
\end{tikzcd}$$

□

63.8.4 Tensor Commutes with Shifts

Proposition 63.24. *Let $n \in \mathbb{Z}$ and let A and A' be R-complexes. Then*

$$(\Sigma^n A) \otimes_R A' \cong \Sigma^n (A \otimes_R A') \cong A \otimes_R (\Sigma^n A')$$

are isomorphisms of R-complexes.

Proof. We will just show that $(\Sigma^n A) \otimes_R A' \cong \Sigma^n (A \otimes_R A')$. The other isomorphism follows from a similar argument. As graded R-modules, we have

$$\begin{aligned}
(\Sigma^n A) \otimes_R A' &= A(-n) \otimes_R A' \\
&= (A \otimes_R A')(-n) \\
&= \Sigma^n (A \otimes_R A').
\end{aligned}$$

We define $\Phi \colon (\Sigma^n A) \otimes_R A' \to \Sigma^n (A \otimes_R A')$ by

$$\Phi(a \otimes a') = a \otimes a'$$

for all elementary tensors $a \otimes a' \in \Sigma^n A \otimes_R A'$. Then Φ is a graded isomorphism of the underlying graded R-module. We claim that it also commutes with the differentials, making it into an isomorphism of R-complexes. Indeed, let $a \otimes a' \in (\Sigma^n A) \otimes_R A'$ with $a \in A_i$ and $a' \in A_j$. Then $a \in (\Sigma^n A)_{i+n}$, and so we have

$$\begin{aligned}
(\Sigma^n \mathrm{d}^{\otimes}_{(A,A')}\Phi)(a \otimes a') &= (-1)^n \mathrm{d}^{\otimes}_{(A,A')}(\Phi(a \otimes a')) \\
&= (-1)^n \mathrm{d}^{\otimes}_{(A,A')}(a \otimes a') \\
&= (-1)^n \mathrm{d}^{\otimes}_{(A,A')}(a \otimes a') \\
&= (-1)^n (\mathrm{d}_A(a) \otimes a' + (-1)^i a \otimes \mathrm{d}_{A'}(a')) \\
&= (-1)^n \mathrm{d}_A(a) \otimes a' + (-1)^{i+n} a \otimes \mathrm{d}_{A'}(a') \\
&= \mathrm{d}_{\Sigma^n A}(a) \otimes a' + (-1)^{i+n} a \otimes \mathrm{d}_{A'}(a') \\
&= \Phi(\mathrm{d}_{\Sigma^n A}(a) \otimes a' + (-1)^{i+n} a \otimes \mathrm{d}_{A'}(a')) \\
&= \Phi(\mathrm{d}^{\otimes}_{(\Sigma^n A,A')}(a \otimes a')) \\
&= (\Phi \mathrm{d}^{\otimes}_{(\Sigma^n A,A')})(a \otimes a')
\end{aligned}$$

□

63.8.5 Tensor Commutes with Mapping Cone

Proposition 63.25. *Let X be an R-complex and let $\varphi \colon A \to A'$ be a chain map of R-complexes. Then*

$$\mathrm{C}(\varphi) \otimes_R X \cong \mathrm{C}(\varphi \otimes_R X)$$

is an isomorphism of R-complexes.

Proof. As graded R-modules, we have

$$\begin{aligned}
\mathrm{C}(\varphi) \otimes_R X &= (A' \oplus A(-1)) \otimes_R X \\
&\cong (A' \otimes_R X) \oplus (A(-1) \otimes_R X) \\
&= (A' \otimes_R X) \oplus (A \otimes_R X)(-1) \\
&= \mathrm{C}(\varphi \otimes_R X),
\end{aligned}$$

where the graded isomorphism in the second line is given by

$$(a', a) \otimes x \mapsto (a' \otimes x, a \otimes x)$$

for all elementary tensors $(a', a) \otimes x \in (A' \oplus A(-1)) \otimes_R X$.

Let $\Phi \colon \mathrm{C}(\varphi) \otimes_R X \to \mathrm{C}(\varphi \otimes_R X)$ be the unique R-linear map such that

$$\Phi(x \otimes (a', a)) = (x \otimes a', x \otimes a)$$

for all elementary tensors $(a', a) \otimes x \in \mathrm{C}(\varphi) \otimes_R X$. Then Φ is a graded isomorphism of the underlying graded R-modules. We claim that it also commutes with the differentials, making it into an isomorphism of R-complexes. Indeed, let $(a', a) \otimes x \in \mathrm{C}(\varphi) \otimes_R X$ be an elementary tensor with $a' \in A'_i$, $a \in A_{i-1}$, and $x \in X_j$. Then we have

$$\begin{aligned}
(\mathrm{d}_{\mathrm{C}(\varphi \otimes_R X)}\Phi)((a', a) \otimes x) &= \mathrm{d}_{\mathrm{C}(\varphi \otimes_R X)}(\Phi((a', a) \otimes x)) \\
&= \mathrm{d}_{\mathrm{C}(\varphi \otimes_R X)}(a' \otimes x, a \otimes x) \\
&= (\mathrm{d}^{\otimes}_{(A',X)}(a' \otimes x) + (\varphi \otimes X)(a \otimes x), -\mathrm{d}^{\otimes}_{(A,X)}(a \otimes x)) \\
&= (\mathrm{d}_{A'}(a') \otimes x + (-1)^i a' \otimes \mathrm{d}_X(x) + \varphi(a) \otimes x, -\mathrm{d}_A(a) \otimes x + (-1)^i a \otimes \mathrm{d}_X(x)) \\
&= ((\mathrm{d}_{A'}(a') \otimes x + \varphi(a) \otimes x + (-1)^i a' \otimes \mathrm{d}_X(x), -\mathrm{d}_A(a) \otimes x + (-1)^i a \otimes \mathrm{d}_X(x)) \\
&= ((\mathrm{d}_{A'}(a') + \varphi(a)) \otimes x, -\mathrm{d}_A(a) \otimes x) + (-1)^i((a' \otimes \mathrm{d}_X(x), a \otimes \mathrm{d}_X(x)) \\
&= \Phi((\mathrm{d}_{A'}(a') + \varphi(a), -\mathrm{d}_A(a)) \otimes x + (-1)^i (a', a) \otimes \mathrm{d}_X(x)) \\
&= \Phi(\mathrm{d}_{\mathrm{C}(\varphi)}(a', a) \otimes x + (-1)^i (a', a) \otimes \mathrm{d}_X(x)) \\
&= \Phi(\mathrm{d}^{\otimes}_{(\mathrm{C}(\varphi),X)}((a', a) \otimes x) \\
&= (\Phi \mathrm{d}^{\otimes}_{(\mathrm{C}(\varphi),X)})((a', a) \otimes x).
\end{aligned}$$

It follows that $\mathrm{d}_{\mathrm{C}(\varphi \otimes_R X)}\Phi = \Phi \mathrm{d}^{\otimes}_{(\mathrm{C}(\varphi),X)}$. Thus Φ gives an isomorphism of R-complexes.

□

Proposition 63.26. *Let A be an R-complex and let $\psi\colon B \to B'$ be a chain map of R-complexes. Then*

$$A \otimes_R \mathrm{C}(\psi) \cong \mathrm{C}(A \otimes_R \psi)$$

is an isomorphism of R-complexes.

Proof. Combining Proposition (63.19) and Proposition (63.25) gives us the isomorphisms

$$\begin{aligned} A \otimes_R \mathrm{C}(\psi) &\cong \mathrm{C}(\psi) \otimes_R A \\ &\cong \mathrm{C}(\psi \otimes_R A) \\ &\cong \mathrm{C}(A \otimes_R \psi). \end{aligned}$$

Following these isomorphisms in terms of an elementary homogeneous element $a \otimes (b', b) \in A_i \otimes \mathrm{C}(\psi)_j$, we have

$$\begin{aligned} a \otimes (b', b) &\mapsto (-1)^{ij}(b', b) \otimes a \\ &\mapsto (-1)^{ij}(b' \otimes a, b \otimes a) \\ &\mapsto (-1)^{ij}((-1)^{ij} a \otimes b', (-1)^{i(j-1)} a \otimes b) \\ &= (a \otimes b', (-1)^{ij + i(j-1)} a \otimes b) \\ &= (a \otimes b', (-1)^{i} a \otimes b) \end{aligned}$$

Let us check that this really does commute with the differentials. Define $\Phi\colon A \otimes_R \mathrm{C}(\psi) \to \mathrm{C}(A \otimes_R \psi)$ by

$$\Phi(a \otimes (b', b)) = (a \otimes b', (-1)^i a \otimes b)$$

for all elementary homogeneous tensors $a \otimes (b', b) \in A_i \otimes_R \mathrm{C}(\psi)_j$. Then we have

$$\begin{aligned} (\mathrm{d}_{\mathrm{C}(A \otimes_R \psi)} \Phi)(a \otimes (b', b)) &= \mathrm{d}_{\mathrm{C}(A \otimes_R \psi)}(a \otimes b', (-1)^i a \otimes b) \\ &= (\mathrm{d}^{\otimes}_{(A,B')}(a \otimes b') + (-1)^i (A \otimes_R \psi)(a \otimes b), -(-1)^i \mathrm{d}^{\otimes}_{(A,B)}(a \otimes b)) \\ &= (\mathrm{d}_A(a) \otimes b' + (-1)^i a \otimes \mathrm{d}_{B'}(b') + (-1)^i a \otimes \psi(b), -(-1)^i \mathrm{d}_A(a) \otimes b - a \otimes \mathrm{d}_B(b)) \\ &= (\mathrm{d}_A(a) \otimes b', -(-1)^i \mathrm{d}_A(a) \otimes b) + ((-1)^i a \otimes \mathrm{d}_{B'}(b') + (-1)^i a \otimes \psi(b), a \otimes -\mathrm{d}_B(b))) \\ &= \Phi(\mathrm{d}_A(a) \otimes (b', b) + (-1)^i a \otimes (\mathrm{d}_{B'}(b') + \psi(b), -\mathrm{d}_B(b))) \\ &= \Phi(\mathrm{d}_A(a) \otimes (b', b) + (-1)^i a \otimes \mathrm{d}_{\mathrm{C}(\psi)}(b', b)) \\ &= (\Phi \mathrm{d}_{A \otimes_R \mathrm{C}(\psi)})(a \otimes (b', b)). \end{aligned}$$

□

63.8.6 Tensor Respects Homotopy Equivalences

Proposition 63.27. *Let $\varphi, \psi\colon A \to A'$ be chains maps of R-complexes A and A' and let B be an R-complex. If φ is homotopic to ψ, then $\varphi \otimes 1\colon A \otimes_R B \to A' \otimes_R B$ is homotopic to $\psi \otimes 1\colon A \otimes_R B \to A' \otimes_R B$.*

Proof. Suppose φ is homotopic to ψ and choose a homotopy $h\colon A \to A'$ from φ to ψ, so

$$\varphi - \psi = \mathrm{d}h + h\mathrm{d}.$$

We claim that $h \otimes 1$ is a homotopy from $\varphi \otimes 1$ to $\psi \otimes 1$. Indeed, we have

$$\begin{aligned} \mathrm{d}(h \otimes 1) + (h \otimes 1)\mathrm{d} &= \mathrm{d}h \otimes 1 + \overline{h} \otimes \mathrm{d} + h\mathrm{d} \otimes 1 - \overline{h} \otimes \mathrm{d} \\ &= (\mathrm{d}h + h\mathrm{d}) \otimes 1 \\ &= (\varphi - \psi) \otimes 1 \\ &= \varphi \otimes 1 - \psi \otimes 1. \end{aligned}$$

Similarly, we claim that $\overline{1} \otimes h$ is a homotopy form $1 \otimes \varphi$ to $1 \otimes \psi$. Indeed, we have

$$\begin{aligned} \mathrm{d}(\overline{1} \otimes h) + (\overline{1} \otimes h)\mathrm{d} &= -\overline{\mathrm{d}} \otimes h + 1 \otimes \mathrm{d}h + \overline{\mathrm{d}} \otimes h + 1 \otimes h\mathrm{d} \\ &= 1 \otimes (\mathrm{d}h + h\mathrm{d}) \\ &= 1 \otimes (\varphi - \psi) \\ &= 1 \otimes \varphi - 1 \otimes \psi. \end{aligned}$$

□

63.8.7 Twisting the tensor complex with a chain map

Definition 63.18. Let (A, d) be R-complexes and let $\alpha\colon A \to A$ be a chain map. We define an R-complex $A \otimes_R^\alpha A$ as follows: as a graded R-module, $A \otimes_R^\alpha A$ is just $A \otimes_R A$. We define the differential $\mathrm{d}_\alpha^\otimes \colon A \otimes_R^\alpha A \to A \otimes_R^\alpha A$ on elementary tensors $a \otimes b \in A_i \otimes_R A_j$ by

$$\mathrm{d}_\alpha^\otimes(a \otimes b) = \mathrm{d}(a) \otimes b + (-1)^i \alpha(a) \otimes \mathrm{d}(b) \tag{253}$$

and then we extend $\mathrm{d}_\alpha^\otimes$ linearly everywhere else. Note that $\mathrm{d}_\alpha^\otimes$ is a well-defined R-linear map since (253) is R-bilinear in a and b. Also note that $\mathrm{d}_\alpha^\otimes$ is graded of degree -1 since α is a chain map. Let us show that we have $\mathrm{d}_\alpha^\otimes \mathrm{d}_\alpha^\otimes = 0$. Let $a \otimes b \in A_i \otimes_R A_j$. Then we have

$$\begin{aligned}
\mathrm{d}_\alpha^\otimes \mathrm{d}_\alpha^\otimes(a \otimes b) &= \mathrm{d}_\alpha^\otimes(\mathrm{d}(a) \otimes b + (-1)^i \alpha(a) \otimes \mathrm{d}(b)) \\
&= \mathrm{d}_\alpha^\otimes(\mathrm{d}(a) \otimes b) + (-1)^i \mathrm{d}_\alpha^\otimes(\alpha(a) \otimes \mathrm{d}(b)) \\
&= \mathrm{d}^2(a) \otimes b + (-1)^{i-1} \alpha \mathrm{d}(a) \otimes \mathrm{d}(b) + (-1)^i \mathrm{d}\alpha(a) \otimes \mathrm{d}(b) + \alpha^2(a) \otimes \mathrm{d}^2(b) \\
&= (-1)^{i-1} \alpha \mathrm{d}(a) \otimes \mathrm{d}(b) + (-1)^i \alpha \mathrm{d}(a) \otimes \mathrm{d}(b) \\
&= 0.
\end{aligned}$$

It follows that $\mathrm{d}_\alpha^\otimes$ is a differential.

If $\alpha\colon A \to A$ is also an R-algebra homomorphism, then observe that

$$\begin{aligned}
\mathrm{d}(\alpha(a)(bc) + (ab)\alpha(c)) &= \mathrm{d}(\alpha(a))(bc) + \alpha^2(a)\mathrm{d}(bc) + \mathrm{d}(ab)\alpha(c) + \alpha(ab)\mathrm{d}(\alpha(c)) \\
&= \alpha(\mathrm{d}(a))(bc) + \alpha^2(a)(\mathrm{d}(b)c) + \alpha^2(a)(\alpha(b)\mathrm{d}(c)) + (\mathrm{d}(a)b)\alpha(c) + (\alpha(a)\mathrm{d}(b))\alpha(c) + \alpha(ab)\alpha(\mathrm{d}(c)) \\
&= \alpha(\mathrm{d}(a))(bc) + (\alpha(a)\mathrm{d}(b))\alpha(c) + (\alpha(a)\alpha(b))(\alpha(\mathrm{d}(c)) + (\mathrm{d}(a)b)\alpha(c) + (\alpha(a)\mathrm{d}(b))\alpha(c) + \alpha(ab)\alpha(\mathrm{d}(c)) \\
&= (\mathrm{d}(a)b)\alpha(c) + (\alpha(a)\alpha(b))(\alpha(\mathrm{d}(c)) + (\mathrm{d}(a)b)\alpha(c) + \alpha(ab)\alpha(\mathrm{d}(c)) \\
&= (\alpha(a)\alpha(b))(\alpha(\mathrm{d}(c)) + \alpha(ab)\alpha(\mathrm{d}(c)) \\
&= 0.
\end{aligned}$$

$$\begin{aligned}
\mathrm{d}(a(bc) + (ab)c) &= \mathrm{d}(a)(bc) + a\mathrm{d}(bc) + \mathrm{d}(ab)c + (ab)\mathrm{d}(c) \\
&= \mathrm{d}(a)(bc) + a(\mathrm{d}(b)c) + a(b\mathrm{d}(c)) + (\mathrm{d}(a)b)c + (a\mathrm{d}(b))c + (ab)\mathrm{d}(c) \\
&= \mathrm{d}(a)(bc) + (\mathrm{d}(a)b)c + a(\mathrm{d}(b)c) + (a\mathrm{d}(b))c + a(b\mathrm{d}(c)) + (ab)\mathrm{d}(c).
\end{aligned}$$

63.9 Hom-Complex

Definition 63.19. Let X and Y be two R-complexes. We define their **hom-complex** $\mathrm{Hom}_R^\star(X, Y)$ to be the R-complex whose underlying graded R-module has homogeneous component in degree $i \in \mathbb{Z}$ given by

$$\mathrm{Hom}_{R,i}^\star(X, Y) = \{\varphi\colon X \to Y \mid \varphi \text{ is a graded } R\text{-linear of degree } i\}.$$

and whose differential, denoted $\mathrm{d}_{X,Y}^\star$ is defined by

$$\mathrm{d}_{X,Y}^\star(\varphi) = \mathrm{d}_Y \varphi - (-1)^{|\varphi|} \varphi \mathrm{d}_X. \tag{254}$$

for all homogeneous $\varphi \in \mathrm{Hom}_R^\star(X, Y)$.

If the ring R is understood from context, then we simplify our notation by saying "$\varphi\colon X \to Y$ is an i-map" to mean "$\varphi\colon X \to Y$ is a graded R-linear map of degree i". If in addition, φ commutes with the differentials (or equivalently $\mathrm{d}^\star(\varphi) = 0$), then we say φ is an i-chain map. If X and Y are understood from context, then we simplify our notation even more by dropping X and Y in the subscripts of $\mathrm{d}_{X,Y}^\star$, d_Y, and d_X. With this notational convention in mind, we may rewrite (254) in a much cleaner format:

$$\mathrm{d}^\star(\varphi) = \mathrm{d}\varphi - (-1)^{|\varphi|} \varphi \mathrm{d} \tag{255}$$

The sign $-(-1)^{|\varphi|}$ in (255) may seem a little unusual at first glance. Indeed, the differential for the tensor compex $X \otimes_R Y$ is defined by

$$\mathrm{d}^\otimes(x \otimes y) = \mathrm{d}(x) \otimes y + (-1)^{|x|} x \otimes \mathrm{d}(y)$$

for all homogeneous $x \in X$ and $y \in Y$. In fact , if we had replaced $-(-1)^{|\varphi|}$ in (254) with $(-1)^{|\varphi|}$, then we would still still obtain a differential. So why should we change things up here? One of the reasons is that it allows us to interpret $\mathrm{d}^\star(\varphi)$ as measuring the failure of the i-map φ to be an i-chain map. Indeed, φ is an i-chain map if and only if $\mathrm{d}\varphi = (-1)^{|\varphi|}\varphi\mathrm{d}$ which is equivalent to saying $\varphi \in \ker \mathrm{d}^\star$. Furthermore, two i-chain maps φ and ψ are homotopy equivalent if and only if there exists an $(i+1)$-map ϕ such that $\varphi - \psi = \mathrm{d}\phi + (-1)^{|\phi|}\phi\mathrm{d}$ which is equivalent to saying $\varphi - \psi \in \operatorname{im} \mathrm{d}^\star$. Thus the homology of the hom-complex has a really nice interpretation:

$$\mathrm{H}_i(\mathrm{Hom}_R^\star(X,Y)) = \{\text{homotopy classes of } i\text{-chain maps } X \to Y\}.$$

This is probably the most important reason we use the $-(-1)^{|\varphi|}$ in (255). Here's another good reason:

Proposition 63.28. *Let (A,d) be a DG R-algebra. Define $\mathrm{m}_{(-)}\colon A \to \mathrm{Hom}_R^\star(A,A)$ by*

$$\mathrm{m}_{(-)}(a) = \mathrm{m}_a$$

for all $a \in A$, where $\mathrm{m}_a\colon A \to A$ is the multiplication by a map defined by

$$\mathrm{m}_a(x) = ax$$

for all $x \in A$. Then $\mathrm{m}_{(-)}$ is an injective DG R-algebra homomorphism.

Proof. Observe that $\mathrm{m}_{(-)}$ is graded of degree 0 since if $a \in A$ is homogeneous, then m_a is graded of degree $|a|$; hence $|\mathrm{m}_{(-)}| = 0$. Next note that $\mathrm{m}_{(-)}$ commutes with the differentials. Indeed, given homogeneous $a \in A$, we have

$$\begin{aligned}
\mathrm{d}^\star_{A,A}\mathrm{m}_{(-)}(a) &= \mathrm{d}^\star_{A,A}(\mathrm{m}_a) \\
&= \mathrm{d}\mathrm{m}_a - (-1)^{|a|}\mathrm{m}_a\mathrm{d} \\
&= \mathrm{m}_{\mathrm{d}(a)} \\
&= \mathrm{m}_{(-)}\mathrm{d}(a)
\end{aligned}$$

where the we obtained the third line from the second line from the fact that for all $x \in A$ we have

$$\begin{aligned}
\left(\mathrm{d}\mathrm{m}_a - (-1)^{|a|}\mathrm{m}_a\mathrm{d}\right)(x) &= \mathrm{d}\mathrm{m}_a(x) - (-1)^{|a|}\mathrm{m}_a\mathrm{d}(x) \\
&= \mathrm{d}(ax) - (-1)^{|a|}a\mathrm{d}(x) \\
&= \mathrm{d}(a)x + (-1)^{|a|}a\mathrm{d}(x) - (-1)^{|a|}a\mathrm{d}(x) \\
&= \mathrm{d}(a)x \\
&= \mathrm{m}_{\mathrm{d}(a)}(x).
\end{aligned}$$

Thus we have $\mathrm{m}_{\mathrm{d}(a)} = \mathrm{d}^\star_{A,A}(\mathrm{m}_a)$ (which depended on the sign in (254)!). It is easy to see why $\mathrm{m}_{(-)}$ is an algebra homorphism. Furthermore it is injective since $1 \in A$. □

Example 63.2. Let P be an R-module viewed as a trivial R-complex where P sits in homological degree 0, and let $N = (N,\mathrm{d})$ be an R-complex such that $N_{\geq 3} = 0 = N_{\leq 0}$ and such that N is exact (meaning $\mathrm{H}(N) = 0$). In particular, N corresponds to the short exact sequence of R-modules:

$$0 \longrightarrow N_2 \xrightarrow{\mathrm{d}_2} N_1 \xrightarrow{\mathrm{d}_1} N_0 \longrightarrow 0 \tag{256}$$

Let us compute $\mathrm{Hom}_R^\star(P,N)$: the component in homological degree i is given by

$$\mathrm{Hom}_{R,i}^\star(P,N) = \begin{cases} \mathrm{Hom}_R(P,N_0) & \text{if } i = 0 \\ \mathrm{Hom}_R(P,N_1) & \text{if } i = 1 \\ \mathrm{Hom}_R(P,N_2) & \text{if } i = 2 \\ 0 & \text{else} \end{cases}$$

and the differential $\mathrm{d}^\star$ is defined by $\mathrm{d}^\star(\varphi) = \mathrm{d}\varphi$ since the differential of P is the zero map. Thus $\mathrm{Hom}_R^\star(P,N)$ corresponds to the complex we get when we apply the functor $\mathrm{Hom}_R(P,-)$ to (259):

$$0 \longrightarrow \mathrm{Hom}_R(P,N_2) \xrightarrow{\mathrm{d}_2^\star} \mathrm{Hom}_R(P,N_1) \xrightarrow{\mathrm{d}_1^\star} \mathrm{Hom}_R(P,N_0) \longrightarrow 0 \tag{257}$$

In particular, P is a projective R-module if and only if $\mathrm{Hom}_R^\star(P,-)$ sends exact complexes to exact complexes.

Example 63.3. Let E be an R-module viewed as a trivial R-complex where P sits in homological degree 0, and let $M = (M, \mathrm{d})$ be an R-complex such that $M_{\geq 3} = 0 = M_{\leq 0}$ and such that M is exact. In particular, M corresponds to the short exact sequence of R-modules:

$$0 \longrightarrow M_2 \xrightarrow{\mathrm{d}_2} M_1 \xrightarrow{\mathrm{d}_1} M_0 \longrightarrow 0 \tag{258}$$

Let us compute $\mathrm{Hom}_R^\star(M, E)$: the component in homological degree i is given by

$$\mathrm{Hom}_{R,i}^\star(M, E) = \begin{cases} \mathrm{Hom}_R(M_0, E) & \text{if } i = 0 \\ \mathrm{Hom}_R(M_1, E) & \text{if } i = -1 \\ \mathrm{Hom}_R(M_2, E) & \text{if } i = -2 \\ 0 & \text{else} \end{cases}$$

and the differential $\mathrm{d}^\star$ is defined by $\mathrm{d}^\star(\varphi) = (-1)^{|\varphi|}\varphi\mathrm{d}$ since the differential of E is the zero map. We can visually represent $\mathrm{Hom}_R^\star(M, E)$ as a complex as below:

$$0 \longrightarrow \mathrm{Hom}_R(M_0, E) \xrightarrow{\mathrm{d}_0^\star} \mathrm{Hom}_R(M_1, E) \xrightarrow{\mathrm{d}_{-1}^\star} \mathrm{Hom}_R(M_2, E) \longrightarrow 0 \tag{259}$$

In particular, E is an injective R-module if and only if $\mathrm{Hom}_R^\star(-, E)$ sends exact complexes to exact complexes. However note that even in this case, $\mathrm{Hom}_R^\star(M, E)$ is not the same R-complex we get when we apply the functor $\mathrm{Hom}_R(-, E)$ (258). Indeed, first of all $\mathrm{Hom}_R(M_2, E)$ sits in homological degree -2, however we want $\mathrm{Hom}_R(M_2, E)$ to sit in homological degree 0. Secondly, the sign in $\mathrm{d}_{-1}^\star$ is wrong since $\mathrm{d}_{-1}^\star(\varphi) = -\varphi\mathrm{d}_1$. In order to correct this we simply apply Σ^2 to $\mathrm{Hom}_R^\star(M, E)$. Indeed, we have

$$(\Sigma^2\mathrm{Hom}_R^\star(M, E))_i = \mathrm{Hom}_{R,i-2}^\star(M, E) = \begin{cases} \mathrm{Hom}_R(M_0, E) & \text{if } i = 2 \\ \mathrm{Hom}_R(M_1, E) & \text{if } i = 1 \\ \mathrm{Hom}_R(M_2, E) & \text{if } i = 0 \\ 0 & \text{else} \end{cases}$$

Furthermore the sign gets corrected since $(\Sigma^2\mathrm{d}^\star)_1 = -\mathrm{d}_{-1}^\star$.

63.9.1 Functorial Properties of Hom

Proposition 63.29. *Let (A, d_A), (A', d'_A), (B, d_B), and (B', d'_B) be R-complexes and let $\varphi\colon A \to B$ and $\phi\colon A' \to B'$ be chain maps. Then we get induced chain maps*

$$\phi_*\colon \mathrm{Hom}_R^\star(A, A') \to \mathrm{Hom}_R^\star(A, B') \quad \textit{and} \quad \varphi^*\colon \mathrm{Hom}_R^\star(B, B') \to \mathrm{Hom}_R^\star(A, B')$$

given by

$$\phi_*(\alpha) = \phi\alpha \quad \textit{and} \quad \varphi^*(\beta) = \beta\varphi$$

for all $\alpha \in \mathrm{Hom}_R^\star(A, A')$ and $\beta \in \mathrm{Hom}_R^\star(B, B')$. Furthermore, the following diagram commutes

$$\begin{array}{ccc} \mathrm{Hom}_R^\star(A, A') & \xrightarrow{\varphi^*} & \mathrm{Hom}_R^\star(B, A') \\ {\scriptstyle \phi_*}\downarrow & & \downarrow{\scriptstyle \phi_*} \\ \mathrm{Hom}_R^\star(A, B') & \xrightarrow[\varphi^*]{} & \mathrm{Hom}_R^\star(B, B') \end{array} \tag{260}$$

Proof. First let us check that ϕ_* is a chain map. It is a graded R-linear map since ϕ is a graded R-linear map of degree 0 and composition is R-linear. It remains to show that ϕ_* commutes with the differentials. Let $\alpha \in \mathrm{Hom}_R^\star(A, A')_i$. Then we have

$$\begin{aligned} (\mathrm{d}_{(A,B')}^\star\phi_*)(\alpha) &= \mathrm{d}_{(A,B')}^\star(\phi_*(\alpha)) \\ &= \mathrm{d}_{(A,B')}^\star(\phi\alpha) \\ &= \mathrm{d}_{B'}\phi\alpha - (-1)^i\phi\alpha\mathrm{d}_A \\ &= \phi\mathrm{d}_{A'}\alpha - (-1)^i\phi\alpha\mathrm{d}_A \\ &= \phi_*(\mathrm{d}_{A'}\alpha - (-1)^i\alpha\mathrm{d}_A) \\ &= \phi_*(\mathrm{d}_{(A,A')}^\star(\alpha)) \\ &= (\phi_*\mathrm{d}_{(A,A')}^\star)(\alpha). \end{aligned}$$

This implies ϕ_* is a chain map. A similar calculation shows that φ^* is a chain map.

Now we check that the diagram (260) commutes. Let $\alpha \in \mathrm{Hom}_R^\star(A, A')_i$. Then we have

$$\begin{aligned}(\phi_*\varphi^*)(\alpha) &= \phi_*(\varphi^*(\alpha)) \\ &= \phi_*(\alpha\varphi) \\ &= \phi\alpha\varphi \\ &= \varphi^*(\phi\alpha) \\ &= \varphi^*(\phi_*(\alpha)) \\ &= (\varphi^*\phi_*)(\alpha).\end{aligned}$$

This implies the diagram commutes. □

Proposition 63.30. *Let A be an R-complex. Then we obtain functors*

$$\mathrm{Hom}_R^\star(A, -)\colon \mathrm{Comp}_R \to \mathrm{Comp}_R \quad \textit{and} \quad \mathrm{Hom}_R^\star(-, A)\colon \mathrm{Comp}_R \to \mathrm{Comp}_R$$

from the category of R-complexes to itself, where the R-complex B is assigned to the R-complexes

$$\mathrm{Hom}_R^\star(A, B) \quad \textit{and} \quad \mathrm{Hom}_R^\star(B, A)$$

respectively, and where the chain map $\varphi\colon B \to B'$ of R-complexes is assigned to the chain maps

$$\mathrm{Hom}_R^\star(A, \varphi) = \varphi_* \quad \textit{and} \quad \mathrm{Hom}_R^\star(\varphi, A) = \varphi^*$$

respectively.

Proof. We will just show that $\mathrm{Hom}_R^\star(A, -)$ is a functor from the category of R-complexes to itself since a similar argument will show that $\mathrm{Hom}_R^\star(-, A)$ is one too. We need to check that $\mathrm{Hom}_R^\star(A, -)$ preserves compositions and identities. We first check that it preserves compositions. Let $\varphi\colon B \to B'$ and $\varphi'\colon B' \to B''$ be two chain maps and let $\alpha \in \mathrm{Hom}_R^\star(A, B)_i$. Then we have

$$\begin{aligned}(\varphi'\varphi)_*(\alpha) &= \varphi'\varphi\alpha \\ &= \varphi'_*(\varphi\alpha) \\ &= \varphi'_*(\varphi_*(\alpha)) \\ &= (\varphi'_*\varphi_*)(\alpha)\end{aligned}$$

It follows that $(\varphi'\varphi)_* = \varphi'_*\varphi_*$. Hence $\mathrm{Hom}_R^\star(A, -)$ preserves compositions. Next we check that $\mathrm{Hom}_R^\star(A, -)$ preserves identities. Let B be an R-complex and let $\alpha\colon A \to B$ be a chain map. Then we have

$$\begin{aligned}(1_B)_* &= 1_B\alpha \\ &= \alpha \\ &= 1_{\mathrm{Hom}_R^\star(A,B)}(\alpha).\end{aligned}$$

It follows that $(1_B)_* = 1_{\mathrm{Hom}_R^\star(A,-)}$. Hence h_A preserves identities. □

Proposition 63.31. *Let F be a covariant functor from the category of R-complexes to itself. Then F is left exact if and only if it is left exact when viewed as a functor of the underlying graded R-modules.*

Proof. One direction is easy, so we prove the other direction. Let

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0 \tag{261}$$

be an exact sequence of R-complexes and chain maps. Then (261) is an exact sequence of graded R-modules and graded homomorphisms. Thus

$$F(M_1) \xrightarrow{F(\varphi_1)} F(M_2) \xrightarrow{F(\varphi_2)} F(M_3) \longrightarrow 0 \tag{262}$$

is an exact sequence of graded R-modules and graded homomorphisms. Since the graded homomorphisms in (262) commute with the differentials, we see that (262) is actually an exact sequence of R-complexes and chain maps.

□

Proposition 63.32. *(Yoneda's Lemma) Let A be an R-complex and let $\mathcal{F}\colon \mathbf{Comp}_R \to \mathbf{Set}$ be a functor. Then we have a bijection*

$$\mathrm{Nat}(\mathcal{C}(A,-),\mathcal{F}) \cong \mathcal{F}(A)$$

which is natural in A. In particular, if B is another R-complex, then

$$\mathrm{Nat}(\mathcal{C}(A,-),C(B,-)) \cong \mathcal{C}(B,A)$$

Note that the diagram (260) tells us that each chain map $\varphi\colon A \to B$ gives rise to a natural transformation $\mathrm{h}^{-}(\varphi)\colon \mathrm{h}_A \to \mathrm{h}_B$. In light of Yoneda's Lemma, we have a map

$$\mathrm{Nat}(C(B,-),\mathcal{C}(A,-)) \to \mathcal{C}(A,B) \to \mathrm{Nat}(\mathrm{h}_A,\mathrm{h}_B).$$

63.9.2 Left Exactness of Contravariant $\mathrm{Hom}_R^\star(-,N)$

Let M and N be R-complexes. We showed earlier that both $\mathrm{Hom}_R^\star(M,-)$ and $\mathrm{Hom}_R^\star(-,N)$ are left exact functors from the category of graded R-modules to itself. In fact, we will see that they The graded version of these functors are

$$\mathrm{Hom}_R^\star(M,-)\colon \mathrm{Grad}_R \to \mathrm{Grad}_R \quad \text{and} \quad \mathrm{Hom}_R^\star(-,N)\colon \mathrm{Grad}_R \to \mathrm{Grad}_R.$$

We want to check that they are also left exact functors. Let's focus on $\mathrm{Hom}_R^\star(-,N)$ first:

Proposition 63.33. *The sequence of graded R-modules and graded homomorphisms*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0 \tag{263}$$

is exact if and only if for all R-modules N the induced sequence

$$0 \longrightarrow \mathrm{Hom}_R^\star(M_3,N) \xrightarrow{\varphi_2^*} \mathrm{Hom}_R^\star(M_2,N) \xrightarrow{\varphi_1^*} \mathrm{Hom}_R^\star(M_1,N) \tag{264}$$

is exact.

Proof. Suppose that (320) is exact and let N be any R-module. Exactness at $\mathrm{Hom}_R^\star(M_3,N)$ follows from the fact that φ_2^* is injective (which follows from the fact that $\mathrm{Hom}_R(-,N)$ is left exact). Next we show exactness at $\mathrm{Hom}_R^\star(M_2,N)$. Let $\psi_2\colon M_2 \to N$ be a graded homomorphism of degree i such that $\psi_2\varphi_1 = 0$. By left exactness of $\mathrm{Hom}_R(-,N)$, there exists a $\psi_3 \in \mathrm{Hom}_R(M,N)$ such that $\psi_2 = \psi_3\varphi_2$. Since φ_2 is surjective, ψ_3 is graded of degree i. Thus $\psi_3 \in \mathrm{Hom}_R^\star(M,N)$. Thus we have exactness at $\mathrm{Hom}_R^\star(M_2,N)$. □

63.9.3 Tensor-Hom Adjointness

Let B be an A-algebra, let X and Y be B-complexes, and let Z be an A-complex. Define a map

$$(-)$$

Proposition 63.34. *Let S be an R-algebra, let M_1, M_2 be S-complexes, and let M_3 be an R-complex. Then we have an isomorphism of S-complexes*

$$\mathrm{Hom}_S^\star(M_1,\mathrm{Hom}_R^\star(M_2,M_3)) \cong \mathrm{Hom}_R^\star(M_1 \otimes_S M_2, M_3). \tag{265}$$

*Moreover (**??**) is natural in M_1, M_2, and M_3. In particular, for any S-complex N, the functor $-\otimes_S N\colon \mathbf{Comp}_R \to \mathbf{Comp}_S$ is the left adjoint to the functor $\mathrm{Hom}_R^\star(N,-)\colon \mathbf{Comp}_S \to \mathbf{Comp}_R$. Hence $-\otimes_S N$ preserves all colimits and $\mathrm{Hom}_R^\star(N,-)$ preserves all limits.*

Proof. We define

$$\Psi_{M_1,M_2,M_3}\colon \mathrm{Hom}_S^\star(M_1,\mathrm{Hom}_R^\star(M_2,M_3)) \to \mathrm{Hom}_R^\star(M_1 \otimes_S M_2, M_3)$$

to be the map which sends a $\psi \in \mathrm{Hom}_S^\star(M_1,\mathrm{Hom}_R^\star(M_2,M_3))$ to the map $\Psi(\psi) \in \mathrm{Hom}_R^\star(M_1 \otimes_S M_2, M_3)$ defined by

$$\Psi(\psi)(u_1 \otimes u_2) = (\psi(u_1))(u_2) \tag{266}$$

for all elementary tensors $u_1 \otimes u_2 \in M_1 \otimes_S M_2$. Note that $\Psi(\psi)$ is a well-defined R-linear map since the map $M_1 \times M_2 \to M_3$ given by

$$(u_1,u_2) \mapsto (\psi(u_1))(u_2)$$

is R-bilinear. We will show that Ψ is an isomorphism of S-complexes by breaking down the proof into several steps:

Step 1: We show that Ψ is S-linear. Let $s, s' \in S$ and $\psi, \psi' \in \mathrm{Hom}_S^\star(M_1, \mathrm{Hom}_R^\star(M_2, M_3))$. We want to show that

$$\Psi(s\psi + s'\psi') = s\Psi(\psi) + s'\Psi(\psi') \tag{267}$$

We will show (**??**) holds, by showing that the two maps agree on all elementary tensors in $M_1 \otimes_S M_2$. So let $u_1 \otimes u_2 \in M_1 \otimes_S M_2$. Then

$$\begin{aligned}
\Psi(s\psi + s'\psi')(u_1 \otimes u_2) &= ((s\psi + s'\psi')(u_1))(u_2) \\
&= ((s\psi)(u_1) + (s'\psi')(u_1))(u_2) \\
&= (\psi(su_1) + \psi(s'u_1))(u_2) \\
&= (\psi(su_1))(u_2) + (\psi(s'u_1))(u_2) \\
&= \Psi(\psi)(su_1 \otimes u_2) + \Psi(\psi')(s'u_1 \otimes u_2) \\
&= (s\Psi(\psi))(u_1 \otimes u_2) + (s'\Psi(\psi'))(u_1 \otimes u_2). \\
&= (s\Psi(\psi) + s'\Psi(\psi))(u_1 \otimes u_2)
\end{aligned}$$

It follows that Ψ is S-linear.

Step 2: We show that Ψ is graded. Let ψ be a graded S-linear map from M_1 to $\mathrm{Hom}_R^\star(M_2, M_3)$ of degree n. We want to show that $\Psi(\psi)$ is a graded of degree n too. To see that $\Psi(\psi)$ is graded of degree n, let $u_1 \otimes u_2$ be an elementary tensor in $M_1 \otimes_S M_2$ where u_i has degree i and u_j has degree j. Since ψ is graded of degree n, u_1 is graded of degree i, and u_2 is graded of degree j, we see that $\psi(u_1)$ is graded of degree $i+n$, and hence

$$(\psi(u_1))(u_2) = \Psi(\psi)(u_1 \otimes u_2)$$

is graded of degree $i + j + n$. It follows that $\Psi(\psi)$ is graded of degree n.

Step 3: We show that Ψ commutes with the differentials. In other words, we want to show that

$$\mathrm{d}^\star_{(M_1 \otimes_S M_2, M_3)} \Psi = \Psi \mathrm{d}^\star_{(M_1, \mathrm{Hom}_R^\star(M_2, M_3))} \tag{268}$$

To see that (268) holds, it suffices to show that it holds when we apply to both sides any graded S-linear map of degree n from M_1 to $\mathrm{Hom}_R^\star(M_2, M_3)$. So let ψ be such a map. Then observe on the one hand, we have

$$\begin{aligned}
(\mathrm{d}^\star_{(M_1 \otimes_S M_2, M_3)} \Psi)(\psi) &= \mathrm{d}^\star_{(M_1 \otimes_S M_2, M_3)}(\Psi(\psi)) \\
&= \mathrm{d}_{M_3}\Psi(\psi) + (-1)^n \Psi(\psi)\mathrm{d}^\otimes_{(M_1, M_2)},
\end{aligned}$$

and on the other hand, we have

$$\begin{aligned}
(\Psi \mathrm{d}^\star_{(M_1, \mathrm{Hom}_R^\star(M_2, M_3))})(\psi) &= \Psi(\mathrm{d}^\star_{(M_1, \mathrm{Hom}_R^\star(M_2, M_3))}(\psi)) \\
&= \Psi(\mathrm{d}^\star_{(M_2, M_3)}\psi + (-1)^n \psi \mathrm{d}_{M_1}) \\
&= \Psi(\mathrm{d}^\star_{(M_2, M_3)}\psi) + (-1)^n \Psi(\psi \mathrm{d}_{M_1}).
\end{aligned}$$

Thus we are reduced to showing that

$$\mathrm{d}_{M_3}\Psi(\psi) + (-1)^n \Psi(\psi)\mathrm{d}^\otimes_{(M_1, M_2)} = \Psi(\mathrm{d}^\star_{(M_2, M_3)}\psi) + (-1)^n \Psi(\psi \mathrm{d}_{M_1}) \tag{269}$$

To see that (269) holds, it suffices to show that it holds when we apply any elementary homogeneous tensor in $M_1 \otimes_S M_2$ to both sides. So let $u_1 \otimes u_2 \in M_{1,i} \otimes_R M_{2,j}$ be such an elementary homogeneous tensor, so u_1 is graded of degree i and u_2 is graded of degree j. In the following calculation, we suppress parentheses as much as possible in order to clean notation. We gave

$$\begin{aligned}
(\mathrm{d}_{M_3}\Psi(\psi) + (-1)^n \Psi(\psi)\mathrm{d}^\otimes_{(M_1, M_2)})(u_1 \otimes u_2) &= \mathrm{d}_{M_3}\Psi(\psi)(u_1 \otimes u_2) + (-1)^n \Psi(\psi)\mathrm{d}^\otimes_{(M_1, M_2)}(u_1 \otimes u_2) \\
&= \mathrm{d}_{M_3}\psi(u_1)(u_2) + (-1)^n \Psi(\psi)(\mathrm{d}_{M_1}(u_1) \otimes u_2 + (-1)^i u_1 \otimes \mathrm{d}_{M_2}(u_2)) \\
&= \mathrm{d}_{M_3}\psi(u_1)(u_2) + (-1)^n \Psi(\psi)(\mathrm{d}_{M_1}(u_1) \otimes u_2) + (-1)^{i+n} \Psi(\psi)(u_1 \otimes \mathrm{d}_{M_2}(u_2)) \\
&= \mathrm{d}_{M_3}\psi(u_1)(u_2) + (-1)^n \psi(\mathrm{d}_{M_1}(u_1))(u_2) + (-1)^{i+n} \psi(u_1)(\mathrm{d}_{M_2}(u_2)) \\
&= (\mathrm{d}_{M_3}\psi(u_1) + (-1)^{i+n}\psi(u_1)\mathrm{d}_{M_2})(u_2) + (-1)^n (\psi \mathrm{d}_{M_1})(u_1)(u_2) \\
&= (\mathrm{d}^\star_{(M_2, M_3)}(\psi(u_1))(u_2) + (-1)^n (\psi \mathrm{d}_{M_1})(u_1)(u_2) \\
&= (\mathrm{d}^\star_{(M_2, M_3)}\psi)(u_1)(u_2) + (-1)^n (\psi \mathrm{d}_{M_1})(u_1)(u_2) \\
&= \Psi(\mathrm{d}^\star_{(M_2, M_3)}\psi)(u_1 \otimes u_2) + (-1)^n \Psi(\psi \mathrm{d}_{M_1})(u_1 \otimes u_2) \\
&= (\Psi(\mathrm{d}^\star_{(M_2, M_3)}\psi) + (-1)^n \Psi(\psi \mathrm{d}_{M_1}))(u_1 \otimes u_2).
\end{aligned}$$

It follows that Ψ commutes with the differentials.

Step 4: We will show that Ψ is a bijection. It will then follows that Ψ gives an isomorphism of S-complexes. We construct its inverse as follows: we define

$$\Phi_{M_1,M_2,M_3}\colon \operatorname{Hom}_R^\star(M_1 \otimes_S M_2, M_3) \to \operatorname{Hom}_S^\star(M_1, \operatorname{Hom}_R^\star(M_2, M_3))$$

to be the map given by

$$(\Phi(\varphi)(u_1))(u_2) = \varphi(u_1 \otimes u_2)$$

for all $\varphi \in \operatorname{Hom}_R^\star(M_1 \otimes_S M_2, M_3)$, $u_1 \in M_1$, and $u_2 \in M_2$. We claim that Ψ and Φ are inverse to each other. Indeed, we have

$$\begin{aligned}\Psi(\Phi(\varphi))(u_1 \otimes u_2) &= (\Phi(\varphi)(u_1))(u_2) \\ &= \varphi(u_1 \otimes u_2)\end{aligned}$$

for all $\varphi \in \operatorname{Hom}_R^\star(M_1 \otimes_S M_2, M_3)$ and $u_1 \otimes u_2 \in M_1 \otimes_S M_2$. Thus $\Psi\Phi = 1$. Similarly, we have

$$\begin{aligned}(\Phi(\Psi(\psi))(u_1))(u_2) &= \Psi(\psi)(u_1 \otimes u_2) \\ &= (\psi(u_1))(u_2)\end{aligned}$$

for all $\psi \in \operatorname{Hom}_S^\star(M_1, \operatorname{Hom}_R^\star(M_2, M_3))$ and $u_1 \in M_1$ and $u_2 \in M_2$. Thus $\Phi\Psi = 1$.

Step 5: We show naturality in M_1, M_2, and M_3. Naturality in M_1 means that if $\lambda\colon M_1 \to M_1'$ is an R-module homomorphism, then we have a commutative diagram

$$\begin{tikzcd}
\operatorname{Hom}_S(M_1', \operatorname{Hom}_R(M_2, M_3)) \arrow[r, "\Psi_{M_1',M_3}"] \arrow[d, "\lambda^*"'] & \operatorname{Hom}_R(M_1' \otimes_S M_2, M_3) \arrow[d, "(\lambda\otimes 1)^*"] \\
\operatorname{Hom}_S(M_1, \operatorname{Hom}_R(M_2, M_3)) \arrow[r, "\Psi_{M_1,M_3}"'] & \operatorname{Hom}_R(M_1 \otimes_S M_2, M_3)
\end{tikzcd}$$

Thus we want to show for all $\psi \in \operatorname{Hom}_S^\star(M_1', \operatorname{Hom}_R^\star(M_2, M_3))$, we have

$$(\lambda \otimes 1)^* \left(\Psi_{M_1',M_3}(\psi)\right) = \Psi_{M_1,M_3}(\lambda^*(\psi)) \tag{270}$$

To see that (**??**) is equal, we apply all elementary tensors to both sides. Let $u_1 \otimes u_2 \in M_1 \otimes_S M_2$. Then we have

$$\begin{aligned}\left((\lambda \otimes 1)^* \left(\Psi_{M_1',M_3}(\psi)\right)\right)(u_1 \otimes u_2) &= (\Psi_{M_1,M_3}(\psi))\,((\lambda \otimes 1)(u_1 \otimes u_2)) \\ &= (\Psi_{M_1,M_3}(\psi))\,(\lambda(u_1) \otimes u_2) \\ &= (\psi(\lambda(u_1))(u_2) \\ &= ((\lambda^*(\psi))(u_1))(u_2) \\ &= (\Psi_{M_1,M_3}(\lambda^*(\psi)))\,(u_1 \otimes u_2) \\ &= (\Psi_{M_1,M_3}(\lambda^*(\psi)))\,(u_1 \otimes u_2).\end{aligned}$$

Similarly, naturality in M_3 means that if $\lambda\colon M_3 \to M_3'$ is an R-module homomorphism, then we have a commutative diagram

$$\begin{tikzcd}
\operatorname{Hom}_S(M_1, \operatorname{Hom}_R(M_2, M_3)) \arrow[r, "\Psi_{M_1,M_3}"] \arrow[d, "(\lambda_*)_*"'] & \operatorname{Hom}_R(M_1 \otimes_S M_2, M_3) \arrow[d, "\lambda_*"] \\
\operatorname{Hom}_S(M_1, \operatorname{Hom}_R(M_2, M_3')) \arrow[r, "\Psi_{M_1,M_3'}"'] & \operatorname{Hom}_R(M_1 \otimes_S M_2, M_3')
\end{tikzcd}$$

Thus we want to show for all $\psi \in \operatorname{Hom}_S(M_1, \operatorname{Hom}_R(M_2, M_3))$, we have

$$\lambda_*\left(\Psi_{M_1,M_3}(\psi)\right) = \Psi_{M_1,M_3'}((\lambda_*)_*(\psi)) \tag{271}$$

To see that (331) is equal, we apply all elementary tensors to both sides. Let $u_1 \otimes u_2 \in M_1 \otimes_S M_2$. Then we have

$$\begin{aligned}(\lambda_* (\Psi_{M_1,M_3}(\psi)))(u_1 \otimes u_2) &= \lambda((\Psi_{M_1,M_3}(\psi))(u_1 \otimes u_2)) \\ &= \lambda((\psi(u_1))(u_2))) \\ &= (\lambda_*(\psi(u_1)))(u_2) \\ &= ((\lambda_*)_*(\psi))(u_1))(u_2) \\ &= \left(\Psi_{M_1,M_3'}((\lambda_*)_*(\psi)))\right)(u_1 \otimes u_2).\end{aligned}$$

□

There is another version of Tensor-Hom adjointness which we will state now but not prove.

Proposition 63.35. *Let S be an R-algebra, let M_2, M_3 be S-complexes, and let M_1 be an R-complex. Then we have an isomorphism of S-complexes*

$$\mathrm{Hom}_R^\star(M_1, \mathrm{Hom}_S^\star(M_2, M_3)) \cong \mathrm{Hom}_S^\star(M_1 \otimes_R M_2, M_3). \tag{272}$$

*Moreover (**??**) is natural in M_1, M_2, and M_3. In particular, for any S-complex N, the functor $- \otimes_S N\colon \mathbf{Comp}_R \to \mathbf{Comp}_S$ is the left adjoint to the functor $\mathrm{Hom}_R^\star(N, -)\colon \mathbf{Comp}_S \to \mathbf{Comp}_R$. Hence $- \otimes_S N$ preserves all colimits and $\mathrm{Hom}_R^\star(N, -)$ preserves all limits.*

63.9.4 Hom Commutes with Shifts

Proposition 63.36. *Let $n \in \mathbb{Z}$ and let A and A' be R-complexes. Then*

$$\mathrm{Hom}_R^\star(\Sigma^n A, A') \cong \Sigma^{-n}\mathrm{Hom}_R^\star(A, A') \quad \textit{and} \quad \mathrm{Hom}_R^\star(A, \Sigma^n A') \cong \Sigma^n \mathrm{Hom}_R^\star(A, A')$$

are isomorphisms of R-complexes.

Remark 116. Thus the covariant functor $\mathrm{Hom}_R^\star(A, -)$ commutes with shifts and the contravariant functor $\mathrm{Hom}_R^\star(-, A')$ anticommutes with shifts.

Proof. We will first show $\mathrm{Hom}_R^\star(\Sigma^n A, A') \cong \Sigma^{-n}\mathrm{Hom}_R^\star(A, A')$. As graded R-modules, we have

$$\begin{aligned}\mathrm{Hom}_R^\star(\Sigma^n A, A') &= \mathrm{Hom}_R^\star(A(-n), A') \\ &= \mathrm{Hom}_R^\star(A, A')(n) \\ &= \Sigma^{-n}\mathrm{Hom}_R^\star(A, A').\end{aligned}$$

We define $\Phi\colon \mathrm{Hom}_R^\star(\Sigma^n A, A') \to \Sigma^{-n}\mathrm{Hom}_R^\star(A, A')$ by

$$\Phi(\alpha) = (-1)^{x_i}\alpha$$

for all $\alpha \in \mathrm{Hom}_R^\star(\Sigma^n A, A')$ where $x_i \in \mathbb{Z}$ satisfies

$$x_i = n + x_{i-1}$$

for all $i \in \mathbb{Z}$. Then Φ is a graded isomorphism of the underlying graded R-module. We claim that it also commutes with the differentials, making it into an isomorphism of R-complexes. Indeed, let $\alpha \in \mathrm{Hom}_R^\star(\Sigma^n A, A')_i$; so $\alpha\colon A \to A'$ is a graded homomorphism of degree $n + i$. Then we have

$$\begin{aligned}(\Sigma^{-n}\mathrm{d}^\star_{(A,A')}\Phi)(\alpha) &= (-1)^{-n}\mathrm{d}^\star_{(A,A')}(\Phi(\alpha)) \\ &= (-1)^{-n+x_i}\mathrm{d}^\star_{(A,A')}(\alpha) \\ &= (-1)^{-n+x_i}(\mathrm{d}_{A'}\alpha - (-1)^{n+i}\alpha\mathrm{d}_A) \\ &= (-1)^{-n+x_i}\mathrm{d}_{A'}\alpha - (-1)^{x_i+i}\alpha\mathrm{d}_A) \\ &= (-1)^{x_{i-1}}\mathrm{d}_{A'}\alpha - (-1)^{i+x_{i-1}+n}\alpha\mathrm{d}_A \\ &= (-1)^{x_{i-1}}\mathrm{d}_{A'}\alpha - (-1)^{i+x_{i-1}}\alpha\mathrm{d}_{\Sigma^n A} \\ &= \Phi(\mathrm{d}_{A'}\alpha - (-1)^i\alpha\mathrm{d}_{\Sigma^n A}) \\ &= \Phi(\mathrm{d}^\star_{(\Sigma^n A, A')}(\alpha)) \\ &= (\Phi\mathrm{d}^\star_{(\Sigma^n A, A')})(\alpha)\end{aligned}$$

Now we will show $\mathrm{Hom}_R^\star(A, \Sigma^n A') \cong \Sigma^n \mathrm{Hom}_R^\star(A, A')$. As graded R-modules, we have

$$\begin{aligned}
\mathrm{Hom}_R^\star(A, \Sigma^n A') &= \mathrm{Hom}_R^\star(A, A'(-n)) \\
&= \mathrm{Hom}_R^\star(A, A')(-n) \\
&= \Sigma^n \mathrm{Hom}_R^\star(A, A').
\end{aligned}$$

We define $\Phi\colon \mathrm{Hom}_R^\star(A, \Sigma^n A') \to \Sigma^n \mathrm{Hom}_R^\star(A, A')$ by

$$\Phi(\alpha) = (-1)^{x_i}\alpha$$

for all $\alpha \in \mathrm{Hom}_R^\star(A, \Sigma^n A')$ where $x_i \in \mathbb{Z}$ satisfies

$$x_i = x_{i-1}$$

for all $i \in \mathbb{Z}$. Then Φ is a graded isomorphism of the underlying graded R-module. We claim that it also commutes with the differentials, making it into an isomorphism of R-complexes. Indeed, let $\alpha \in \mathrm{Hom}_R^\star(A, \Sigma^n A')_i$; so $\alpha\colon A \to A'$ is a graded homomorphism of degree $i - n$. Then we have

$$\begin{aligned}
(\Sigma^n \mathrm{d}^\star_{(A,A')}\Phi)(\alpha) &= (-1)^n \mathrm{d}^\star_{(A,A')}(\Phi(\alpha)) \\
&= (-1)^{n+x_i}\mathrm{d}^\star_{(A,A')}(\alpha) \\
&= (-1)^{n+x_i}(\mathrm{d}_{A'}\alpha - (-1)^{i-n}\alpha\mathrm{d}_A) \\
&= (-1)^{n+x_i}\mathrm{d}_{A'}\alpha - (-1)^{x_i+i}\alpha\mathrm{d}_A) \\
&= (-1)^{x_{i-1}}\mathrm{d}_{\Sigma^n A'}\alpha - (-1)^{x_{i-1}+i}\alpha\mathrm{d}_A \\
&= \Phi(\mathrm{d}_{\Sigma^n A'}\alpha - (-1)^i\alpha\mathrm{d}_A) \\
&= \Phi(\mathrm{d}^\star_{(A,\Sigma^n A')}(\alpha)) \\
&= (\Phi\mathrm{d}^\star_{(A,\Sigma^n A')})(\alpha)
\end{aligned}$$

□

63.9.5 Hom Commutes with Mapping Cone

Proposition 63.37. *Let A and B be R-complexes and let $\varphi\colon A \to B$ be a chain map. Then for all R-complexes X and Y we have natural isomorphisms*

$$\mathrm{Hom}_R^\star(X, \mathrm{C}(\varphi)) \simeq \mathrm{C}(\varphi_*) \quad \textit{and} \quad \Sigma\mathrm{Hom}_R^\star(\mathrm{C}(\varphi), Y) \simeq \mathrm{C}(\varphi^*).$$

Proof. It suffices to show $\mathrm{Hom}_R^\star(X, \mathrm{C}(\varphi)) \cong \mathrm{C}(\varphi_*)$ since the other argument is the same. Let $C = \mathrm{C}(\varphi) = B + eA$ be the mapping cone. Denote $A' = \mathrm{Hom}_R^\star(X, A)$, $B' = \mathrm{Hom}_R^\star(X, B)$, and $C' = \mathrm{Hom}_R^\star(X, C)$. Our goal is to show that $C' \simeq \mathrm{C}(\varphi_*)$. First note that as graded R-modules we have

$$C' \simeq B' \oplus A'(-1) = B' + eA' = \mathrm{C}(\varphi_*),$$

where the isomorphism $\Phi\colon C' \simeq \mathrm{C}(\varphi_*)$ is given by $\Phi(\gamma) = \beta + e\alpha$ where $\beta = \pi_1\gamma$ and $\alpha = \pi_2\gamma$ where $\pi_1\colon B \oplus A(-1) \to B$ and $\pi_2\colon B \oplus A(-1) \to A(-1)$ are the canonical projection maps. Now let $\gamma = \beta + e\alpha \in C'_i$. Then we have

$$\begin{aligned}
\Phi\mathrm{d}^\star(\gamma) &= \Phi(\mathrm{d}\gamma - (-1)^i\gamma\mathrm{d}) \\
&= \pi_1\mathrm{d}\gamma + e\pi_2\mathrm{d}\gamma - (-1)^i\pi_1\gamma\mathrm{d} - (-1)^i e\pi_2\gamma\mathrm{d} \\
&= \mathrm{d}\beta + \varphi\alpha - e\mathrm{d}\alpha - (-1)^i\beta\mathrm{d} - (-1)^i e\alpha\mathrm{d} \\
&= \mathrm{d}^\star(\beta) + \varphi_*(\alpha) - e\mathrm{d}^\star(\alpha) \\
&= \mathrm{d}(\beta + e\alpha) \\
&= \mathrm{d}(\Phi\gamma).
\end{aligned}$$

It follows that Φ is chain map. □

63.9.6 Hom Preserves Homotopy Equivalences

Proposition 63.38. *Let B be an R-complex, let $\varphi\colon A \to A'$ and $\psi\colon A \to A'$ be two chain maps of R-complexes, and suppose $\varphi \sim \psi$. Then $\mathrm{Hom}_R^\star(\varphi, B) \sim \mathrm{Hom}_R^\star(\psi, B)$.*

Proof. Choose a homotopy $h\colon A \to A'$ from φ to ψ (so $\varphi - \psi = \mathrm{d}_{A'}h + h\mathrm{d}_A$). To ease the notation in the following calculation, we write $\varphi^\star = \mathrm{Hom}_R^\star(\varphi, B)$, $\psi^\star = \mathrm{Hom}_R^\star(\psi, B)$, and $h^\star = \mathrm{Hom}_R^\star(h, B)$. We claim that $h^\star\colon \mathrm{Hom}_R^\star(A', B) \to \mathrm{Hom}_R^\star(A, B)$ is a homotopy from $\varphi^\star$ to $\psi^\star$. Indeed, let $\alpha\colon A' \to B$ be a graded R-linear map of degree i. Then observe that

$$\begin{aligned}
(\mathrm{d}^\star_{(A,B)}h^\star + h^\star\mathrm{d}^\star_{(A',B)})(\alpha) &= (-1)^i\mathrm{d}^\star_{(A,B)}(\alpha h) + h^\star(\mathrm{d}_B\alpha - (-1)^i\alpha\mathrm{d}_{A'}) \\
&= (-1)^i\mathrm{d}_B\alpha h + (-1)^i(-1)^i\alpha h\mathrm{d}_A - (-1)^i\mathrm{d}_B\alpha h - (-1)^i(-1)^{i+1}\alpha\mathrm{d}_{A'}h \\
&= \alpha h\mathrm{d}_A + \alpha\mathrm{d}_{A'}h \\
&= \alpha(h\mathrm{d}_A + \mathrm{d}_{A'}h) \\
&= \alpha(\varphi - \psi) \\
&= (\varphi^\star - \psi^\star)(\alpha)
\end{aligned}$$

Thus $h^\star$ is indeed a homotopy from $\varphi^\star$ to $\psi^\star$. □

Corollary 67. *Suppose $\varphi\colon A \to A'$ is a homotopy of equivalence of R-complexes. Then $\mathrm{Hom}_R^\star(\varphi, B)\colon \mathrm{Hom}_R^\star(A', B) \to \mathrm{Hom}_R^\star(A, B)$ is a homotopy equivalence of R-complexes.*

Proof. Let $\varphi'\colon A' \to A$ be the homotopy inverse to φ. Thus $\varphi\varphi' \sim 1_{A'}$ and $\varphi'\varphi \sim 1_A$. It follows that

$$\begin{aligned}
1_{\mathrm{Hom}_R^\star(A',B)} &= \mathrm{Hom}_R^\star(1_{A'}, B) \\
&\sim \mathrm{Hom}_R^\star(\varphi\varphi', B) \\
&= \mathrm{Hom}_R^\star(\varphi', B)\mathrm{Hom}_R^\star(\varphi, B).
\end{aligned}$$

Similarly, we have $1_{\mathrm{Hom}_R^\star(A,B)} \sim \mathrm{Hom}_R^\star(\varphi, B)\mathrm{Hom}_R^\star(\varphi', B)$. Therefore $\mathrm{Hom}_R^\star(\varphi, B)$ is a homotopy equivalence of R-complexes. □

63.9.7 Twisting the hom complex with a chain map

Definition 63.20. Let (A, d) be an R-complex and let $\alpha\colon A \to A$ be a chain map. We define an R-complex $\mathrm{Hom}_R^{\star_\alpha}(A, A)$ as follows: as a graded R-module, $\mathrm{Hom}_R^{\star_\alpha}(A, A)$ is just $\mathrm{Hom}_R^\star(A, A)$. We define the differential $\mathrm{d}^\star_\alpha\colon \mathrm{Hom}_R^{\star_\alpha}(A, A) \to \mathrm{Hom}_R^{\star_\alpha}(A, A)$ on graded R-linear map $\varphi\colon A \to A$ of degree i by

$$\mathrm{d}^\star_\alpha(\varphi) = \mathrm{d}\varphi + (-1)^i\alpha\varphi\mathrm{d} \tag{273}$$

and then we extend $\mathrm{d}^\star_\alpha$ linearly everywhere else. Note that $\mathrm{d}^\star_\alpha$ is graded of degree -1 since α is a chain map. Let us show that we have $\mathrm{d}^\star_\alpha\mathrm{d}^\star_\alpha = 0$. Let $\varphi\colon A \to A$ be a graded R-linear map of degree i . Then we have

$$\begin{aligned}
\mathrm{d}^\star_\alpha\mathrm{d}^\star_\alpha(\varphi) &= \mathrm{d}^\star_\alpha(\mathrm{d}\varphi + (-1)^i\alpha\varphi\mathrm{d}) \\
&= \mathrm{d}\mathrm{d}\varphi + (-1)^{i-1}\alpha\mathrm{d}\varphi\mathrm{d} + (-1)^i\mathrm{d}\alpha\varphi\mathrm{d} + (-1)^{i-1}\alpha\alpha\varphi\mathrm{d}\mathrm{d} \\
&= (-1)^{i-1}\alpha\mathrm{d}\varphi\mathrm{d} + (-1)^i\alpha\mathrm{d}\varphi\mathrm{d} \\
&= 0.
\end{aligned}$$

It follows that $\mathrm{d}^\star_\alpha$ is a differential.

63.10 Total Complex

Definition 63.21. A **double R-complex** is a bi-graded R-module

$$X = \bigoplus_{i,j \in \mathbb{Z}} X_{i,j}$$

equipped with two R-linear maps $\partial, \partial'\colon X \to X$, where ∂ is graded of degree $(-1, 0)$ and where ∂' is graded of degree $(0, -1)$, such that

$$\partial\partial = 0 = \partial'\partial' \quad \text{and} \quad \partial\partial' = \partial'\partial.$$

Definition 63.22. Let X be a double R-complex. The **total R-complex** associated to X, denoted $A = \operatorname{Tot} X$, is the R-complex whose graded R-module has component

$$A_n = \bigoplus_{i+j=n} X_{i,j}$$

in homological degree n and whose differential d is defined on the bi-homogeneous component $X_{i,j}$ by

$$\mathrm{d}|_{X_{i,j}} = \partial + (-1)^i \partial'.$$

In particular, if $a \in A$, then we can express a in terms of its bi-homogeneous components, say $a = \sum_{i,j} x_{i,j}$, and the differential would be given by

$$\mathrm{d}a = \sum_{i,j} \mathrm{d}(x_{i,j}) = \sum_{i,j} \partial(x_{i,j}) + (-1)^i \partial'(x_{i,j}).$$

Example 63.4. Let A and B be R-complexes. The tensor product $A \otimes_R B$ can be viewed as a double complex with respect to the differentials $\mathrm{d}^1 = \mathrm{d} \otimes 1$ and $\mathrm{d}^2 = 1 \otimes \mathrm{d}$ where the homogeneous component of $A \otimes_R B$ is bi-degree (i, j) is $A_i \otimes_R B_j$. Then the total complex of $A \otimes_R B$ viewed as a double complex gives us the usual tensor complex $A \otimes_R B$.

64 Spectral Sequences

Definition 64.1. A **spectral sequence** is a sequence of R-complexes (E^n, d^n) for $n \geq 1$ such that

$$E^{n+1} = \mathrm{H}(E^n)$$

as graded R-modules. We define the **limit** of (E^n), denoted E^∞, as follows: first set $Z^1 = E^1$ and $B^1 = 0$. Next we set $Z^2 = \ker(\mathrm{d}^1)$ and $B^2 = \operatorname{im}(\mathrm{d}^1)$. More generally, for $n \geq 2$ we set:

$$Z^{n+1} = \ker(Z^n \twoheadrightarrow E^n \xrightarrow{\mathrm{d}^n} E^n) \quad \text{and} \quad B^{n+1}/B^n = \operatorname{im}(E^n \xrightarrow{\mathrm{d}^n} E^n = Z^n/B^n).$$

Clearly we have $B^n \subset B^{n+1} \subset Z^{n+1} \subset Z^n$. Furthermore, observe that

$$\begin{aligned} Z^{n+1}/B^{n+1} &= (Z^{n+1}/B^n)/(B^{n+1}/B^n) \\ &= \ker(\mathrm{d}^n)/\operatorname{im}(\mathrm{d}^n) \\ &= \mathrm{H}(E^n) \\ &= E^{n+1}. \end{aligned}$$

With this in mind, we set

$$Z^\infty = \bigcap_{n \geq 1} Z^n, \quad B^\infty = \bigcup_{n \geq 1} B^n, \quad \text{and} \quad E^\infty = Z^\infty / B^\infty.$$

We say that the spectral sequence **collapses at** E^m if $E^m = E^\infty$ or equivalently if $\mathrm{d}^n = 0$ for all $n \geq m$.

Definition 64.2. A **bigraded spectral sequence** is a spectral sequence (E^n) such that the underlying module of E^n is bi-graded:

$$E^n = \bigoplus_{i,j \in \mathbb{Z}} E^n_{i,j}.$$

Here the component of E^n in homological degree $k \in \mathbb{Z}$ is given by

$$E^n_k = \bigoplus_{\substack{i,j \in \mathbb{Z} \\ i+j=k}} E^n_{i,j}.$$

We further require the differential of E^n to be bi-graded of bi-degree $(-n, n-1)$. In particular this means that if $a \in E^n_{i,j}$, then $\mathrm{d}^n a \in E^n_{i-n,j+n-1}$. We say (E^n) is a **first quadrant** bigraded spectral sequence if $E^n_{i,j} = 0$ whenever $i < 0$ or $j < 0$. In this case, note that for i, j fixed, we have $E^n_{i,j} = E^{n+1}_{i,j}$ for all large n (e.g. for $n > \max\{i, j+1\}$).

64.1 Exact Couples

An **exact couple** is an exact triangle of them form

$$\begin{tikzcd} D \arrow[rr, "\alpha"] & & D \arrow[dl, "\beta"] \\ & E \arrow[ul, "\gamma"] & \end{tikzcd} \tag{274}$$

that is, a diagram of R-modules and maps as above, which is exact in the obvious sense that $\ker \alpha = \operatorname{im} \gamma$, $\ker \gamma = \operatorname{im} \beta$, and $\ker \beta = \operatorname{im} \alpha$. Let $\mathrm{d}^1 := \beta\gamma$, let $Z^2 := \ker \mathrm{d}^1$, and let $B^2 := \operatorname{im} \mathrm{d}^1$. Note by exactness of the couple we have

$$\begin{aligned} Z^2 &= \ker \mathrm{d}^1 & \qquad B^2 &= \operatorname{im} \mathrm{d}^1 \\ &= \ker(\beta\gamma) & &= \beta\gamma E \\ &= \gamma^{-1}(\ker \beta) & &= \beta(\operatorname{im} \gamma) \\ &= \gamma^{-1}(\alpha D) & &= \beta(\ker \alpha). \end{aligned}$$

Also note that since $\gamma\beta = 0$, we have $\mathrm{d}^1\mathrm{d}^1 = 0$, so $E^1 = (E, \mathrm{d}^1)$ is a differential R-module. We let $E^2 := \mathrm{H}E = Z^2/B^2$ denote its homology. The **derived exact couple** of (274) is the exact triangle

$$\begin{tikzcd} \alpha D \arrow[rr, "\alpha'"] & & \alpha D \arrow[dl, "\beta'"] \\ & \mathrm{H}E \arrow[ul, "\gamma'"] & \end{tikzcd} \tag{275}$$

where $\alpha' = \alpha|_{\alpha D}$, where $\beta' = \beta\alpha^{-1}$ taking αd to the homology class of βd, and where γ' is the map induced by γ on Z^2 (which automoatically kills B^2). Note that β' is well-defined because $\ker \alpha = \operatorname{im} \gamma$ is taken to B^2 by β. The proof of exactness is completely straightforward. We set $\mathrm{d}^2 := \beta'\gamma' = \beta\alpha^{-1}\gamma'$ which gives $\mathrm{H}E$ the structure of a differential R-module whose homology is denoted $\mathrm{HH}E = Z^3/B^3$ where $Z^3 := \ker(Z^2 \twoheadrightarrow E^2 \xrightarrow{\mathrm{d}^2} E^2)$ and $B^3/B^2 := \operatorname{im}(E^2 \xrightarrow{\mathrm{d}^2} E^2 = Z^2/B^2)$. Again note by exactness of the couple we have

$$\begin{aligned} Z^3 &= \ker(\mathrm{d}^2\pi) & \qquad B^3/B^2 &= \operatorname{im}(\mathrm{d}^2) \\ &= \pi^{-1}(\ker \mathrm{d}^2) & &= \beta'\gamma' E^2 \\ &= \pi^{-1}(\ker(\beta'\gamma')) & &= \beta'(\operatorname{im} \gamma') \\ &= \pi^{-1}(\gamma'^{-1}(\ker \beta')) & &= \beta'(\ker \alpha') \\ &= \gamma^{-1}(\alpha^2 D) & &= \beta(\ker \alpha^2)/B^2. \end{aligned}$$

where $\pi \colon Z^2 \twoheadrightarrow E^2 = Z^2/B^2$ denotes the quotient map. Thus $Z^3 = \gamma^{-1}(\alpha^2 D)$ and $B^3 = \beta(\ker \alpha^2)$. The derived exact couple of (275) is the exact triangle

$$\begin{tikzcd} \alpha^2 D \arrow[rr, "\alpha''"] & & \alpha^2 D \arrow[dl, "\beta''"] \\ & \mathrm{HH}E \arrow[ul, "\gamma''"] & \end{tikzcd} \tag{276}$$

where $\alpha'' = \alpha|_{\alpha^2 D}$, where $\beta'' = \beta\alpha^{-2}$, and where γ'' is the map induced by γ on Z^3. We set $\mathrm{d}^3 := \beta''\gamma'' = \beta\alpha^{-2}\gamma''$ which gives $\mathrm{HH}E$ the structure of a differential R-module. More generally, we obtain a spectral sequence (E^n) where

$$E^{n+1} = \mathrm{H}E^n = \mathrm{H}^n E \quad \text{and} \quad \mathrm{d}^{n+1} = \beta^n\gamma^n = \beta\alpha^{-n}\gamma^n,$$

called the **spectral sequence of the exact couple**. We have $Z^{n+1} = \gamma^{-1}(\alpha^n D)$ and $B^{n+1} = \beta(\ker \alpha^n)$. In particular we have

$$E^\infty = \gamma^{-1}\left(\bigcap_n \alpha^n D\right) / \beta\left(\bigcup_n \ker \alpha^n\right).$$

64.1.1 Where do exact couples come from?

Let us now give a construction of where exact couples come from. Let A be a differential R-module, let $\alpha \colon A \to A$ be a monomorphism, and let $\overline{A} = A/\alpha A$. By adjoining an element α to R and letting it act as α on A if necessary, we may think of the map α as induced by multiplication with an element α of R which is an A-regular element. The module $\overline{A}$ inherits a differential from A, so the short exact sequence of differential modules

$$0 \longrightarrow A \xrightarrow{\alpha} A \longrightarrow \overline{A} \longrightarrow 0 \tag{277}$$

gives rise to an exact couple in homology

$$\begin{tikzcd} \mathrm{H}A \arrow[rr, "\alpha"] & & \mathrm{H}A \arrow[dl, "\beta"] \\ & \mathrm{H}\overline{A} \arrow[ul, "\gamma"] & \end{tikzcd} \tag{278}$$

The spectral sequence of this exact couple is called the **spectral sequence of α on** A. In this case, the map $\gamma\colon \mathrm{H}\overline{A} \to \mathrm{H}A$ is the one induced by $\alpha^{-1}\mathrm{d}\colon A' \to A$ where $A' = \{a \in A \mid \mathrm{d}a \in \alpha A\}$. For instance, let $e \in \mathrm{H}\overline{A}$ and let $a \in A$ be a representative for e. Thus $\mathrm{d}a = \alpha a'$ for some $a' \in A$ and all other representatives of e are of the form $a + \mathrm{d}a'' + \alpha a'''$ where $a'', a''' \in A$. Then $\gamma e \in \mathrm{H}A$ is represented by a'. In particular we may write $\gamma = \alpha^{-1}\mathrm{d}$ and $\mathrm{d}^1 = \beta\alpha^{-1}\mathrm{d}$.

The module Z^{n+1} is the set of all classes in $\mathrm{H}\overline{A}$ which can be lifted modulo α^{n+1}, that is, the set of all classes which have a representative in A (not necessarily a cycle) that becomes a cycle modulo α^{n+1}:

$$Z^{n+1} = \{\overline{a} \in \mathrm{H}\overline{A} \mid \mathrm{d}a = \alpha^{n+1}a' \text{ for some } a' \in A \text{ (necessarily } \mathrm{d}a' = 0)\}.$$

In particular, if $\overline{a} \in Z^{n+1}$, then then $\mathrm{d}a = \alpha^{n+1}a'$ for some $a' \in A$ (necessarily $\mathrm{d}a' = 0$) which implies $\mathrm{d}^{n+1}\overline{a} = \overline{a'}$. Intuitively, one should interpret $\alpha^{n+1}a'$ as being close to 0 for n sufficiently large and so in some sense we have $Z^{n+1} \to \ker \mathrm{d}$ as $n \to \infty$. The module B^{n+1} is the image in $\mathrm{H}\overline{A}$ of the α^n-torsion in $\mathrm{H}A$:

$$B^{n+1} = \{\overline{a} \in \mathrm{H}\overline{A} \mid \alpha^n a = \mathrm{d}a' \text{ for some } a' \in A \text{ (necessarily } \mathrm{d}a = 0)\}.$$

Again if we interpret $\alpha^n a$ as being close to 0 for sufficiently large n, then intuitively we have $B^{n+1} \to \operatorname{im} \mathrm{d}$ as $n \to \infty$. In particular, intuitively we have $E^{n+1} \to \mathrm{H}A$ as $n \to \infty$.

64.2 Filtered Complexes

Example 64.1. Let $(X_{(k)})$ be an ascending filtered R-complex X. In order to avoid confusion in notation, the component of $X_{(k)}$ in homological degree i is denoted $X_{(k),i}$. Let

$$A = \mathrm{bl}\, X = \bigoplus_{k \in \mathbb{Z}} X_{(k)} = \sum_{k \in \mathbb{Z}} t^k X_{(k)}$$

and let $\alpha\colon A \to A$ be the multiplication by t map given by $\alpha(t^k x) = t^{k+1}x$ where $x \in X_{(k)}$. Note that

$$\overline{A} = A/\alpha = \mathrm{gr}\, X = \bigoplus_{k \in \mathbb{Z}} X_{(k)}/X_{(k-1)} = \sum_{k \in \mathbb{Z}} t^k \overline{X}_{(k)}.$$

Thus the spectral sequence of α on A starts out as

$$E = \mathrm{H}(\mathrm{gr}\, X) = \bigoplus_{k \in \mathbb{Z}} \mathrm{H}(\overline{X}_{(k)}) = \bigoplus_{k \in \mathbb{Z}} E_{(k)}.$$

With this in mind, observe that

$$\begin{aligned} Z^{n+1}_{(k)} &= \{t^k \overline{x} \in E_{(k)} \mid \mathrm{d}x \in X_{(k+n+1)}\} \\ &= (\{x \in X_{(k)} \mid \mathrm{d}x \in X_{(k+n+1)}\} + X_{(k-1)})/(X_{(k-1)} + \mathrm{d}X_{(k)}) \end{aligned}$$

Similarly we have

$$\begin{aligned} B^{n+1}_{(k)} &= \{t^k \overline{x} \in E_{(k)} \mid x = \mathrm{d}x' \text{ for some } x' \in X_{(k-n)}\} \\ &= ((X_{(k)} \cap \mathrm{d}X_{(k-n)}) + X_{(k+1)})/(X_{(k+1)} + \mathrm{d}X_{(k)}) \end{aligned}$$

Example 64.2. Let $X = (X_k)$ be a filtered R-complex. In order to avoid confusion in notation, the component of X_k in homological degree i is denoted $X_{k,i}$. Let

$$A = \mathrm{bl}\, X = X \oplus tX_1 \oplus t^2 X_2 \oplus \cdots$$

and let $\alpha\colon A \to A$ be the map given by

$$\alpha(t^k x) = \begin{cases} t^{k-1}x & \text{if } k \geq 1 \\ 0 & \text{if } k = 0. \end{cases}$$

In other words, α is a slightly modified version of the multiplication by t^{-1} map (one should basically think about α as being the multiplication by t^{-1} map). Note that

$$\overline{A} = A/\alpha = \operatorname{gr} X = (X/X_1) \oplus (X_1/X_2)t \oplus (X_2/X_3)t^2 \oplus \cdots .$$

Thus the spectral sequence of α on A starts out as

$$E^1 = \mathrm{H}(\operatorname{gr} X) = \bigoplus_k \mathrm{H}(X_k/X_{k+1}) = \bigoplus_k E^1_k.$$

With this in mind, observe that

$$\begin{aligned} Z^{n+1}_k &= \{t^k \overline{x} \in E^1_k \mid x \in X_k \text{ and } \mathrm{d}x \in X_{k+n+1}\} \\ &= (\{x \in X_k \mid \mathrm{d}x \in X_{k+n+1}\} + X_{k+1})/(X_{k+1} + \mathrm{d}X_k) \end{aligned}$$

Similarly we have

$$\begin{aligned} B^{n+1}_k &= \{t^k \overline{x} \in E^1_k \mid x = \mathrm{d}x' \text{ for some } x' \in X_{k-n}\} \\ &= ((X_k \cap \mathrm{d}X_{k-n}) + X_{k+1})/(X_{k+1} + \mathrm{d}X_k) \end{aligned}$$

Example 64.3. Let (Y, ∂, ∂') be a double R-complex where ∂ is bi-graded of degree $(-1, 0)$, where ∂' is bi-graded of degree $(0, 1)$, and where $Y_{i,j} = 0$ for all $j < 0$. Let $X = \operatorname{Tot} Y$ and equip X with the filtration $(X^{\geq k})$ where $X^{\geq k}$ is the R-subcomplex of X whose underlying graded R-module is given by

$$X^{\geq k} = \bigoplus_{i \in \mathbb{Z},\, j \geq k} Y_{i,j}$$

and whose differential is just the restriction of the differential of X on $X^{\geq k}$. Let

$$A = \operatorname{bl} X = X \oplus tX^{\geq 1} \oplus t^2 X^{\geq 2} \oplus \cdots$$

and let $\alpha\colon A \to A$ be the map given by

$$\alpha(t^m x) = \begin{cases} t^{m-1}x & \text{if } k \geq 1 \\ 0 & \text{if } k = 0. \end{cases}$$

In other words, α is a slightly modified version of the multiplication by t^{-1} map. Note that

$$\overline{A} = A/\alpha = \operatorname{gr} X = X^0 \oplus tX^1 \oplus t^2 X^2 \oplus \cdots$$

where X^k is the R-complex whose underlying graded R-module is

$$X^k = \bigoplus_{i \in \mathbb{Z}} X_{i,k}$$

and whose differential is $\partial|_{X^k}$. We will see that the E^1 terms are bigraded with components given by

$$E^1_{i,j} = \mathrm{H}_j(X_{i,-}),$$

and we will see that if $X_{i,j} = 0$ for all $j < 0$ then the sequence converges:

$$E^\infty = \operatorname{gr} \mathrm{H}(A).$$

65 Ext and Tor

65.1 Projective Resolutions

Definition 65.1. Let M be an R-module. An **augmented projective resolution of** M **over** R is an R-complex (P, d) such that

1. P is a projective R-module. Equivalently, P_i is a projective R-module for all $i \in \mathbb{Z}$;

2. $P_i = 0$ for all $i < 0$;

3. $\mathrm{H}_0(P) \cong M$ and $\mathrm{H}_i(P) = 0$ for all $i > 0$.

Theorem 65.1. *Let (P, d) and (P', d') be two projective resolutions of M over R. Then (P, d) and (P', d') are homotopically equivalent.*

Proof. For each $i \geq 0$, let $M_i' := \operatorname{im} \mathrm{d}_i'$ and let $M_i := \operatorname{im} \mathrm{d}_i$. We build a chain map $\varphi \colon (P, \mathrm{d}) \to (P', \mathrm{d}')$ by constructing R-module homomorphism $\varphi_i \colon P_i \to P_i'$ which commute with the differentials using induction on $i \geq 0$. First consider the base case $i = 0$. Since $P_0/M_1 \cong P_0'/M_1'$, there exists a homomorphism $\psi_0 \colon P_0 \to P_0'/M_0'$. Then since P_0 is projective and since $\mathrm{d}_0' \colon P_0' \to P_0'/M_1$ is a surjective homomorphism, we can lift $\psi_0 : P_0 \to P_0'/M_0'$ along $\mathrm{d}_0' : P_0' \to P_0'/M_1$ to a homomorphism $\varphi_0 \colon P_0 \to P_0'$ such that $\mathrm{d}_0'\varphi_0 = \psi_0$.

Now suppose for some $i > 0$ we have constructed R-module homomorphisms $\varphi_0, \varphi_1, \dots, \varphi_i$ which commute with the differentials. We need to construct an R-module homomorphism $\varphi_{i+1} \colon P_{i+1} \to P_{i+1}'$ which commutes with the differentials. First, we claim that $\operatorname{im}(\varphi_i \mathrm{d}_{i+1}) \subseteq M_{i+1}'$. To see this, note that

$$\begin{aligned} \mathrm{d}_i'\varphi_i\mathrm{d}_{i+1} &= \varphi_{i-1}\mathrm{d}_i\mathrm{d}_{i+1} \\ &= 0. \end{aligned}$$

Thus, since $i > 0$, we have

$$\begin{aligned} \operatorname{im}(\varphi_i\mathrm{d}_{i+1}) &\subseteq \ker \mathrm{d}_i \\ &= \operatorname{im} \mathrm{d}_{i+1}' \\ &= M_{i+1}'. \end{aligned}$$

Now since P_{i+1} is projective and $\mathrm{d}_{i+1}' \colon P_{i+1} \to M_{i+1}$ is surjective, we can lift $\varphi_i\mathrm{d}_{i+1} : P_{i+1} \to M_{i+1}'$ along $\mathrm{d}_{i+1}' : P_{i+1}' \to M_{i+1}'$ to a homomorphism $\varphi_{i+1} \colon P_{i+1} \to P_{i+1}'$ such that $\mathrm{d}_{i+1}'\varphi_{i+1} = \varphi_i\mathrm{d}_{i+1}$.

By a similar construction as above, we get a chain map $\varphi' \colon (P', \mathrm{d}') \to (P, \mathrm{d})$. Now we claim that $\varphi'\varphi$ is homotopic to id_P and similarly $\varphi\varphi'$ is homotopic to $\mathrm{id}_{P'}$. It suffices to show that $\varphi'\varphi \sim \mathrm{id}_P$ (a similar argument will give $\varphi\varphi' \sim \mathrm{id}_{P'}$). The idea is to build the homotopy $h \colon (P, \mathrm{d}) \to (P, \mathrm{d})$ using induction on $i \geq 0$. The homotopy equation that we need is

$$\varphi'\varphi - 1 = \mathrm{d}h + h\mathrm{d}, \tag{279}$$

where we write 1 instead of id_P is clean notation. Since P_0 is projective and $\mathrm{d}_1 \colon P_1 \to P_0$ is a surjective morphism, there exists a homomorphism $h_0 \colon P_0 \to P_1$ such that

$$\varphi_0'\varphi_0 - 1 = \mathrm{d}_1 h_0. \tag{280}$$

In homological degree $i = 0$, the equation (279) becomes (280). Thus, we are on the right track.

Now we use induction. Suppose for $i > 0$ we have constructed an R-module homomorphism $h_i \colon P_i \to P_{i+1}$ such that

$$\varphi_i'\varphi_i - 1 = \mathrm{d}_{i+1}h_i + h_{i-1}\mathrm{d}_i. \tag{281}$$

Observe that $\operatorname{Im}(\varphi_i'\varphi_i - 1 - h_{i-1}\mathrm{d}_i) \subseteq M_{i+1}$. Indeed, note that

$$\begin{aligned} \mathrm{d}_i(\varphi_i'\varphi_i - 1 - h_{i-1}\mathrm{d}_i) &= \mathrm{d}_i\varphi_i'\varphi_i - \mathrm{d}_i - \mathrm{d}_ih_{i-1}\mathrm{d}_i \\ &= \varphi_{i-1}'\mathrm{d}_i'\varphi_i - \mathrm{d}_i - \mathrm{d}_ih_{i-1}\mathrm{d}_i \\ &= \varphi_{i-1}'\varphi_{i-1}\mathrm{d}_i - \mathrm{d}_i - \mathrm{d}_ih_{i-1}\mathrm{d}_i \\ &= (\varphi_{i-1}'\varphi_{i-1} - 1)\mathrm{d}_i - \mathrm{d}_ih_{i-1}\mathrm{d}_i \\ &= (\mathrm{d}_ih_{i-1} + h_{i-2}\mathrm{d}_{i-1})\mathrm{d}_i - \mathrm{d}_ih_{i-1}\mathrm{d}_i \\ &= \mathrm{d}_ih_{i-1}\mathrm{d}_i + h_{i-2}\mathrm{d}_{i-1}\mathrm{d}_i - \mathrm{d}_ih_{i-1}\mathrm{d}_i \\ &= \mathrm{d}_ih_{i-1}\mathrm{d}_i - \mathrm{d}_ih_{i-1}\mathrm{d}_i \\ &= 0. \end{aligned}$$

Therefore since P_{i+1} is projective and since $\mathrm{d}_{i+2} \colon P_{i+2} \to M_{i+2}$ is a surjective homomorphism, there exists $h_{i+1} \colon P_{i+1} \to P_{i+2}$ such that

$$\varphi_i'\varphi_i - 1 - h_{i-1}\mathrm{d}_i = \mathrm{d}_{i+2}h_{i+1},$$

which is the homotopy equation in degree $i + 1$. $\square$

65.2 Projective Dimension

Definition 65.2. Let M be an R-module. The **projective dimenion of** M **over** R, denoted $\mathrm{pd}_R(M)$, is defined to be

$$\mathrm{pd}_R(M) = \inf \{\sup P \mid P \text{ is a projective resolution of } M \text{ over } R\}.$$

The **global dimension** of R, denoted $\mathrm{gldim}\, R$, is defined to be

$$\mathrm{gldim}\, R = \sup \{\mathrm{pd}_R(M) \mid M \text{ is an } R\text{-module}\}.$$

In fact, it is a theorem from Auslander that it is enough to take the supremum for finitely generated R-modules. That is,

$$\mathrm{gldim}\, R = \sup \{\mathrm{pd}_R(M) \mid M \text{ is a finitely generated } R\text{-module}\}.$$

Proposition 65.1. *Let $(R, \mathfrak{m})$ be a local ring and let M be a finitely generated nonzero R-module. Then*

$$\mathrm{pd}_R(M) = \inf_{i \in \mathbb{Z}} \left\{ \mathrm{Tor}_{i+1}^R(R/\mathfrak{m}, M) = 0 \right\}.$$

Thus the global dimension of R is equal to $\mathrm{pd}_R(R/\mathfrak{m})$.

Proof. Denote $n = \mathrm{pd}_R(M)$ and $m = \inf_{i \in \mathbb{N}} \left\{ \mathrm{Tor}_{i+1}^R(R/\mathfrak{m}, M) = 0 \right\}$. Choose a minimal projective resolution of M over R, say (P, d). Then

$$\mathrm{Tor}_{i+1}^R(R/\mathfrak{m}, M) \cong \mathrm{H}_{i+1}(R/\mathfrak{m} \otimes_R P) \cong 0$$

for all $i \geq n$. In particular, this implies $m \leq n$. On the other hand, since P is minimal, the differential on $R/\mathfrak{m} \otimes_R P$ is the zero map: $\overline{1} \otimes \mathrm{d} = 0$. In particular, this implies

$$\mathrm{Tor}_i^R(R/\mathfrak{m}, M) \cong P_i \ncong 0.$$

for all $0 \leq i \leq n$. Thus $m \geq n$. The last part of the proposition follows from symmetry of Tor. □

Proposition 65.2. *Suppose $(R, \mathfrak{m})$ is a regular local ring of dimension n. Then the global dimension of R is n.*

Proof. Let $x_1, \dots, x_n$ generate the maximal ideal $\mathfrak{m}$ of R. Then the Koszul complex $\mathcal{K}(x_1, \dots, x_n)$ is a minimal free resolution of $R/\mathfrak{m}$ over R. It follows that $n = \mathrm{pd}_R(R/\mathfrak{m})$ is equal to the global dimension of R. □

65.2.1 Minimal Projective Resolutions over a Noetherian Local Ring

Definition 65.3. Let $(R, \mathfrak{m})$ be a Noetherian local ring, let M be a finitely generated R-module, and let (P, d) be a projective resolution of M over R. We say P is **minimal** if $\mathrm{d}(P) \subset \mathfrak{m}P$.

Proposition 65.3. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, let M be a finitely generated R-module, and let (P, d) and (P', d') be two minimal projective resolutions of M over R. Then for each $i \in \mathbb{Z}$, the ranks of P_i and P_i' are finite and equal to each other. We denote this common rank by $\beta_i(M)$, and we call it the **ith Betti number of** M.*

Proof. Choose chain map $\alpha \colon (P, \mathrm{d}) \to (P', \mathrm{d}')$ and $\alpha' \colon (P', \mathrm{d}') \to (P, \mathrm{d})$ together with a homotopy $h \colon (P, \mathrm{d}) \to (P', \mathrm{d}')$ such that

$$\alpha'\alpha - 1 = \mathrm{d}'h + h\mathrm{d}. \tag{282}$$

Since $\mathrm{d}(P) \subset \mathfrak{m}P$ and $\mathrm{d}'(P') \subset \mathfrak{m}P'$, the homotopy equation (282) reduces to

$$\alpha'\alpha - 1 \equiv 0 \bmod \mathfrak{m}P'.$$

In other words, $\alpha \colon P \to P'$ induces an isomorphism $\overline{\alpha} \colon P/\mathfrak{m}P \to P'/\mathfrak{m}P'$ of graded $(R/\mathfrak{m})$-vector spaces. In particular, for each $i \in \mathbb{Z}$, we have isomorphisms

$$\overline{\alpha}_i \colon P_i/\mathfrak{m}P_i \to P_i'/\mathfrak{m}P_i'$$

of $(R/\mathfrak{m})$-vector spaces. Therefore by Nakayama's Lemma, for all $i \in \mathbb{Z}$, we have

$$\begin{aligned}
\mathrm{rank}(P_i) &= \dim_{R/\mathfrak{m}}(P_i/\mathfrak{m}P_i) \\
&= \dim_{R/\mathfrak{m}}(P_i'/\mathfrak{m}P_i') \\
&= \mathrm{rank}(P_i').
\end{aligned}$$

□

65.3 Definition of Tor

Definition 65.4. Let M and N be R-modules. We define the **Tor** with respect to M and N as follows: Choose a projective resolution of M, say (P, d), then set

$$\mathrm{Tor}^R(M,N) := \mathrm{H}(P \otimes_R N).$$

We need to check that this definition does not depend on the choice of a projective resolution of M, so suppose (P', d') is another projective resolution of M. By Theorem (65.1), there exists a homotopy equivalence from (P, d) to (P', d'), say $\varphi \colon (P, \mathrm{d}) \to (P, \mathrm{d}')$ and $\varphi' \colon (P', \mathrm{d}') \to (P, \mathrm{d})$ with homotopies $h \colon (P, \mathrm{d}) \to (P, \mathrm{d})$ and $h' \colon (P, \mathrm{d}) \to (P, \mathrm{d}')$ such that

$$\varphi'\varphi - 1 = \mathrm{d}h + h\mathrm{d} \qquad \text{and} \qquad \varphi\varphi' - 1 = \mathrm{d}'h' + h'\mathrm{d}'.$$

We claim that $P \otimes_R N$ is homotopically equivalent to $P' \otimes_R N$ via the pair of maps $\varphi \otimes 1 \colon P \otimes_R N \to P' \otimes_R N$ and $\varphi' \otimes 1 \colon P' \otimes_R N \to P \otimes_R N$ with homotopies given by $h \otimes 1 \colon P \otimes_R N \to P' \otimes_R N$ and $h' \otimes_R 1 \colon P' \otimes_R N \to P \otimes_R N$ respectively. Indeed, we have

$$\begin{aligned}
(\varphi' \otimes 1)(\varphi \otimes 1) - 1 \otimes 1 &= \varphi'\varphi \otimes 1 - 1 \otimes 1 \\
&= (\varphi'\varphi - 1) \otimes 1 \\
&= (\mathrm{d}h + h\mathrm{d}) \otimes 1 \\
&= \mathrm{d}h \otimes 1 + h\mathrm{d} \otimes 1 \\
&= \mathrm{d}^{P \otimes_R N}(h \otimes 1) + (h \otimes 1)\mathrm{d}^{P \otimes_R N}.
\end{aligned}$$

A similar calculation shows

$$(\varphi \otimes 1)(\varphi' \otimes 1) = \mathrm{d}^{P' \otimes_R N}(h' \otimes 1) + (h' \otimes 1)\mathrm{d}^{P' \otimes_R N}.$$

Thus $P \otimes_R N$ is homotopically equivalent to $P' \otimes_R N$ and hence

$$\mathrm{H}(P \otimes_R N) = \mathrm{H}(P' \otimes_R N).$$

Therefore the definition of Tor is well-defined.

65.4 Examples of Tor

Example 65.1. Let I and J be ideals in R. We compute $\mathrm{Tor}_1^R(R/I, R/J)$. First we tensor the short exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

with R/J to get the exact sequence

$$\begin{tikzcd}
 & I/IJ \arrow[r] & R/J \arrow[r] & R/(I+J) \arrow[r] & 0 \\
0 \cong \mathrm{Tor}_1^R(R, R/J) \arrow[r] & \mathrm{Tor}_1^R(R/I, R/J) \arrow[u, rounded corners, to path={-- ([xshift=2ex]\tikztostart.east) |- ([yshift=4ex]\tikztotarget.south) -| ([xshift=-4ex]\tikztotarget.west) -- (\tikztotarget.west)}] & & &
\end{tikzcd}$$

where $\mathrm{Tor}_1^R(R, R/J) \cong 0$ for trivial reasons. From here, it follows that $\mathrm{Tor}_1^R(R/I, R/J)$ is isomorphic to the kernel of the map $I/IJ \to R/J$, which is just $I \cap J/IJ$.

Example 65.2. Let $R = K[x,y,z]$, $I = \langle xy^2z^3, x^2yz^3, x^3yz^2, x^3y^2z, x^2y^3z, xy^3z^2 \rangle$, and $J = \langle x, y \rangle$. We compute $\mathrm{Tor}_i^R(R/I, R/J)$ for all i. An augmented free resolution for R/I comes from the permutohedron of order 3. It is given by

$$0 \longrightarrow R \xrightarrow{\varphi_3} R^6 \xrightarrow{\varphi_2} R^6 \xrightarrow{\varphi_1} R \longrightarrow R/I$$

where

$$\varphi_3 = \begin{pmatrix} xy \\ y^2 \\ yz \\ z^2 \\ xz \\ x^2 \end{pmatrix}, \qquad \varphi_2 = \begin{pmatrix} -x & 0 & 0 & 0 & 0 & y \\ y & -x & 0 & 0 & 0 & 0 \\ 0 & z & -y & 0 & 0 & 0 \\ 0 & 0 & z & -y & 0 & 0 \\ 0 & 0 & 0 & x & -z & 0 \\ 0 & 0 & 0 & 0 & x & -z \end{pmatrix}, \qquad \varphi_1 = \begin{pmatrix} xy^2z^3 & x^2yz^3 & x^3yz^2 & x^3y^2z & x^2y^3z & xy^3z^2 \end{pmatrix}.$$

We now truncate this resolution by replacing the R/I term with 0 and then tensor the truncated resolution with R/J to get:

$$0 \longrightarrow R/J \xrightarrow{\widetilde{\varphi}_3} (R/J)^6 \xrightarrow{\widetilde{\varphi}_2} (R/J)^6 \xrightarrow{\widetilde{\varphi}_1} R/J \longrightarrow 0$$

where $\overline{\varphi}_i$ is given by

$$\overline{\varphi}_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \overline{z}^2 \\ 0 \\ 0 \end{pmatrix}, \qquad \overline{\varphi}_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \overline{z} & 0 & 0 & 0 & 0 \\ 0 & 0 & \overline{z} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\overline{z} & 0 \\ 0 & 0 & 0 & 0 & 0 & -\overline{z} \end{pmatrix}, \qquad \overline{\varphi}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

From this, we see that

$$\begin{aligned} \mathrm{Tor}_0^R(R/I, R/J) &\cong R/\langle x, y\rangle \\ \mathrm{Tor}_1^R(R/I, R/J) &\cong (R/\langle x, y\rangle)^2 \oplus (R/\langle x, y, z\rangle)^4 \\ \mathrm{Tor}_2^R(R/I, R/J) &\cong (R/\langle x, y\rangle) \oplus \left(R/\langle x, y, z^2\rangle\right), \end{aligned}$$

and $\mathrm{Tor}_i^R(R/I, R/J) \cong 0$ for all $i \geq 3$.

65.5 Definition of Ext

Definition 65.5. Let M and N be R-modules. We define the **Ext** with respect to M and N as follows: Choose a projective resolution of M, say (P, d), then set

$$\mathrm{Ext}_R(M, N) := \mathrm{H}(\mathrm{Hom}_R^\star(P, N)).$$

We need to check that this definition does not depend on the choice of a projective resolution of M, so suppose (P', d') is another projective resolution of M. By Theorem (65.1), there exists a homotopy equivalence from (P, d) to (P', d'), say $\varphi\colon (P, \mathrm{d}) \to (P, \mathrm{d}')$ and $\varphi'\colon (P', \mathrm{d}') \to (P, \mathrm{d})$ with homotopies $h\colon (P, \mathrm{d}) \to (P, \mathrm{d})$ and $h'\colon (P, \mathrm{d}) \to (P, \mathrm{d}')$ such that

$$\varphi'\varphi - 1 = \mathrm{d}h + h\mathrm{d} \qquad \text{and} \qquad \varphi\varphi' - 1 = \mathrm{d}'h' + h'\mathrm{d}'.$$

We claim that $\mathrm{Hom}_R^\star(P, N)$ is homotopically equivalent to $\mathrm{Hom}_R^\star(P', N)$ via the pair of maps $\varphi^\star\colon \mathrm{Hom}_R^\star(P, N) \to \mathrm{Hom}_R^\star(P', N)$ and $\varphi'^\star\colon P' \otimes_R N \to P \otimes_R N$ with homotopies given by $h^\star\colon \mathrm{Hom}_R^\star(P, N) \to \mathrm{Hom}_R^\star(P, N)$ and $h'^\star\colon \mathrm{Hom}_R^\star(P', N) \to \mathrm{Hom}_R^\star(P', N)$ respectively. Indeed, if $\psi \in \mathrm{Hom}_R(P_i, N)$, then we have

$$\begin{aligned} (\varphi'^\star\varphi^\star - 1^\star)(\psi) &= \psi(\varphi'\varphi - 1) \\ &= \psi(\mathrm{d}h + h\mathrm{d}) \\ &= (\mathrm{d}^\star h^\star + h^\star \mathrm{d}^\star)(\psi). \end{aligned}$$

It follows that $\varphi'^\star\varphi^\star - 1^\star = \mathrm{d}^\star h^\star + h^\star \mathrm{d}^\star$. A similar calculation shows $\varphi^\star\varphi'^\star - 1^\star = \mathrm{d}^\star h'^\star + h'^\star \mathrm{d}^\star$. Thus $\mathrm{Hom}_R^\star(P, N)$ is homotopically equivalent to $\mathrm{Hom}_R^\star(P', N)$ and hence

$$\mathrm{H}(\mathrm{Hom}_R^\star(P, N)) = \mathrm{H}(\mathrm{Hom}_R^\star(P', N)).$$

Therefore the definition of Ext is well-defined.

65.6 Balance of Ext

We are striving for balance of Ext: the sketch of that proof goes like this: We have

$$\mathrm{Hom}_R(P, N) \xrightarrow[\varepsilon_*]{\simeq} \mathrm{Hom}_R(P, E) \xleftarrow[\tau^*]{\simeq} \mathrm{Hom}_R(M, E).$$

The quasiisomorphisms are: augment $P \xrightarrow[\simeq]{\tau} M$ and $N \xrightarrow[\simeq]{\varepsilon} E$. Then $\mathrm{Hom}_R(P, \mathrm{C}(\varepsilon)) \cong \mathrm{C}(\varepsilon_*)$ where $\mathrm{C}(\varepsilon)$ is exact because ε is quasiisomorphism and $\mathrm{Hom}_R(P, \mathrm{C}(\varepsilon))$ is exact because P is bounded below complex of projectives. Therefore $\mathrm{C}(\varepsilon_*)$ is exact, which implies ε_* is a quasiisomorphism.

Lemma 65.2. *Let I be a bounded above complex of injective R-modules. Then $\mathrm{Hom}_R(-, I)$ respects exact complexes. That is, if U is exact, then the complex $\mathrm{Hom}_R(U, I)$ is exact.*

Proposition 65.4. *Let P be a bounded below complex of projective R-modules and let I be a bounded above complex of injective R-modules. Then $\mathrm{Hom}_R(P, -)$ and $\mathrm{Hom}_R(-, I)$ respect quasiisomorphisms. That is, given a quasiisomorphism $\phi\colon U \to V$, the chain maps $\phi_*\colon \mathrm{Hom}_R(P, U) \to \mathrm{Hom}_R(P, V)$ and $\phi^*\colon \mathrm{Hom}_R(V, I) \to \mathrm{Hom}_R(U, I)$ are quasiisomorphisms.*

Proof. We have

$$\begin{aligned} V \xrightarrow[\simeq]{\phi} U &\implies \mathrm{C}(\phi) \text{ is exact} \\ &\implies \mathrm{Hom}_R(\mathrm{C}(\phi), I) \text{ is exact} \\ &\implies \mathrm{C}(\mathrm{Hom}_R(\phi, I)) \text{ is exact} \\ &\implies \mathrm{Hom}(\phi, I) = \phi_* \text{ is quasiisomorphism} \end{aligned}$$

□

Theorem 65.3. *(Balance for Ext) Let P be a projective resolution of an R-module M and let I be an injective resolution of an R-module N. Then*

$$\mathrm{Ext}^i_R(M,N) = \mathrm{H}_{-i}(\mathrm{Hom}_R(P,N)) \cong \mathrm{H}_{-i}(\mathrm{Hom}_R(P,I)) \cong \mathrm{H}_{-i}(\mathrm{Hom}_R(M,I)).$$

Proof. Resolution gives us quasiisomorphisms $P \xrightarrow[\simeq]{\tau} M$ and $N \xrightarrow[\simeq]{\varepsilon} I$. Thus

$$\mathrm{Hom}_R(P,N) \xrightarrow[\simeq]{\varepsilon_*} \mathrm{Hom}_R(P,I) \xleftarrow[\simeq]{\tau^*} \mathrm{Hom}_R(M,I).$$

□

65.7 Shift Property of Tor and Ext

Proposition 65.5. *Let A be a ring. Let M and N finitely generated A-modules, and for $i \geq 0$, let M_i and N_i denote there respective nonnegative syzygies. For $j \geq 1$, we have*

$$\begin{aligned} Ext_A^{j+1}(M_i,N) &\cong Ext_A^j(M_{i+1},N) \\ Tor^A_{j+1}(M_i,N) &\cong Tor^A_j(M_{i+1},N) \\ Tor^A_{j+1}(M,N_i) &\cong Tor^A_j(M,N_{i+1}) \end{aligned}$$

Moreover, assume A is Gorenstein, M and N are maximal Cohen-Macaulay, and for $i \leq -1$, let M_i and N_i denote their respective nonnegative syzygies. Then for $j \geq 1$, we have

$$\begin{aligned} Ext_A^{j+1}(M_i,N) &\cong Ext_A^j(M_{i+1},N) \\ Ext_A^{j}(M,N_i) &\cong Ext_A^{j+1}(M,N_{i+1}) \\ Tor^A_{j+1}(M_i,N) &\cong Tor^A_j(M_{i+1},N) \\ Tor^A_{j+1}(M,N_i) &\cong Tor^A_j(M,N_{i+1}) \end{aligned}$$

66 Differential Graded Algebras

66.1 DG Algebras

Let (A, d) be an R-complex. A **graded-multiplication** on A is a graded R-linear map $\mathrm{m}\colon A \otimes_R A \to A$ of the underlying graded R-modules. The universal mapping property on graded tensor products tells us that there exists a unique graded R-bilinear map $B_{\mathrm{m}}\colon A \times A \to A$ such that

$$B_{\mathrm{m}}(a,b) = \mathrm{m}(a \otimes b)$$

for all $(a,b) \in A \times A$. However since B_{m} is *uniquely* determined by m, we often identify B_{m} with m and simply think of m as a graded R-bilinear map. In fact, we often drop m altogether and simply denote this multiplication map by

$$\sum a_i \otimes b_i \mapsto \sum a_i b_i$$

for all $\sum a_i \otimes b_i \in A \otimes_R A$. At the end of the day, context will make everything clear.

Suppose m is a graded multiplication As the name of the definition suggests, a graded-multiplication on A must respect the grading. In particular, this means that if $a \in A_i$ and $b \in A_j$, then $ab \in A_{i+j}$. We can also impose other conditions on a graded-multiplication on A.

Definition 66.1. Let (A, d) be an R-complex and let m be a graded-multiplication on A.

1. We say m is **associative** if
$$a(bc) = (ab)c$$
for all $a, b, c \in A$.

2. We say m is **graded-commutative** if
$$ab = (-1)^i ba$$
for all $a \in A_i$ and $b \in A_j$ for all $i, j \in \mathbb{Z}$.

3. We say m is **strictly graded-commutative** if it is graded-commutative and satisfies the following extra property:
$$a^2 = 0$$
for all $a \in A_i$ for all i odd.

4. We say m is **unital** if there exists an $e \in A$ such that
$$ae = e = ea$$
for all $a \in A$.

5. We say a graded-multiplication satisfies **Leibniz law** if
$$\mathrm{d}(ab) = \mathrm{d}(a)b + (-1)^i a\mathrm{d}(b)$$
for all $a \in A_i$ and $b \in A_j$ for all $i, j \in \mathbb{Z}$. This is equivalent to m being a chain map!

6. We say $(A, \mathrm{m}, \mathrm{d})$ is a **differential graded R-algebra** (or **DG R-algebra**) if m is a graded-multiplication on A which satisfies conditions 1-5.

Remark 117. If the differential d and the multiplication map m are understood from context, then we will denote a differential graded R-algebra simply as "A" rather than as a triple "$(A, \mathrm{m}, \mathrm{d})$". We will also often introduce a differential grade R-algebra as "A" without specifying how the differential and multiplication map are to be denoted. In this case, the differential is denoted "d_A" and the multiplication map is denoted "m_A".

Definition 66.2. Let (A, d) and (A', d') be two DG R-algebras. A chain map $\varphi \colon (A, \mathrm{d}) \to (A', \mathrm{d}')$ is said to be a **DG-algebra morphism** if it respects multiplication and identity. In other words, we need
$$\varphi(ab) = \varphi(a)\varphi(b)$$
for all $a, b \in A$, and we need
$$\varphi(1) = 1.$$

We obtain a category of DG R-algebras.

66.1.1 Tensor Product of DG Algebras is DG Algebra

Proposition 66.1. *Let A and B be two DG R-algebras. Then $A \otimes_R B$ is is a DG R-algebra.*

Proof. Let $\mathrm{m}_A \colon A \otimes_R A \to A$ be the multiplication map for A and let $\mathrm{m}_B \colon B \otimes_R B \to B$ the multiplication map for B. Then
$$\begin{aligned}(A \otimes_R B) \otimes_R (A \otimes_R B) &\cong A \otimes_R (B \otimes_R (A \otimes_R B)) \\ &\cong A \otimes_R ((B \otimes_R A) \otimes_R B) \\ &\cong A \otimes_R ((A \otimes_R B) \otimes_R B) \\ &\cong\end{aligned}$$
$$A \otimes_R B)$$
□

Proposition 66.2. *Let (A, d) and (A', d') be two DG R-algebras. Then $(A \otimes_R A', \mathrm{d}^{A \otimes_R A'})$ is a DG R-algebra.*

Proof. Throughout this proof, denote $\mathrm{d}^{\otimes} := \mathrm{d}^{A \otimes_R A'}$. We define multiplication on $A \otimes_R A'$ by the formula
$$(a \otimes a')(b \otimes b') = (-1)^{i'j} ab \otimes a'b'. \tag{283}$$

for all $a \otimes a' \in A_i \otimes_R A_{i'}$ and $b \otimes b' \in A_j \otimes_R A_{j'}$. It is easy to check that (283) is associative and unital with with unit being $e_A \otimes e_{A'}$ where e_A is the unit of A and $e_{A'}$ is the unit of A'. Let us check that Leibniz law is satisfied. Let $a \otimes a', b \otimes b' \in A \otimes_R A'$. Then we have

$$
\begin{aligned}
\mathrm{d}^{\otimes}((a \otimes a')(b \otimes b')) &= (-1)^{i'j}\mathrm{d}^{\otimes}(ab \otimes a'b') \\
&= (-1)^{i'j}(\mathrm{d}(ab) \otimes a'b' + (-1)^{i+j} ab \otimes \mathrm{d}'(a'b')) \\
&= (-1)^{i'j}((\mathrm{d}(a)b + (-1)^i a\mathrm{d}(b)) \otimes a'b' + (-1)^{i+j} ab \otimes (\mathrm{d}'(a')b' + (-1)^{i'} a'\mathrm{d}'(b'))) \\
&= (-1)^{i'j}\mathrm{d}(a)b \otimes a'b' + (-1)^{i'j+i} a\mathrm{d}(b) \otimes a'b' + (-1)^{i'j+i+j} ab \otimes \mathrm{d}'(a')b' + (-1)^{i'j+i+j+i'} ab \otimes a'\mathrm{d}'(b') \\
&= (-1)^{i'j}\mathrm{d}(a)b \otimes a'b' + (-1)^{i+j(i'+1)} ab \otimes \mathrm{d}'(a')b' + (-1)^{i+i'+i'(j+1)} a\mathrm{d}(b) \otimes a'b' + (-1)^{i+i'+j+i'j}(ab \otimes a'\mathrm{d}'(b')) \\
&= (\mathrm{d}(a) \otimes a')(b \otimes b') + (-1)^i (a \otimes \mathrm{d}'(a'))(b \otimes b') + (-1)^{i+i'}(a \otimes a')(\mathrm{d}(b) \otimes b') + (-1)^{i+i'+j}(a \otimes a')(b \otimes \mathrm{d}'(b')) \\
&= (\mathrm{d}(a) \otimes a' + (-1)^i a \otimes \mathrm{d}'(a'))(b \otimes b') + (-1)^{i+i'}(a \otimes a')(\mathrm{d}(b) \otimes b' + (-1)^j b \otimes \mathrm{d}'(b')) \\
&= (\mathrm{d}^{\otimes}(a \otimes a'))(b \otimes b') + (-1)^{i+i'}(a \otimes a')(\mathrm{d}^{\otimes}(b \otimes b')).
\end{aligned}
$$

Thus $\mathrm{d}^{\otimes}$ satifies Leibniz law with respect to (283).

□

Proposition 66.3. *Let F be an R-complex of free modules and let B be a DG R-algebras. Then $\mathrm{Hom}_R^{\star}(F, B)$ is a DG R-algebra.*

Proof. Let $\{e_\lambda\}$ be a homogeneous basis for F indexed over a set Λ. We define a graded-multiplication on $\mathrm{Hom}_R^{\star}(F, B)$ as follows: let $\varphi \in \mathrm{Hom}_R^{\star}(F, B)_i$ and $\psi \in \mathrm{Hom}_R^{\star}(F, B)_j$, then we define $\varphi \smile \psi \in \mathrm{Hom}_R^{\star}(F, B)_{i+j}$ to be the unique graded R-linear map defined on basis elements $\{e_\lambda\}$ by

$$
(\varphi \smile \psi)(e_\lambda) = \varphi(s_-^{n-i} e_\lambda)\psi(s_+^{n-j} e_\lambda)
$$

for all $\lambda \in \Lambda$. Note that we are defining $\varphi \smile \psi$ on $\{e_\lambda\}$ and *then* extending R-linearly. Thus $(\varphi \smile \psi)(re_\lambda) = r\varphi(e_\lambda)\psi(e_\lambda)$ (not $r^2\varphi(e_\lambda)\psi(e_\lambda)$)! Similarly, $(\varphi \smile \psi)(e_\lambda + e_\mu) = \varphi(e_\lambda)\psi(e_\lambda) + \varphi(e_\mu)\psi(e_\mu)$ (not $\varphi(e_\lambda)\psi(e_\lambda) + \varphi(e_\mu)\psi(e_\mu) + \varphi(e_\lambda)\psi(e_\mu) + \varphi(e_\mu)\psi(e_\lambda)$)!
for all $a \in A$. Observe that

$$
\mathrm{d}(\varphi \cdot \psi) = \mathrm{d}\varphi \cdot \psi + (-1)^i \varphi \cdot \mathrm{d}\psi
$$

Indeed, we have

$$
\begin{aligned}
\mathrm{d}(\varphi \cdot \psi)(a) &= \mathrm{d}(\varphi(a)\psi(a)) \\
&= (\mathrm{d}\varphi(a))\psi(a) + (-1)^{i+n}\varphi(a)(\mathrm{d}\psi(a))
\end{aligned}
$$

Now we want to show $\cdot$ induces an R-bilinear map in homology. First let us show that $\mathrm{H}(\varphi \cdot \psi)$ is a graded R-linear map. Let □

66.1.2 Hom of DG Algebras is a Noncommutative DG Algebra

Proposition 66.4. *Let (A, d) be a DG R-algebras. Then $\mathrm{Hom}_R^{\star}(A, A')$ is a noncommutative DG R-algebra.*

Proof. We define multiplication on $\mathrm{Hom}_R^{\star}(A, A)$ via composition of functions. Thus if $\varphi\colon A \to A$ and $\psi\colon A \to A$ are graded homomorphisms of degrees i and j respectively. Then $\varphi\psi\colon A \to A'$ is given by

$$
(\varphi\psi)(a) = \varphi(\psi(a))
$$

for all $a \in A$. Note that $\varphi\psi$ is a graded R-homomorphism of degree $i + j$. Multiplication is easy seen to satisfy associativity and the identity map $1_A\colon A \to A$ serves as the identity element with respect to this multiplication. Moreover, Leibniz law is satisfied: we have

$$
\begin{aligned}
\mathrm{d}^{\star}(\varphi)\psi + (-1)^i\varphi\mathrm{d}^{\star}(\psi) &= (\mathrm{d}\varphi - (-1)^i\varphi\mathrm{d})\psi + (-1)^i\varphi(\mathrm{d}\psi - (-1)^j\psi\mathrm{d}) \\
&= \mathrm{d}\varphi\psi - (-1)^i\varphi\mathrm{d}\psi + (-1)^i\varphi\mathrm{d}\psi - (-1)^{i+j}\varphi\psi\mathrm{d} \\
&= \mathrm{d}\varphi\psi - (-1)^{i+j}\varphi\psi\mathrm{d} \\
&= \mathrm{d}^{\star}(\varphi\psi).
\end{aligned}
$$

for all $\varphi \in \mathrm{Hom}_R^{\star}(A, A)_i$ and $\psi \in \mathrm{Hom}_R^{\star}(A, A)_j$.

□

66.1.3 DG Algebra Embedding

Proposition 66.5. *Let A be a DG algebra. Define $\varphi\colon A \to \mathrm{Hom}_R^\star(A, A)$ by*

$$\varphi(a) = m_a$$

for all $a \in A$ where $m_a\colon A \to A$ is the homothety map, given by

$$m_a(x) = ax$$

for all $x \in A$. Then φ is an injective DG algebra homomorphism.

Proof. Note that $\varphi\colon A \to \mathrm{Hom}_R^\star(A, A)$ is easily seen to be a graded R-homomorphism. Let us check that it commutes with the differentials so that it is a chain map. Let $a \in A_i$. Observe that

$$\begin{aligned} \mathrm{d}m_a(x) &= \mathrm{d}(ax) \\ &= \mathrm{d}(a)x + (-1)^i a\mathrm{d}(x) \\ &= m_{\mathrm{d}(a)}(x) + (-1)^i m_a(\mathrm{d}(x)) \\ &= (m_{\mathrm{d}(a)} + (-1)^i m_a \mathrm{d})(x) \end{aligned}$$

for all $x \in A$. It follows that

$$\mathrm{d}m_a = m_{\mathrm{d}(a)} + (-1)^i m_a \mathrm{d}.$$

Thus

$$\begin{aligned} (\mathrm{d}^\star \varphi)(a) &= \mathrm{d}^\star(\varphi(a)) \\ &= \mathrm{d}^\star m_a \\ &= \mathrm{d}m_a - (-1)^i m_a \mathrm{d} \\ &= m_{\mathrm{d}(a)} \\ &= \varphi(\mathrm{d}(a)) \\ &= (\varphi\mathrm{d})(a), \end{aligned}$$

and so φ commutes with the differentials. Thus φ is a chain map.

Let us now check that φ is a DG algebra homomorphism. Let $a, b \in A$. Observe that we have

$$\begin{aligned} (m_a m_b)(x) &= m_a(m_b(x)) \\ &= m_a(bx) \\ &= a(bx) \\ &= (ab)x \\ &= m_{ab}(x) \end{aligned}$$

for all $x \in A$. It follows that $m_a m_b = m_{ab}$. Thus

$$\begin{aligned} \varphi(ab) &= m_{ab} \\ &= m_a m_b \\ &= \varphi(a)\varphi(b), \end{aligned}$$

and hence φ respects addition, and also $\varphi(1) = 1_A$, where e is the identity in A and 1_A is the identity in $\mathrm{Hom}_R^\star(A, A)$.

Finally, note that φ is injective. Indeed, suppose $m_a = 0$ for some $a \in A$, then

$$\begin{aligned} 0 &= m_a(1) \\ &= a \cdot 1 \\ &= a \end{aligned}$$

implies $\ker \varphi = 0$. □

Proposition 66.6. *Let R be a ring, let I be an ideal in R, and let (A, d) be a DG algebra resolution of R/I over R. Then I kills* $\mathrm{H}(A)$.

Proof. The embedding of DG Algebras $A \to \mathrm{Hom}_R(A, A)$, given by $a \mapsto m_a$, induces a map in the 0th homology

$$R/I \to \{\text{homotopy classes of chain maps } A \to A\}.$$

In particular, if x is in I, then m_x must be null-homotopic. Hence I kills $\mathrm{H}(A)$. □

Proposition 66.7. *Let R be a ring, let I be an ideal in R, and let (A, d) and (A', d') be two DG algebra resolutions of R/I over R. Then $\mathrm{Hom}^{\star}_R(A, A)$ is homotopically equivalent to $\mathrm{Hom}^{\star}_R(A', A')$.*

Proof. Since A and A' are homotopically equivalent, we may choose chain maps $\varphi \colon A \to A'$ and $\varphi' \colon A' \to A$ together with homotopies $h \colon A \to A'$ and $h' \colon A \to A'$ where

$$\varphi'\varphi - 1 = \mathrm{d}h + h\mathrm{d} \qquad \text{and} \qquad \varphi\varphi' - 1 = \mathrm{d}'h' + h'\mathrm{d}'.$$

Define $\gamma \colon \mathrm{Hom}^{\star}_R(A, A) \to \mathrm{Hom}^{\star}_R(A', A')$ by

$$\gamma(\alpha) = \varphi\alpha\varphi'$$

for all $\alpha \in \mathrm{Hom}^{\star}_R(A, A)$. We claim that γ is a chain map. Indeed, it is graded since φ and φ' have degree 0. It is an R-module homomorphism since if $r, s \in R$ and $\alpha, \beta \in \mathrm{Hom}^{\star}_R(A, A)$, then we have

$$\begin{aligned}
\gamma(r\alpha + s\beta) &= \varphi(r\alpha + s\beta)\varphi' \\
&= \varphi r\alpha\varphi' + \varphi s\phi\varphi' \\
&= r\varphi\alpha\varphi' + s\varphi\beta\varphi' \\
&= r\gamma(\alpha) + s\gamma(\beta).
\end{aligned}$$

It commutes with the differentials since if $\alpha \in \mathrm{Hom}^{\star}_R(A, A)_i$, then we have

$$\begin{aligned}
(\mathrm{d}^{\star}_{A'}\gamma)(\alpha) &= \mathrm{d}^{\star}_{A'}(\gamma(\alpha)) \\
&= \mathrm{d}^{\star}_{A'}(\varphi\alpha\varphi') \\
&= \mathrm{d}'\varphi\alpha\varphi' + (-1)^i\varphi\alpha\varphi'\mathrm{d}' \\
&= \varphi\mathrm{d}\alpha\varphi' + (-1)^i\varphi\alpha\mathrm{d}\varphi' \\
&= \varphi(\mathrm{d}\alpha + (-1)^i\alpha\mathrm{d})\varphi' \\
&= \gamma(\mathrm{d}\alpha + (-1)^i\alpha\mathrm{d}) \\
&= \gamma(\mathrm{d}^{\star}_A(\alpha)) \\
&= (\gamma\mathrm{d}^{\star}_A)(\alpha).
\end{aligned}$$

Similarly, we define $\gamma' \colon \mathrm{Hom}^{\star}_R(A', A') \to \mathrm{Hom}^{\star}_R(A, A)$ by

$$\gamma'(\alpha') = \varphi'\alpha'\varphi$$

for all $\alpha' \in \mathrm{Hom}^{\star}_R(A', A')$. We claim that $\gamma'\gamma \sim 1_{\mathrm{Hom}^{\star}_R(A,A)}$ and $\gamma'\gamma \sim 1_{\mathrm{Hom}^{\star}_R(A',A')}$. It suffices to show that $\gamma'\gamma \sim 1_{\mathrm{Hom}^{\star}_R(A,A)}$ as the other homotopy equivalence will follows by a similar argument. Let $H \colon \mathrm{Hom}^{\star}_R(A, A) \to \mathrm{Hom}^{\star}_R(A, A)$ be defined by

$$H(\alpha) = h\alpha\mathrm{d}h + h\alpha h\mathrm{d} + h\alpha + \alpha h$$

for all $\alpha \in \mathrm{Hom}^{\star}_R(A, A)$. Now let $\alpha \in \mathrm{Hom}^{\star}_R(A, A)_i$. Then we have

$$\begin{aligned}
(\gamma'\gamma - 1)(\alpha) &= (\gamma'\gamma)(\alpha) - \alpha \\
&= \gamma'(\gamma(\alpha)) - \alpha \\
&= \gamma'(\varphi\alpha\varphi') - \alpha \\
&= \varphi'\varphi\alpha\varphi'\varphi - \alpha \\
&= (\mathrm{d}h + h\mathrm{d} + 1)\alpha(\mathrm{d}h + h\mathrm{d} + 1) - \alpha \\
&= \mathrm{d}h\alpha\mathrm{d}h + \mathrm{d}h\alpha h\mathrm{d} + \mathrm{d}h\alpha + h\mathrm{d}\alpha\mathrm{d}h + h\mathrm{d}\alpha h\mathrm{d} + h\mathrm{d}\alpha + \alpha\mathrm{d}h + \alpha h\mathrm{d} + \alpha - \alpha \\
&= \mathrm{d}(h\alpha\mathrm{d}h + h\alpha h\mathrm{d}) + h\mathrm{d}\alpha\mathrm{d}h + h\mathrm{d}\alpha h\mathrm{d} + (\mathrm{d}h + h\mathrm{d})\alpha + \alpha(\mathrm{d}h + h\mathrm{d}) \\
\\
&= \mathrm{d}(h\alpha\mathrm{d}h + h\alpha h\mathrm{d}) + h\mathrm{d}\alpha\mathrm{d}h + h\mathrm{d}\alpha h\mathrm{d} \\
&= \mathrm{d}(h\alpha\mathrm{d}h + h\alpha h\mathrm{d}) + (-1)^i h\alpha h\mathrm{d}\mathrm{d} + h\mathrm{d}\alpha\mathrm{d}h + h\mathrm{d}\alpha h\mathrm{d} \\
&= \mathrm{d}(h\alpha\mathrm{d}h + h\alpha h\mathrm{d}) + (-1)^i(h\alpha\mathrm{d}h + h\alpha h\mathrm{d} - h\alpha\mathrm{d}h)\mathrm{d} + h\mathrm{d}\alpha\mathrm{d}h + h\mathrm{d}\alpha h\mathrm{d} \\
&= \mathrm{d}(h\alpha\mathrm{d}h + h\alpha h\mathrm{d}) + (-1)^i(h\alpha\mathrm{d}h + h\alpha h\mathrm{d})\mathrm{d} + h\mathrm{d}\alpha\mathrm{d}h + h\mathrm{d}\alpha h\mathrm{d} - (-1)^i h\alpha\mathrm{d}h\mathrm{d} \\
&= \mathrm{d}(h\alpha\mathrm{d}h + h\alpha h\mathrm{d}) + (-1)^i(h\alpha\mathrm{d}h + h\alpha h\mathrm{d})\mathrm{d} + (h\mathrm{d}\alpha\mathrm{d}h + h\mathrm{d}\alpha h\mathrm{d}) - (-1)^i(h\alpha\mathrm{d}\mathrm{d}h + h\alpha\mathrm{d}h\mathrm{d}) \\
&= \mathrm{d}H(\alpha) + (-1)^i H(\alpha)\mathrm{d} + H(\mathrm{d}\alpha) - (-1)^i H(\alpha\mathrm{d}) \\
&= \mathrm{d}H(\alpha) + (-1)^i H(\alpha)\mathrm{d} + H(\mathrm{d}\alpha) - (-1)^i H(\alpha\mathrm{d}) \\
&= \mathrm{d}H(\alpha) - (-1)^{i+1} H(\alpha)\mathrm{d} + H(\mathrm{d}\alpha - (-1)^i\alpha\mathrm{d}) \\
&= \mathrm{d}^{\star}(H(\alpha)) + H(\mathrm{d}^{\star}(\alpha)) \\
&= (\mathrm{d}^{\star}H + H\mathrm{d}^{\star})(\alpha)
\end{aligned}$$

□

$$
\begin{aligned}
(\gamma'\gamma - 1)(\alpha) &= (\gamma'\gamma)(\alpha) - \alpha \\
&= \gamma'(\gamma(\alpha)) - \alpha \\
&= \gamma'(\varphi\alpha\varphi') - \alpha \\
&= \varphi'\varphi\alpha\varphi'\varphi - \alpha \\
&= (\mathrm{d}h + h\mathrm{d} + 1)\alpha(\mathrm{d}h + h\mathrm{d} + 1) - \alpha \\
&= \mathrm{d}h\alpha\mathrm{d}h + \mathrm{d}h\alpha h\mathrm{d} + \mathrm{d}h\alpha + h\mathrm{d}\alpha\mathrm{d}h + h\mathrm{d}\alpha h\mathrm{d} + h\mathrm{d}\alpha + \alpha\mathrm{d}h + \alpha h\mathrm{d} + \alpha - \alpha \\
&= \mathrm{d}(h\alpha\mathrm{d}h + h\alpha h\mathrm{d}) + h\mathrm{d}\alpha\mathrm{d}h + h\mathrm{d}\alpha h\mathrm{d} + (\mathrm{d}h + h\mathrm{d})\alpha + \alpha(\mathrm{d}h + h\mathrm{d})
\end{aligned}
$$

$$
\begin{aligned}
&= \mathrm{d}h\alpha + \alpha h\mathrm{d} + h\mathrm{d}\alpha + \alpha\mathrm{d}h \\
&= \mathrm{d}h\alpha - (-1)^i\mathrm{d}\alpha h + (-1)^i h\alpha\mathrm{d} + \alpha h\mathrm{d} + h\mathrm{d}\alpha + (-1)^i\mathrm{d}\alpha h - (-1)^i h\alpha\mathrm{d} + \alpha\mathrm{d}h \\
&= \mathrm{d}(h\alpha - (-1)^i\alpha h) + (-1)^i(h\alpha - (-1)^i\alpha h)\mathrm{d} + h\mathrm{d}\alpha + (-1)^i\mathrm{d}\alpha h - (-1)^i h\alpha\mathrm{d} + \alpha\mathrm{d}h \\
&= \mathrm{d}H(\alpha) + (-1)^i H(\alpha)\mathrm{d} + H(\mathrm{d}\alpha) - (-1)^i H(\alpha\mathrm{d}) \\
&= \mathrm{d}H(\alpha) + (-1)^i H(\alpha)\mathrm{d} + H(\mathrm{d}\alpha) - (-1)^i H(\alpha\mathrm{d}) \\
&= \mathrm{d}H(\alpha) - (-1)^{i+1} H(\alpha)\mathrm{d} + H(\mathrm{d}\alpha - (-1)^i\alpha\mathrm{d}) \\
&= \mathrm{d}^\star(H(\alpha)) + H(\mathrm{d}^\star(\alpha)) \\
&= (\mathrm{d}^\star H + H\mathrm{d}^\star)(\alpha)
\end{aligned}
$$

66.1.4 Direct Sum of DG Algebras is DG Algebra

Proposition 66.8. *Let (A, d) and (A', d') be two DG R-algebras. Then $(A \oplus_R A', \mathrm{d}^{A\oplus_R A'})$ is a DG R-algebra.*

Proof. Throughout this proof, denote $\mathrm{d}^\oplus := \mathrm{d}^{A\oplus_R A'}$. We define multiplication on $A \oplus_R A'$ by the formula

$$(a, a')(b, b') = (-1)^{i'j}(ab, a'b') \tag{284}$$

for all $a \otimes a' \in A_i \otimes_R A_{i'}$ and $b \otimes b' \in A_j \otimes_R A_{j'}$. It is easy to check that (283) is associative and unital with with unit being $e_A \otimes e_{A'}$ where e_A is the unit of A and $e_{A'}$ is the unit of A'. Let us check that Leibniz law is satisfied. Let $a \otimes a', b \otimes b' \in A \otimes_R A'$. Then we have

$$
\begin{aligned}
\mathrm{d}^\oplus((a,a')(b,b')) &= (-1)^{i'j}\mathrm{d}^\oplus(ab, a'b') \\
&= (-1)^{i'j}\mathrm{d}^\oplus(ab, a'b') \\
&= (-1)^{i'j}((\mathrm{d}(a)b + (-1)^i a\mathrm{d}(b)) \otimes a'b' + (-1)^{i+j}ab \otimes (\mathrm{d}'(a')b' + (-1)^{i'}a'\mathrm{d}'(b'))) \\
&= (-1)^{i'j}\mathrm{d}(a)b \otimes a'b' + (-1)^{i'j+i}a\mathrm{d}(b) \otimes a'b' + (-1)^{i'j+i+j}ab \otimes \mathrm{d}'(a')b' + (-1)^{i'j+i+j+i'}ab \otimes a'\mathrm{d}'(b') \\
&= (-1)^{i'j}\mathrm{d}(a)b \otimes a'b' + (-1)^{i+j(i'+1)}ab \otimes \mathrm{d}'(a')b' + (-1)^{i+i'+i'(j+1)}a\mathrm{d}(b) \otimes a'b' + (-1)^{i+i'+j+i'j}(ab \otimes a'\mathrm{d}'(b')) \\
&= (\mathrm{d}(a) \otimes a')(b \otimes b') + (-1)^i(a \otimes \mathrm{d}'(a'))(b \otimes b') + (-1)^{i+i'}(a \otimes a')(\mathrm{d}(b) \otimes b') + (-1)^{i+i'+j}(a \otimes a')(b \otimes \mathrm{d}'(b')) \\
&= (\mathrm{d}(a) \otimes a' + (-1)^i a \otimes \mathrm{d}'(a'))(b \otimes b') + (-1)^{i+i'}(a \otimes a')(\mathrm{d}(b) \otimes b' + (-1)^j b \otimes \mathrm{d}'(b')) \\
&= (\mathrm{d}^\otimes(a \otimes a'))(b \otimes b') + (-1)^{i+i'}(a \otimes a')(\mathrm{d}^\otimes(b \otimes b')).
\end{aligned}
$$

Thus $\mathrm{d}^\otimes$ satisfies Leibniz law with respect to (283). □

66.1.5 Localization of DG-Algebra

Let (A, d) be a DG R-algebra and let S be a multiplicatively-closed subset of A consisting of homogeneous elements of even degree. The **localization of** (A, d) **with respect to** S is the R-complex (A_S, d_S) where A_S is the graded R-module whose component in degree i is

$$(A_S)_i = \{a/s \mid j \in \mathbb{N}, a \in A_{i+j}, \text{ and } s \in A_j\}.$$

The differential d_S is defined as follows: if $a \in A_{i+j}$ and $s \in A_j$, then $a/s \in (A_S)_i$ and

$$\mathrm{d}_S\left(\frac{a}{s}\right) = \frac{\mathrm{d}(a)s - (-1)^{i+j}a\mathrm{d}(s)}{s^2}.$$

To see that this is well-defined, suppose $a/s = a'/s'$ with both $|s|$ and $|s'|$ even, so $as' = a's$ and $|a| = |a'|$. Applying the differential gives us

$$\mathrm{d}(a)s' + (-1)^{|a|}a\mathrm{d}(s') = \mathrm{d}(a')s + (-1)^{|a'|}a'\mathrm{d}(s).$$

We need to show that

$$\frac{\mathrm{d}(a)s - (-1)^{|a|}a\mathrm{d}(s)}{s^2} = \frac{\mathrm{d}(a')s' - (-1)^{|a'|}a'\mathrm{d}(s')}{s'^2}.$$

Or in other words, we need to show

$$\left(\mathrm{d}(a)s - (-1)^{|a|}a\mathrm{d}(s)\right)s'^2 = \left(\mathrm{d}(a')s' - (-1)^{|a'|}a'\mathrm{d}(s')\right)s^2.$$

We have

$$\begin{aligned}
\left(\mathrm{d}(a)s - (-1)^{|a|}a\mathrm{d}(s)\right)s'^2 &= \mathrm{d}(a)ss'^2 - (-1)^{|a|}a\mathrm{d}(s)s'^2 \\
&= \mathrm{d}(a)s'^2s - (-1)^{|a|}as'^2\mathrm{d}(s) \\
&= (\mathrm{d}(a')s + (-1)^{|a'|}a'\mathrm{d}(s) - (-1)^{|a|}a\mathrm{d}(s'))s's - (-1)^{|a|}a'ss'\mathrm{d}(s) \\
&= \mathrm{d}(a')s's^2 + (-1)^{|a'|}a'\mathrm{d}(s)s's - (-1)^{|a|}a\mathrm{d}(s')s's - (-1)^{|a|}a'ss'\mathrm{d}(s) \\
&= \mathrm{d}(a')s's^2 + (-1)^{|a'|}a'\mathrm{d}(s)s's - (-1)^{|a|}a'\mathrm{d}(s')s^2 - (-1)^{|a|}a'ss'\mathrm{d}(s) \\
&= \mathrm{d}(a')s's^2 - (-1)^{|a|}a'\mathrm{d}(s')s^2 + (-1)^{|a'|}a'\mathrm{d}(s)s's - (-1)^{|a|}a'ss'\mathrm{d}(s) \\
&= \mathrm{d}(a')s's^2 - (-1)^{|a'|}a'\mathrm{d}(s')s^2 \\
&= \left(\mathrm{d}(a')s' - (-1)^{|a'|}a'\mathrm{d}(s')\right)s^2
\end{aligned}$$

Next, we need to check that $\mathrm{d}_S^2 = 0$. We have

$$\begin{aligned}
\mathrm{d}_S^2\left(\frac{a}{s}\right) &= \mathrm{d}_S\left(\frac{\mathrm{d}(a)s - (-1)^{|a|}a\mathrm{d}(s)}{s^2}\right) \\
&= \frac{\mathrm{d}\left(\mathrm{d}(a)s - (-1)^{|a|}a\mathrm{d}(s)\right)s^2 - (-1)^{|a|-1}\left(\mathrm{d}(a)s - (-1)^{|a|}a\mathrm{d}(s)\right)\mathrm{d}(s^2)}{s^4} \\
&= \frac{((-1)^{|a|-1}\mathrm{d}(a)\mathrm{d}(s) - (-1)^{|a|}\mathrm{d}(a)\mathrm{d}(s))s^2 + (-1)^{|a|}\left(\mathrm{d}(a)s - (-1)^{|a|}a\mathrm{d}(s)\right)2s\mathrm{d}(s)}{s^4} \\
&= \frac{(-1)^{|a|-1}2\mathrm{d}(a)\mathrm{d}(s)s^2 + (-1)^{|a|}2\mathrm{d}(a)\mathrm{d}(s)s^2 - 2a\mathrm{d}(s)^2s}{s^4} \\
&= \frac{0}{s^4} \\
&= 0.
\end{aligned}$$

Next, we need to check that Leibniz law is satisfies. We have

$$\begin{aligned}
\mathrm{d}_S\left(\frac{aa'}{ss'}\right) &= \frac{\mathrm{d}(aa')ss' - (-1)^{|a|+|a'|}aa'\mathrm{d}(ss')}{s^2s'^2} \\
&= \frac{\mathrm{d}(aa')ss' - (-1)^{|a|+|a'|}aa'\mathrm{d}(ss')}{s^2s'^2} \\
&= \frac{\mathrm{d}(a)a'ss' + (-1)^{|a|}a\mathrm{d}(a')ss' - (-1)^{|a|+|a'|}aa'\mathrm{d}(s)s' - (-1)^{|a|+|a'|}aa's\mathrm{d}(s')}{s^2s'^2} \\
&= \frac{\mathrm{d}(a)sa's' - (-1)^{|a|}a\mathrm{d}(s)a's' + (-1)^{|a|}as\mathrm{d}(a')s' - (-1)^{|a'|+|a|}asa'\mathrm{d}(s')}{s^2s'^2} \\
&= \frac{\mathrm{d}(a)sa's' - (-1)^{|a|}a\mathrm{d}(s)a's' + (-1)^{|a|}as\mathrm{d}(a')s' - (-1)^{|a'|+|a|}asa'\mathrm{d}(s')}{s^2s'^2} \\
&= \frac{\mathrm{d}(a)sa's' - (-1)^{|a|}a\mathrm{d}(s)a's'}{s^2s'^2} + \frac{(-1)^{|a|}as\mathrm{d}(a')s' - (-1)^{|a'|+|a|}asa'\mathrm{d}(s')}{s^2s'^2} \\
&= \left(\frac{\mathrm{d}(a)s - (-1)^{|a|}a\mathrm{d}(s)}{s^2}\right)\frac{a'}{s'} + (-1)^{|a|}\frac{a}{s}\left(\frac{\mathrm{d}(a')s' - (-1)^{|a'|}a'\mathrm{d}(s')}{s'^2}\right) \\
&= \mathrm{d}_S\left(\frac{a}{s}\right)\frac{a'}{s'} + (-1)^{|a|}\frac{a}{s}\mathrm{d}_S\left(\frac{a'}{s'}\right).
\end{aligned}$$

66.2 DG Modules

Definition 66.3. Let (A, d_A) be a DG R-algebra. A (right) **differential graded A-module** (or DG A-module for short) is an R-complex (M, d_M) equipped with a chain map

$$\star\colon (M \otimes_R A, \mathrm{d}^{M\otimes_R A}) \to (M, \mathrm{d}_M)$$

denoted $u \otimes a \mapsto \star(u \otimes a)$ (or just ua if context is clear). In other words, M has an A-module structure which behaves well with respect to the Leibniz law:

$$\mathrm{d}_M(ua) = \mathrm{d}_M(u)a + (-1)^i u\mathrm{d}_A(a)$$

for all $u \in M_i$ and $a \in A$. If (I, d_I) is an R-complex with $I \subset A$ and $\star$ being the usual multiplication map, then say (I, d_I) is a **DG ideal** in (A, d_A).

Definition 66.4. Let (A, d) be a DG R-algebra and let (M, d_M) and (N, d_N) be DG A-modules. A chain map $\varphi\colon (M, \mathrm{d}_M) \to (N, \mathrm{d}_N)$ is said to be a **DG-module morphism** if it respects A-scaling. In other words, we need

$$\varphi(ua) = \varphi(u)a$$

for all $u \in M$ and $a \in A$ (so the underlying map $\varphi\colon M \to N$ of A-modules is an A-module homomorphism). The category of (right) differential graded A-modules is denoted $\mathrm{Mod}_{(A,\mathrm{d})}$.

Obtaining a Differential Graded A-Module from an R-Complex

Example 66.1. Let (A, d_A) be a differential graded R-algebra and let (M, d_M) be an R-complex. Then the R-complex $(M \otimes_R A, \mathrm{d}^{M\otimes_R A})$ is a DG A-module.

66.2.1 Completion of DG Algebra with respect to an Ideal

Let (A, d) be a DG R-algebra and let (I, d) be a DG ideal in (A, d). We define the I-adic DG algebra, denoted $(\widehat{A}_I, \widehat{\mathrm{d}}_I)$, where

$$\widehat{A}_I := \varprojlim A/I^n = \{(\overline{a_n}) \in A/I^n \mid a_n \equiv a_m \bmod I^m \text{ whenever } n \geq m\}$$

and where $\widehat{\mathrm{d}}_I$ is defined pointwise:

$$\widehat{\mathrm{d}}_I((\overline{a_n})) = (\overline{\mathrm{d}(a_n)})$$

for all $(\overline{a_n}) \in \widehat{A}_I$. Note that the ith homogeneous component of $\widehat{A}_I$ is

$$(\widehat{A}_I)_i = \varprojlim_n (A_i/I_i^n) = \{(\overline{a_n}) \in A_i/I_i^n \mid a_n \equiv a_m \bmod I_i^m \text{ whenever } n \geq m\}.$$

In particular, if $(\overline{a_n}) \in (\widehat{A}_I)_i$, then $a_n \in A_i$ for all $i \geq 0$. Suppose $(\overline{a_n}) \in \ker \widehat{\mathrm{d}}_I$. Then $\mathrm{d}(a_n) \in I^n$ for all $n \in \mathbb{N}$.

66.2.2 Blowing up DG Algebra with respect to an Ideal

Let (A, d) be a DG R-algebra and let I be a DG ideal in A. Let

$$\mathrm{N}_I(A) := A \oplus A/I \oplus A/I^2 \oplus \cdots = A + (A/I)t + (A/I^2)t^2 + \cdots$$

and let $\mathrm{d}^{\mathrm{N}_I(A)} \colon \mathrm{N}_I(A) \to \mathrm{N}_I(A)$ be the unique graded linear map such that

$$\mathrm{d}^{\mathrm{N}_I(A)}(\overline{a}t^n) = \overline{\mathrm{d}(a)}t^{n-1},$$

for all $\overline{a}t^n \in (A/I^n)t^n$[10].

Proposition 66.9. *Let (A, d) be a DG R-algebra and let I be a DG ideal in A such that $I \subset A_+$. Then*

$$\mathrm{H}_n(\mathrm{N}_I(A)) = 0 \textit{ for } n \gg 0 \textit{ if and only if } \mathrm{H}(A) = 0.$$

Proof. Suppose first that $\mathrm{H}(A) = 0$ and assume for a contradiction that $\mathrm{H}_n(\mathrm{N}_I(A)) \neq 0$ for $n \gg 0$. Choose a $(\overline{a}$
Suppose $k \in \mathbb{Z}$ such that $\mathrm{H}_i(A) = 0$ for all $i \geq k$. We wish to show that □

Note that

$$\mathrm{H}_n(\mathrm{N}_I(A)) \cong \frac{\mathrm{d}^{-1}(I^{n-1})}{\mathrm{im}\ \mathrm{d} + I^n}.$$

Thus, we want to show that

$$\mathrm{d}^{-1}(I^{n-1}) = \mathrm{im}\ \mathrm{d} + I^n$$

for $n \gg 0$. The theorem would follow at once if we can show that

$$\mathrm{d}^{-1}(I^{n-1}) \subset I^{n-1}$$

for $n \gg 0$. Assume for a contradiction that we can find $a_n \in A \backslash I^n$ such that $\mathrm{d}(a_n) \in I^n$.

We claim that $\mathrm{H}_i(A) \cong \mathrm{H}_i(\mathrm{N}_I(A))$ for all i

66.3 The Koszul Complex

Throughout this subsection, let $\underline{x} = x_1, \ldots, x_n$ be a sequence in R. We will construct a DG R-algebra called the **Koszul complex** of $\underline{x}$. Before doing so, we need to discuss ordered sets.

66.3.1 Ordered Sets

An **ordered set** is a set with a total linear ordering on it. The **ordered set** $[n]$ is the set $\{1, \ldots, n\}$ equipped with the natural ordering $1 < \cdots < n$. Let σ be a subset of $\{1, \ldots, n\}$. Then the natural ordering on $\{1, \ldots, n\}$ induces a natural ordering on σ. If we want to think of σ as a set equipped with this natural ordering, then we will write $[\sigma]$. If $\sigma = \{\lambda_1, \ldots, \lambda_k\}$, where $1 \leq \lambda_1 < \cdots < \lambda_k \leq n$, then we will also write $[\sigma] = [\lambda_1, \ldots, \lambda_k]$. If we write "suppose $[\sigma] = [\lambda_1, \ldots, \lambda_k]$", then it is understood that $1 \leq \lambda_1 < \cdots < \lambda_k \leq n$. For each $i \in \mathbb{Z}$ such that $0 \leq i \leq n$, we denote

$$S_i[n] := \{\sigma \subseteq \{1, \ldots, n\} \mid |\sigma| = i\}.$$

Compliments

Let $\sigma \subseteq [n]$. We denote by $\sigma^\star$ to be the **compliment** of σ in $[n]$, that is,

$$\sigma^\star := [n] \backslash \sigma.$$

If $[\sigma] = [\lambda_1, \ldots, \lambda_k]$, then we write $\sigma^\star = [\lambda_1^\star, \ldots, \lambda_{n-k}^\star]$.

[10] Here, the $\overline{a}$ is understood to be a coset in A/I^n with represenative $a \in A$.

Signature

Let σ and τ be two disjoint subsets of $\{1, \dots, n\}$. Suppose that

$$[\sigma] = [\lambda_1, \dots, \lambda_k] \quad \text{and} \quad [\sigma'] = [\lambda_{k+1}, \dots, \lambda_{k+m}].$$

Then

$$[\sigma \cup \sigma'] = [\lambda_{\pi(1)}, \dots, \lambda_{\pi(k+m)}],$$

where $\pi \colon S_{k+m} \to S_{k+m}$ is the permutation which puts everything in the correct order. We define

$$\langle \sigma, \tau \rangle := \operatorname{sign}(\pi).$$

Remark 118. Let $\lambda \in \{1, \dots, n\}$ and let $\sigma \subseteq \{1, \dots, n\}$. To clean notation, we often drop the curly brackets around singleton elements $\{\lambda\}$ in what follows. For instance, we will write $\sigma \backslash \lambda$ instead of $\sigma \backslash \{\lambda\}$ and $\sigma \cup \lambda$ instead of $\sigma \cup \{\lambda\}$. We will also write $\langle \lambda, \sigma \rangle$ (or $\langle \sigma, \lambda \rangle$) instead of $\langle \{\lambda\}, \sigma \rangle$ (respectively $\langle \sigma, \{\lambda\} \rangle$).

Example 66.2. Consider $n = 4$. We perform some computations:

$$\begin{aligned}
\langle 2, \{1,4\} \rangle &= -1 \\
\langle 2, 3 \rangle &= 1 \\
\langle 3, 2 \rangle &= -1 \\
\langle \{1,4\}, 2 \rangle &= -1 \\
\langle 2, \{1,3,4\} \rangle &= -1 \\
\langle \{1,3,4\}, 2 \rangle &= 1 \\
\langle \{1,3\}, \{2,4\} \rangle &= -1 \\
\langle \{2,4\}, \{1,3\} \rangle &= -1
\end{aligned}$$

Signature Identities

Proposition 66.10. *Let σ, τ, and $\{\lambda\}$ be mutually disjoint subsets of $\{1, \dots, n\}$. Then*

$$\langle \lambda, \sigma \cup \tau \rangle = \langle \lambda, \sigma \rangle \langle \lambda, \tau \rangle.$$

Proof. The permutation with puts λ in the proper order in $[\lambda] \cup [\sigma \cup \tau]$ is just a composition of the permutation which puts λ in the proper order in $[\lambda] \cup [\sigma]$ with the permutation which puts λ in the proper order in $[\lambda] \cup [\tau]$. $\square$

Proposition 66.11. *Let σ and τ be two disjoint subsets of $\{1, \dots, n\}$. If $\lambda \in \sigma$, then*

$$\langle \sigma, \tau \rangle = \langle \sigma \backslash \lambda, \tau \rangle \langle \lambda, \tau \rangle.$$

Similarly, if $\mu \in \tau$, then

$$\langle \sigma, \tau \rangle = \langle \sigma, \mu \rangle \langle \sigma, \tau \backslash \mu \rangle. \tag{285}$$

Proof. Suppose $\lambda \in \sigma$. We can place $[\sigma] \cup [\tau]$ into proper order by moving λ all the way to the left of $[\sigma]$, then place $[\sigma \backslash \lambda] \cup [\tau]$ into proper order, then place $[\lambda] \cup [\sigma \backslash \lambda \cup \tau]$ into proper order. This gives us

$$\begin{aligned}
\langle \sigma, \tau \rangle &= \langle \lambda, \sigma \backslash \lambda \rangle \langle \sigma \backslash \lambda, \tau \rangle \langle \lambda, (\sigma \backslash \lambda) \cup \tau \rangle \rangle \\
&= \langle \lambda, \sigma \backslash \lambda \rangle \langle \sigma \backslash \lambda, \tau \rangle \langle \lambda, \sigma \backslash \lambda \rangle \langle \lambda, \tau \rangle \\
&= \langle \sigma \backslash \lambda, \tau \rangle \langle \lambda, \tau \rangle
\end{aligned}$$

An analagous argument gives (285). $\square$

66.3.2 Definition of the Koszul Complex

We are now ready to define the Koszul complex of $\underline{x}$.

Definition 66.5. The **Koszul complex** of $\underline{x}$, denoted $(\mathcal{K}(\underline{x}), \mathrm{d}^{\mathcal{K}(\underline{x})})$ (or more simply by $\mathcal{K}(\underline{x})$), is the R-complex whose underlying graded R-module $\mathcal{K}(x)$ has as its homogeneous component in degree i given by

$$\mathcal{K}_i(\underline{x}) := \begin{cases} \bigoplus_{\sigma \in S_i[n]} Re_\sigma & \text{if } 0 \leq i \leq n \\ 0 & \text{if } i > n \text{ or if } i < 0. \end{cases}$$

and whose differential $\mathrm{d}^{\mathcal{K}(\underline{x})}$ is uniquely determined by

$$\mathrm{d}^{\mathcal{K}(\underline{x})}(e_\sigma) = \sum_{\lambda \in \sigma} \langle \lambda, \sigma \backslash \lambda \rangle x_\lambda e_{\sigma \backslash \lambda}$$

for all nonempty $\sigma \subseteq \{1, \ldots, n\}$.

More generally, suppose M is an R-module. The **Koszul complex** of $\underline{x}$ with **coefficients** in M, denoted $(\mathcal{K}(\underline{x}, M), \mathrm{d}^{\mathcal{K}(\underline{x}, M)})$ (or more simply by $\mathcal{K}(\underline{x}, M)$), is the R-complex $\mathcal{K}(\underline{x}) \otimes_R M$. The homology of this R-complex is denoted $\mathrm{H}(\mathcal{K}(\underline{x}, M))$.

Exercise 7. Check that $(\mathcal{K}(\underline{x}), \mathrm{d}^{\mathcal{K}(\underline{x})})$ is an R-complex. In particular, show $\mathrm{d}^{\mathcal{K}(\underline{x})}\mathrm{d}^{\mathcal{K}(\underline{x})} = 0$.

Example 66.3. Here's what the Koszul complex $\mathcal{K}(x_1, x_2, x_3)$ looks like:

$$\begin{tikzcd}[column sep=huge]
R \arrow[r, "\begin{pmatrix} x_1 \\ -x_2 \\ x_3 \end{pmatrix}"] & R^3 \arrow[r, "\begin{pmatrix} 0 & -x_3 & -x_2 \\ -x_3 & 0 & x_1 \\ x_2 & x_1 & 0 \end{pmatrix}"] & R^3 \arrow[r, "\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}"] & R
\end{tikzcd}$$

$$\begin{aligned}
e_{\{1,2,3\}} &\longmapsto x_1 e_{\{2,3\}} - x_2 e_{\{1,3\}} + x_3 e_{\{1,2\}} \\
e_{\{2,3\}} &\longmapsto x_2 e_{\{3\}} - x_3 e_{\{2\}} \\
e_{\{1,3\}} &\longmapsto x_1 e_{\{3\}} - x_3 e_{\{1\}} \\
e_{\{1,2\}} &\longmapsto x_1 e_{\{2\}} - x_2 e_{\{1\}} \\
e_{\{1\}} &\longmapsto x_1 \\
e_{\{2\}} &\longmapsto x_2 \\
e_{\{3\}} &\longmapsto x_3
\end{aligned}$$

66.3.3 Koszul Complex as Tensor Product

Proposition 66.12. *We have an isomorphism of R-complexes:*

$$(\mathcal{K}(x_1), \mathrm{d}^{\mathcal{K}(x_1)}) \otimes_R \cdots \otimes_R (\mathcal{K}(x_n), \mathrm{d}^{\mathcal{K}(x_n)}) \cong (\mathcal{K}(\underline{x}), \mathrm{d}^{\mathcal{K}(\underline{x})}).$$

Remark 119. Note that Proposition (63.23) gives an unambiguous interpretation for $(\mathcal{K}(x_1), \mathrm{d}^{\mathcal{K}(x_1)}) \otimes_R \cdots \otimes_R (\mathcal{K}(x_n), \mathrm{d}^{\mathcal{K}(x_n)})$.

Proof. For each $1 \leq \lambda \leq n$, write $\mathcal{K}(x_\lambda) = R \oplus Re_\lambda$ (so $\{1\}$ is a basis for $\mathcal{K}(x_\lambda)_0$ and $\{e_\lambda\}$ is a basis for $\mathcal{K}(x_\lambda)_1$). Let

$$\varphi \colon \mathcal{K}(x_1) \otimes_R \cdots \otimes_R \mathcal{K}(x_n) \to \mathcal{K}(\underline{x})$$

be the unique graded linear map [11] such that

$$\varphi(1 \otimes \cdots \otimes 1) = 1 \quad \text{and} \quad \varphi(1 \otimes \cdots \otimes e_{\lambda_1} \otimes \cdots \otimes e_{\lambda_i} \cdots \otimes 1) = e_{\{\lambda_1, \ldots, \lambda_i\}}$$

for all $1 \leq \lambda_1 < \cdots < \lambda_i \leq n$. Then φ is an isomorphism since it restricts to a bijection on basis sets.

For the rest of the proof, denote $\mathrm{d}^{\mathcal{K}} := \mathrm{d}^{\mathcal{K}(\underline{x})}$ and $\mathrm{d}^{\otimes} := \mathrm{d}^{\mathcal{K}(x_1) \otimes_R \cdots \otimes_R \mathcal{K}(x_n)}$. To see that φ is an isomorphism of R-complexes, we need to show that

$$\varphi \mathrm{d}^{\otimes} = \mathrm{d}^{\mathcal{K}} \varphi. \tag{286}$$

It suffices to check (**??**) on the basis elements. We have

$$\begin{aligned}
\mathrm{d}^{\mathcal{K}} \varphi(1 \otimes \cdots \otimes 1) &= \mathrm{d}^{\mathcal{K}}(1) \\
&= 0 \\
&= \varphi(0) \\
&= \varphi \mathrm{d}^{\otimes}(1 \otimes \cdots \otimes 1),
\end{aligned}$$

[11] We say unique graded linear map here because $\mathcal{K}(x_1) \otimes_R \cdots \otimes_R \mathcal{K}(x_n)$ is free with basis elements of the form $1 \otimes \cdots \otimes 1$ and $1 \otimes \cdots \otimes e_{\lambda_1} \otimes \cdots \otimes e_{\lambda_i} \cdots \otimes 1$ for $1 \leq \lambda_1 < \cdots < \lambda_i \leq n$ and φ respects the grading.

and

$$
\begin{aligned}
\mathrm{d}^{\mathcal{K}}\varphi(1\otimes\cdots\otimes e_{\lambda_1}\otimes\cdots\otimes e_{\lambda_i}\cdots\otimes 1) &= \mathrm{d}^{\mathcal{K}}(e_{\{\lambda_1,\dots,\lambda_i\}}) \\
&= \sum_{\mu=1}^{i}(-1)^{\mu-1}x_{\lambda_\mu}e_{\{\lambda_1,\dots,\lambda_i\}} \\
&= \sum_{\mu=1}^{i}(-1)^{\mu-1}x_{\lambda_\mu}\varphi(1\otimes\cdots\otimes e_{\lambda_1}\otimes\cdots\otimes\widehat{e}_{\lambda_\mu}\otimes\cdots\otimes e_{\lambda_i}\otimes\cdots\otimes 1) \\
&= \varphi\sum_{\mu=1}^{i}(-1)^{\mu-1}x_{\lambda_\mu}1\otimes\cdots\otimes e_{\lambda_1}\otimes\cdots\otimes\widehat{e}_{\lambda_\mu}\otimes\cdots\otimes e_{\lambda_i}\otimes\cdots\otimes 1) \\
&= \varphi\mathrm{d}^{\otimes}(1\otimes\cdots\otimes e_{\lambda_1}\otimes\cdots\otimes e_{\lambda_i}\cdots\otimes 1).
\end{aligned}
$$

for all $1\leq\lambda_1<\cdots<\lambda_i\leq n$. □

66.3.4 Koszul Complex is a DG Algebra

Proposition 66.13. *Let $\underline{x}=x_1,\dots,x_n$ be a sequence of elements in R. The Koszul complex $(\mathcal{K}(\underline{x}),\mathrm{d}^{\mathcal{K}(\underline{x})})$ is a DG algebra, with multiplication being uniquely determined on elementary tensors: for $\sigma,\tau\subseteq[n]$, we map $e_\sigma\otimes e_\tau\mapsto e_\sigma e_\tau$, where*

$$
e_\sigma e_\tau=\begin{cases}\langle\sigma,\tau\rangle e_{\sigma\cup\tau} & \text{if } \sigma\cap\tau=\varnothing\\ 0 & \text{if } \sigma\cap\tau\neq\varnothing\end{cases} \tag{287}
$$

Proof. Throughout this proof, denote $\mathrm{d}:=\mathrm{d}^{\mathcal{K}(\underline{x})}$. We first want to show that $\mathcal{K}(\underline{x})$ is an associative, unital, and strictly graded-commutative R-algebra. Since $\mathcal{K}(\underline{x})$ is a free R-module with $\{e_\sigma\mid\sigma\subseteq[n]\}$ as a basis, it suffices to check associativity and graded-commutativitythese properties on the basis elements. We first note that $e_\varnothing$ serves as the identity for the multiplication rule (**??**). Indeed, let $\sigma\subseteq[n]$. Then since $\sigma\cap\varnothing=\varnothing$, we have

$$
e_\sigma e_\varnothing=e_\sigma=e_\varnothing e_\sigma.
$$

Thus the underlying R-algebra $\mathcal{K}(\underline{x})$ is unital.

Next we check the underlying R-algebra $\mathcal{K}(\underline{x})$ is associative. Let $\sigma,\tau,\kappa\subseteq[n]$. If $\sigma\cap\tau\cap\kappa\neq\varnothing$, then it is clear that

$$
\begin{aligned}
e_\sigma(e_\tau e_\kappa) &= 0 \\
&= (e_\sigma e_\tau)e_\kappa,
\end{aligned}
$$

so assume $\sigma\cap\tau\cap\kappa=\varnothing$. Then

$$
\begin{aligned}
e_\sigma(e_\tau e_\kappa) &= \langle\tau,\kappa\rangle e_\sigma e_{\tau\cup\kappa} \\
&= \langle\sigma,\tau\cup\kappa\rangle\langle\tau,\kappa\rangle e_{\sigma\cup\tau\cup\kappa} \\
&= \langle\sigma,\tau\rangle\langle\sigma,\kappa\rangle\langle\tau,\kappa\rangle e_{\sigma\cup\tau\cup\kappa} \\
&= \langle\sigma,\tau\rangle\langle\sigma\cup\tau,\kappa\rangle e_{\sigma\cup\tau\cup\kappa} \\
&= \langle\sigma,\tau\rangle e_{\sigma\cup\tau}e_\kappa \\
&= (e_\sigma e_\tau)e_\kappa.
\end{aligned}
$$

Next we check the underlying R-algebra $\mathcal{K}(\underline{x})$ is graded-commutative. Let $\sigma,\tau\subseteq[n]$. If $\sigma\cap\tau\neq\varnothing$, then

$$
\begin{aligned}
e_\sigma e_\tau &= 0 \\
&= (-1)^{|\sigma||\tau|}e_\tau e_\sigma.
\end{aligned}
$$

Suppose $\sigma\cap\tau=\varnothing$. Then

$$
\begin{aligned}
e_\sigma e_\tau &= \langle\sigma,\tau\rangle e_{\sigma\cup\tau} \\
&= (-1)^{|\sigma||\tau|}\langle\tau,\sigma\rangle e_{\sigma\cup\tau} \\
&= (-1)^{|\sigma||\tau|}e_\tau e_\sigma.
\end{aligned}
$$

Next we check the underlying R-algebra $\mathcal{K}(\underline{x})$ is strictly graded-commutative. Let $\sigma\subseteq[n]$ such that $|\sigma|$ is odd. Then

$$
\begin{aligned}
e_\sigma^2 &= e_\sigma e_\sigma \\
&= 0
\end{aligned}
$$

since $\sigma \cap \sigma \neq \emptyset$.

Finally, we need to check Leibniz law. First note that multiplication by $e_\emptyset$ and e_σ satisfies Leibniz law:

$$\begin{aligned}
\mathrm{d}(e_\sigma)e_\emptyset - e_\sigma d(e_\emptyset) &= \mathrm{d}(e_\sigma)e_\emptyset \\
&= \mathrm{d}(e_\sigma) \\
&= \mathrm{d}(e_\sigma e_\emptyset),
\end{aligned}$$

and similarly

$$\begin{aligned}
\mathrm{d}(e_\emptyset)e_\sigma + e_\emptyset \mathrm{d}(e_\sigma) &= e_\emptyset \mathrm{d}(e_\sigma) \\
&= \mathrm{d}(e_\sigma) \\
&= \mathrm{d}(e_\emptyset e_\sigma),
\end{aligned}$$

Next, let $\lambda \in [n]$ and let $\tau \subseteq [n]$. If $\lambda \in \tau$, then the pair (e_λ, e_τ) satisfies Leibniz law trivially, so suppose that $\lambda \notin \tau$. Then

$$\begin{aligned}
\mathrm{d}(e_\lambda)e_\tau - e_\lambda \mathrm{d}(e_\tau) &= x_\lambda e_\tau - e_\lambda \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle x_\mu e_{\tau \backslash \mu} \\
&= x_\lambda e_\tau - \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle \langle \lambda, \tau \backslash \mu \rangle x_\mu e_{\tau \backslash \mu \cup \lambda} \\
&= x_\lambda e_\tau - \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle \langle \lambda, \tau \rangle \langle \lambda, \mu \rangle x_\mu e_{\tau \backslash \mu \cup \lambda} \\
&= x_\lambda e_\tau + \sum_{\mu \in \tau} \langle \lambda, \tau \rangle \langle \mu, \tau \backslash \mu \rangle \langle \mu, \lambda \rangle x_\mu e_{\tau \backslash \mu \cup \lambda} \\
&= x_\lambda e_\tau + \sum_{\mu \in \tau} \langle \lambda, \tau \rangle \langle \mu, \tau \backslash \mu \cup \lambda \rangle x_\mu e_{\tau \backslash \mu \cup \lambda} \\
&= \langle \lambda, \tau \rangle \langle \lambda, \tau \rangle x_\lambda e_\tau + \sum_{\mu \in \tau} \langle \lambda, \tau \rangle \langle \mu, \tau \backslash \mu \cup \lambda \rangle x_\mu e_{\tau \backslash \mu \cup \lambda} \\
&= \langle \lambda, \tau \rangle \sum_{\mu \in \tau \cup \lambda} \langle \mu, (\tau \cup \lambda) \backslash \mu \rangle x_\mu e_{(\tau \cup \lambda) \backslash \mu} \\
&= \langle \lambda, \tau \rangle \mathrm{d}(e_{\tau \cup \lambda}) \\
&= \mathrm{d}(e_\lambda e_\tau),
\end{aligned}$$

where we used Proposition (66.11) to get from the second line to the third line. Next suppose $\tau \subseteq [n]$ and $\lambda \in \tau$. Then

$$\begin{aligned}
\mathrm{d}(e_\lambda)e_\tau - e_\lambda d(e_\tau) &= x_\lambda e_\tau - e_\lambda \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle x_\mu e_{\tau \backslash \mu} \\
&= x_\lambda e_\tau - \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle x_\mu e_\lambda e_{\tau \backslash \mu} \\
&= x_\lambda e_\tau - \langle \lambda, \tau \backslash \lambda \rangle \langle \lambda, \tau \backslash \lambda \rangle x_\lambda e_\tau \\
&= x_\lambda e_\tau - x_\lambda e_\tau \\
&= 0 \\
&= \mathrm{d}(0) \\
&= \mathrm{d}(e_\lambda e_\tau).
\end{aligned}$$

Thus we have shown (**??**) satisfies the Leibniz law for all pairs (λ, τ) where $\lambda \in [n]$ and $\tau \subseteq [n]$. We prove by induction on $|\sigma| = i \geq 1$ that (**??**) satisfies the Leibniz law for all pairs (σ, τ) where $\sigma, \tau \subseteq [n]$. The base case $i = 1$ was just shown. Now suppose we have shown (**??**) satisfies the Leibniz law for all pairs (σ, τ) where $\sigma, \tau \subseteq [n]$ such that $|\sigma| = i < n$. Let $\sigma, \tau \subseteq [n]$ such that $|\sigma| = i + 1$. Choose $\lambda \in \sigma$. Then

$$\begin{aligned}
\mathrm{d}(e_\sigma e_\tau) &= \mathrm{d}(e_\lambda e_{\sigma \backslash \lambda} e_\tau) \\
&= x_\lambda e_{\sigma \backslash \lambda} e_\tau - e_\lambda \mathrm{d}(e_{\sigma \backslash \lambda} e_\tau) \\
&= x_\lambda e_{\sigma \backslash \lambda} e_\tau - e_\lambda (\mathrm{d}(e_{\sigma \backslash \lambda}) e_\tau + (-1)^{|\sigma|-1} e_{\sigma \backslash \lambda} \mathrm{d}(e_\tau)) \\
&= (x_\lambda e_{\sigma \backslash \lambda} - e_\lambda \mathrm{d}(e_{\sigma \backslash \lambda})) e_\tau + (-1)^{|\sigma|} e_\sigma \mathrm{d}(e_\tau) \\
&= \mathrm{d}(e_\lambda e_{\sigma \backslash \lambda}) e_\tau + (-1)^{|\sigma|} e_\sigma \mathrm{d}(e_\tau) \\
&= \mathrm{d}(e_\sigma) e_\tau + (-1)^{|\sigma|+1} e_\sigma \mathrm{d}(e_\tau),
\end{aligned}$$

where we used the base case on the pairs $(e_\lambda, e_{\sigma \backslash \lambda} e_\tau)$[12] and $(e_\lambda, e_{\sigma \backslash \lambda})$ and where we used the induction hypothesis on the pair $(e_{\sigma \backslash \lambda}, e_\tau)$. and where we used the base case on the pair $(e_\lambda, e_{\sigma \backslash \lambda})$. □

[12] If $e_{\sigma \backslash \lambda} e_\tau = 0$, then obviously Leibniz law holds for the pair $(e_\lambda, e_{\sigma \backslash \lambda} e_\tau)$.

66.3.5 The Dual Koszul Complex

We now want to discuss the dual Koszul complex of $\underline{x}$.

Definition 66.6. The **dual Koszul complex of** $\underline{x}$ is the R-complex

$$\mathrm{Hom}_R^\star(\mathcal{K}(\underline{x}), R),$$

where R is viewed as a trivial R-complex (trivially grading with $\mathrm{d} = 0$). We denote by $\mathcal{K}^\star(\underline{x})$ to be the graded R-module hom $\mathrm{Hom}_R^\star(\mathcal{K}(\underline{x}), R)$. We also denote by $\mathrm{d}^{\mathcal{K}^\star(\underline{x})}$ to be the corresponding differential. We can describe the dual Koszul complex more explicitly as follows: the graded R-module $\mathcal{K}^\star(\underline{x})$ has

$$\mathcal{K}_i^\star(\underline{x}) := \begin{cases} \bigoplus_{\sigma \in S_{-i}[n]} Re_\sigma^\star & \text{if } -n \leq i \leq 0 \\ 0 & \text{if } i < n \text{ or if } i > 0. \end{cases}$$

as its ith homogeneous component, where $e_\sigma^\star \colon \mathcal{K}(\underline{x}) \to R$ is uniquely determined by

$$e_\sigma^\star(e_{\sigma'}) = \begin{cases} 1 & \sigma = \sigma' \\ 0 & \text{else.} \end{cases}$$

for all $\sigma, \sigma' \subseteq [n]$. The differential $\mathrm{d}^{\mathcal{K}^\star(\underline{x})}$ is uniquely determined by

$$\mathrm{d}^{\mathcal{K}^\star(\underline{x})}(e_\sigma^\star) = (-1)^{|\sigma|+1} \sum_{\lambda^\star \in \sigma^\star} \langle \lambda^\star, \sigma \rangle r_\lambda e_{\sigma \cup \lambda^\star}^\star$$

for all $\sigma \subseteq [n]$.

Duality

Theorem 66.1. *There exists an isomorphism of R-complexes*

$$S^n \mathrm{Hom}_R^\star(\mathcal{K}(\underline{x}), R) \cong \mathcal{K}(\underline{x}).$$

In particular, we have an isomorphism of R-modules

$$\mathrm{H}_i(\mathcal{K}(\underline{x})) \cong \mathrm{H}_{i-n}(\mathcal{K}^\star(\underline{x}))$$

for all $i \in \mathbb{Z}$.

Proof. Let $i \in \mathbb{Z}$. If $i > n$ or $i < 0$, then theorem is obvious, so we may assume that $0 \leq i \leq n$. Let $\varphi \colon S^n(\mathcal{K}^\star(\underline{r}), d^{\mathcal{K}^\star(\underline{r})}) \to (\mathcal{K}(\underline{r}), d^{\mathcal{K}(\underline{r})})$ be the unique R-module graded homomorphism such that

$$\varphi(e_\sigma^\star) = \langle \sigma^\star, \sigma \rangle e_{\sigma^\star}.$$

for all $1 \leq \lambda_1 < \cdots < \lambda_i \leq n$. Then φ is an isomorphism of graded R-modules since it restricts to a bijection of basis sets. To see that φ is an isomorphism of R-complexes, we need to show that it commutes with the differentials. To do this, we first simplify notation by denoting $d^\star := (d^{\mathcal{K}^\star(\underline{r})})^{\Sigma^n}$ and $d := d^{\mathcal{K}(\underline{r})}$. Now we have

$$\begin{aligned}
d\varphi(e^\star_\sigma) &= d(\langle \sigma^\star, \sigma\rangle e_{\sigma^\star}) \\
&= \langle \sigma^\star, \sigma\rangle d(e_{\sigma^\star}) \\
&= \sum_{\lambda^\star \in \sigma^\star} \langle \sigma^\star, \sigma\rangle \langle \lambda^\star, \sigma^\star \backslash \lambda^\star\rangle r_{\lambda^\star} e_{\sigma^\star \backslash \lambda^\star} \\
&= \sum_{\lambda^\star \in \sigma^\star} \langle \lambda^\star, \sigma^\star \backslash \lambda^\star\rangle \langle \sigma^\star, \sigma\rangle r_{\lambda^\star} e_{\sigma^\star \backslash \lambda^\star} \\
&= \sum_{\lambda^\star \in \sigma^\star} \langle \lambda^\star, \sigma^\star \backslash \lambda^\star\rangle \langle \sigma^\star \backslash \lambda^\star, \sigma\rangle \langle \lambda^\star, \sigma\rangle r_{\lambda^\star} e_{\sigma^\star \backslash \lambda^\star} \\
&= \sum_{\lambda^\star \in \sigma^\star} \langle \sigma^\star \backslash \lambda^\star, \sigma \cup \lambda^\star\rangle \langle \lambda^\star, \sigma\rangle r_{\lambda^\star} e_{\sigma^\star \backslash \lambda^\star} \\
&= \sum_{\lambda^\star \in \sigma^\star} \langle \lambda^\star, \sigma\rangle \langle \sigma^\star \backslash \lambda^\star, \sigma \cup \lambda^\star\rangle r_{\lambda^\star} e_{\sigma^\star \backslash \lambda^\star} \\
&= \sum_{\lambda^\star \in \sigma^\star} \langle \lambda^\star, \sigma\rangle \langle (\sigma \cup \lambda^\star)^\star, \sigma \cup \lambda^\star\rangle r_{\lambda^\star} e_{(\sigma \cup \lambda^\star)^\star} \\
&= \sum_{\lambda^\star \in \sigma^\star} \langle \lambda^\star, \sigma\rangle r_{\lambda^\star} \varphi(e^\star_{\sigma \cup \lambda^\star}) \\
&= \varphi \sum_{\lambda^\star \in \sigma^\star} \langle \lambda^\star, \sigma\rangle r_{\lambda^\star} e^\star_{\sigma \cup \lambda^\star} \\
&= \varphi d^\star(e^\star_\sigma)
\end{aligned}$$

where we used the fact that $\sigma^\star \backslash \lambda^\star = (\sigma \cup \lambda^\star)^\star$ and $\langle \sigma^\star, \sigma\rangle = \langle \lambda^\star, \sigma^\star \backslash \lambda^\star\rangle \langle \lambda^\star, \sigma\rangle \langle \sigma^\star \backslash \lambda^\star, \sigma \cup \lambda^\star\rangle$. □

66.3.6 Mapping Cone of Homothety Map as Tensor Product

Proposition 66.14. *Let (A, d) be an R-complex, let $x \in R$, and let $\mu_x \colon (A, \mathrm{d}) \to (A, \mathrm{d})$ be the multiplication by x homothety map. Then*

$$(\mathrm{C}(\mu_x), \mathrm{d}^{\mathrm{C}(\mu_x)}) \cong (\mathcal{K}(x), \mathrm{d}^{\mathcal{K}(x)}) \otimes_R (A, \mathrm{d}).$$

Proof. Let $\mathcal{K}(x) = R \oplus Re$ (so $\{1\}$ is a basis for $\mathcal{K}(x)_0$ and $\{e\}$ is a basis for $\mathcal{K}(x)_1$). Let $\varphi \colon \mathcal{K}(x) \otimes_R A \to \mathrm{C}(\mu_x)$ be defined by

$$\varphi(1 \otimes a + e \otimes b) = (a, b)$$

for all $i \in \mathbb{Z}$, $a \in A_i$, and $b \in A_{i-1}$. Clearly φ is an isomorphism of graded R-modules. To see that φ is an isomorphism of R-complexes, we need to check that

$$\mathrm{d}^{\mathrm{C}(\mu_x)}\varphi = \varphi \mathrm{d}^{\mathcal{K}(x) \otimes_R A} \tag{288}$$

Let $i \in \mathbb{Z}$, $a \in A_i$, and $b \in A_{i-1}$. Then

$$\begin{aligned}
\mathrm{d}^{\mathrm{C}(\mu_x)}\varphi(1 \otimes a + e \otimes b) &= \mathrm{d}^{\mathrm{C}(\mu_x)}(a, b) \\
&= (\mathrm{d}(a) + xb, -\mathrm{d}(b)) \\
&= \varphi(1 \otimes (\mathrm{d}(a) + xb) + e \otimes (-\mathrm{d}(b))) \\
&= \varphi(1 \otimes \mathrm{d}(a) + x \otimes b - e \otimes \mathrm{d}(b)) \\
&= \varphi(\mathrm{d}^{\mathcal{K}(x) \otimes_R A}(1 \otimes a) + \mathrm{d}^{\mathcal{K}(x) \otimes_R A}(e \otimes b)) \\
&= \varphi \mathrm{d}^{\mathcal{K}(x) \otimes_R A}(1 \otimes a + e \otimes b).
\end{aligned}$$

□

66.3.7 Properties of the Koszul Complex

Proposition 66.15. *Let $\lambda \in [n]$. Then the homothety map*

$$\mu_{x_\lambda} \colon (\mathcal{K}(\underline{x}), \mathrm{d}^{\mathcal{K}(\underline{x})}) \to (\mathcal{K}(\underline{x}), \mathrm{d}^{\mathcal{K}(\underline{x})})$$

is null-homotopic. In particular, $x_\lambda \mathrm{H}(\mathcal{K}(\underline{x})) \cong 0$.

Proof. Denote $\mathrm{d} := \mathrm{d}^{\mathcal{K}(\underline{x})}$ and let $h \colon \mathcal{K}(\underline{x}) \to \mathcal{K}(\underline{x})$ be the unique graded homomorphism of degree 1 such that

$$h(e_\sigma) = e_\lambda e_\sigma$$

for all $\sigma \subseteq [n]$. Then

$$\begin{aligned}(h\mathrm{d} + h\mathrm{d})(e_\sigma) &= \mathrm{d}(e_\lambda e_\sigma) + e_\lambda \mathrm{d}(e_\sigma) \\ &= x_\lambda e_\sigma - e_\lambda \mathrm{d}(e_\sigma) + e_\lambda \mathrm{d}(e_\sigma) \\ &= x_\lambda e_\sigma\end{aligned}$$

for all $\sigma \subseteq [n]$. It follows that

$$\mathrm{d}h + h\mathrm{d} = \mu_{x_\lambda}$$

on all of $\mathcal{K}(\underline{x})$. Thus the homothety map μ_{x_λ} is null-homotopic. □

Proposition 66.16. *The following conditions are equivalent.*

1. $\langle \underline{x} \rangle = R$,
2. $\mathrm{H}(\mathcal{K}(\underline{x})) \cong 0$,
3. $\mathrm{H}_0(\mathcal{K}(\underline{x})) \cong 0$.

This follows immediately from Proposition (66.15) and the fact that $\mathrm{H}_0(\mathcal{K}(\underline{x})) \cong R/\langle \underline{x} \rangle$, but we will give an alternative proof:

Proof. Throughout this proof, we denote $\mathrm{d} := \mathrm{d}^{\mathcal{K}(\underline{x})}$.

($1 \implies 2$) Since $\langle \underline{x} \rangle = R$, there exists $y_1, \dots, y_n \in R$ such that

$$\sum_{\lambda=1}^{n} x_\lambda y_\lambda = 1.$$

Choose such $y_1, \dots, y_n \in R$ and let $\overline{f} \in \mathrm{H}(\mathcal{K}(\underline{x}))$ (so $f \in \ker \mathrm{d}$ is a representative of the coset $\overline{f}$). Then

$$\begin{aligned}\mathrm{d}\left(\sum_{\lambda=1}^{n} y_\lambda e_\lambda f\right) &= \sum_{\lambda=1}^{n} y_\lambda \mathrm{d}(e_\lambda f) \\ &= \sum_{\lambda=1}^{n} y_\lambda (\mathrm{d}(e_\lambda) f - e_\lambda \mathrm{d}(f)) \\ &= \sum_{\lambda=1}^{n} y_\lambda x_\lambda f \\ &= \left(\sum_{\lambda=1}^{n} y_\lambda x_\lambda\right) f \\ &= f.\end{aligned}$$

Thus, $f \in \operatorname{im} \mathrm{d}$, which implies $\mathrm{H}(\mathcal{K}(\underline{x})) = 0$.

($2 \implies 3$) $\mathrm{H}(\mathcal{K}(\underline{x})) \cong 0$ if and only if $\mathrm{H}_i(\mathcal{K}(\underline{x})) \cong 0$ for all $i \in \mathbb{Z}$. In particular, $\mathrm{H}(\mathcal{K}(\underline{x})) \cong 0$ implies $\mathrm{H}_0(\mathcal{K}(\underline{x})) \cong 0$.

($3 \implies 1$) We have

$$\begin{aligned}0 &\cong \mathrm{H}(\mathcal{K}(\underline{x})) \\ &= R/\langle \underline{x} \rangle,\end{aligned}$$

which implies $\langle \underline{x} \rangle = R$. □

Proposition 66.17. *Let $x \in R$ and let A be an R-complex. For every $i \geq 0$, we have a short exact sequence*

$$0 \to \mathrm{H}_0(x, \mathrm{H}_i(A)) \to \mathrm{H}_i(\mathcal{K}(x) \otimes_R A) \to \mathrm{H}_1(x, \mathrm{H}_{i-1}(A)) \to 0.$$

67 Advanced Homological Algebra

Definition 67.1. Let

$$0 \longrightarrow A \xrightarrow{\varphi} A' \xrightarrow{\varphi'} A'' \longrightarrow 0 \tag{289}$$

be an exact sequence of R-complexes and chain maps. We say (289) is **degree-wise exact** if it is exact when viewed as a sequence of graded R-modules, that is, if for each $i \in \mathbb{Z}$ the sequence

$$0 \longrightarrow A_i \xrightarrow{\varphi_i} A'_i \xrightarrow{\varphi'_i} A''_i \longrightarrow 0 \tag{290}$$

is exact. Similarly, we say (289) is **degree-wise split exact** if (289) is split exact for each $i \in \mathbb{Z}$.

Proposition 67.1. *Let*

be an exact sequence of R-complexes and chain maps. Assume that for all $p \in \mathbb{Z}$ the sequence $\xi_p = (0 \to A_p \xrightarrow{\alpha_p} B_p \xrightarrow{\beta_p} C_p \to 0)$ is split exact. Then for all R-complexes X, Y the sequences $\xi_* = \mathrm{Hom}_R(X, \xi)$ and $\xi^* = \mathrm{Hom}_R(\xi, Y)$ are short exact.

Proof. Focus on ξ^*. First note that $0 \to C^* \xrightarrow{\beta^*} B \xrightarrow{\alpha^*} A^*$ is exact by left exactness. Need to show α^* is surjective. Note that ξ_p split implies $\gamma_p \colon B_p \to A_p$ such that $\gamma_p \alpha_p = 1_{A_p}$. We have

$$\begin{aligned}
\mathrm{Hom}_R(\alpha_p, Y_{p+n}) &= \mathrm{Hom}_R(\gamma_p, Y_{p+n}) \\
&= \mathrm{Hom}_R(\gamma_p \alpha_p, Y_{p+n}) \\
&= \mathrm{Hom}_R(1_{A_p}, Y_{p+n}) \\
&= 1_{\mathrm{Hom}_R(A_p, Y_{p+n})}.
\end{aligned}$$

□

Remark 120. There is a notion of split exactness for sequences of R-complexes and chain maps. Essentially the splitting map has to commute with the differentials.

Definition 67.2. Exact sequence ξ as above is called **degree-wise split exact**

67.1 Resolutions

Definition 67.3. Let M be an R-complex.

1. A **projective resolution of** M is a bounded below R-complex of projective R-modules P equipped with a quasiisomorphism $\tau \colon P \xrightarrow{\simeq} M$. In this case, we say (P, τ) (or just P if context is clear) is a projective resolution of M.

2. An **injective resolution of** M is a bounded above R-complex of injective R-modules E equipped with a quasiisomorphism $\varepsilon \colon M \xrightarrow{\simeq} E$. In this case, we say (E, ε) (or just E if context is clear) is an injective resolution of M.

67.1.1 Existence of projective resolutions

Proposition 67.2. *Let M, N, and P be R-modules, let $\psi\colon N \to M$ be an R-linear map, and let $\varphi\colon P \twoheadrightarrow M$ be an R-linear map. Define the **pullback of** $\psi\colon N \to M$ **and** $\varphi\colon P \twoheadrightarrow M$ to be the R-module*

$$N \times_M P := \{(v,w) \in N \times P \mid \psi v = \varphi w\}$$

equipped with the R-linear maps $\pi_1\colon N \times_M P \to N$ and $\pi_2\colon N \times_M P \to P$ given by

$$\pi_1(v,w) = v \quad \text{and} \quad \pi_2(v,w) = w$$

for all $(v,w) \in N \times_M P$. Then the following diagram commutes

$$\begin{tikzcd}
0 \arrow[r] & \ker \pi_2 \arrow[r] \arrow[d, "\pi_1|_{\ker \pi_2}"] & N \times_M P \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & P \arrow[r] \arrow[d, "\varphi"] & P/(N \times_M P) \arrow[r] \arrow[d, "\overline{\varphi}"] & 0 \\
0 \arrow[r] & \ker \psi \arrow[r] & N \arrow[r, "\psi"] & M \arrow[r] & M/N \arrow[r] & 0
\end{tikzcd}$$

where $\overline{\varphi}\colon P/(N \times_M P) \to M/N$ given by

$$\overline{\varphi}(\overline{w}) = \overline{\varphi(w)}$$

for all $\overline{w} \in P/(N \times_M P)$ and where $\varphi|_{\ker \pi_2}$ is the restriction of φ to $\ker \pi_2$. Moreover,

1. *$\pi_1|_{\ker \pi_2}$ is an isomorphism and $\overline{\varphi}$ is injective.*
2. *if φ is injective, then π_1 is injective.*
3. *if φ is surjective, then π_1 is surjective and $\overline{\varphi}$ is an isomorphism.*

Proof. We first need to check that $\overline{\varphi}$ is well-defined. Suppose $v + v'$ is another representative of $\overline{v}$ where $v' \in \operatorname{im} \pi_2$. Choose $[u', v'] \in N \times_M P$ such that $\pi_2[u', v'] = v'$ (so $\varphi(v') = \psi(u')$). Then

$$\begin{aligned}
\overline{\varphi}(\overline{v + v'}) &= \overline{\varphi(v + v')} \\
&= \overline{\varphi(v) + \varphi(v')} \\
&= \overline{\varphi(v) + \psi(u')} \\
&= \overline{\varphi(v)}.
\end{aligned}$$

Thus $\overline{\varphi}$ is well-defined. Similarly, note that $\pi_1|_{\ker \pi_2}$ lands in $\ker \psi$. Indeed, let $(v,w) \in \ker \pi_2$. Thus $(v,w) \in N \times_M P$, meaning $\psi v = \varphi w$, and we have $\pi_2(v,w) = w = 0$. But then $\psi v = 0$ implies $v \in \ker \psi$. We now finish the remaining part of the problem:

1. First we show $\pi_1|_{\ker \pi_2}$ is surjective. Let $v \in \ker \psi$, thus $\psi v = 0$. Then $(v, 0) \in \ker \pi_2$ and $\pi_1(v,0) = v$. It follows that $\pi_1|_{\ker \pi_2}$ is surjective. Next we show $\pi_1|_{\ker \pi_2}$ is injective. Suppose $(v,0) \in \ker \pi_2$ such that $\pi_1(v,0) = v = 0$. Then clearly $(v,0) = 0$, thus $\pi_1|_{\ker \pi_2}$ is injective, hence an isomorphism. Next we show $\overline{\varphi}$ is injective. Let $\overline{w} \in P/(N \times_M P)$ such that $\overline{\varphi}\overline{w} = 0$ in M/N. Then there exists $v \in N$ such that $\psi v = \varphi w$. However this implies $w = \pi_2(v,w)$ which implies $\overline{w} = 0$ in $P/(N \times_M P)$. Hence $\overline{\varphi}$ is injective.

2. Now suppose that φ is injective. First we show π_1 is injective. Let $(v,w) \in N \times_M P$ (so $\psi v = \varphi w$) such that $\pi_1(v,w) = v = 0$. Then $\varphi w = \psi v = 0$ implies $w = 0$ since φ is injective. It follows that $(v,w) = 0$, hence π_1 is injective. Next we show $\overline{\varphi}$ is is surjective (hence an isomorphism).

3. 2. Now suppose that φ is surjective. First we show π_1 is surjective. Let $v \in N$. Since φ is surjective, there exists $w \in P$ such that $\psi v = \varphi w$. In particular, $(v,w) \in N \times_M P$ and $\pi_1(v,w) = v$. It follows that φ is surjective. Clearly $\overline{\varphi}$ is surjective since φ is surjective, hence it is an isomorphism.

$\square$

Proof. We first need to check that $\overline{\varphi}$ is well-defined. Suppose $v + v'$ is another representative of $\overline{v}$ where $v' \in \operatorname{im} \pi_2$. Choose $[u', v'] \in N \times_M P$ such that $\pi_2[u', v'] = v'$ (so $\varphi(v') = \psi(u')$). Then

$$\begin{aligned}
\overline{\varphi}(\overline{v + v'}) &= \overline{\varphi(v + v')} \\
&= \overline{\varphi(v) + \varphi(v')} \\
&= \overline{\varphi(v) + \psi(u')} \\
&= \overline{\varphi(v)}.
\end{aligned}$$

Thus $\overline{\varphi}$ is well-defined. Clearly, $\overline{\varphi}$ is a surjective R-linear map since φ is a surjective R-linear map. It remains to show that $\overline{\varphi}$ is injective. Suppose $\overline{v} \in \ker \overline{\varphi}$. Then $\varphi(v) \in \operatorname{im} \psi$. Choose $u \in N$ such that $\psi(u) = \varphi(v)$. Then $[u, v] \in N \times_M P$ and $v = \pi_2[u, v]$. It follows that $\overline{v} = 0$ in $P/\pi_2(N \times_M P)$.

Let us now check that $\pi_1|_{\ker \pi_2}$ lands in $\ker \psi$. Let $u \in \ker \pi_2$. Then

$$\begin{aligned} \psi\pi_1(u) &= \varphi\pi_2(u) \\ &= \varphi(0) \\ &= 0 \end{aligned}$$

implies $\pi_1(u) \in \ker \psi$. Thus $\pi_1|_{\ker \pi_2}$ lands in $\ker \psi$. Now we check that $\pi_1|_{\ker \pi_2}$ is an R-linear isomorphism. It is clearly an R-linear isomomorphism since it is the restriction of the homomorphism π_1. To see that $\pi_1|_{\ker \pi_2}$ is surjective, let $u \in \ker \psi$. Since

$$\begin{aligned} \psi(u) &= 0 \\ &= \varphi(0), \end{aligned}$$

we see that $[u, 0] \in N \times_M P$. Moreover we have $\pi_2[u, 0] = 0$ and so $[u, 0] \in \ker \pi_2$, and since $\pi_1[u, 0] = u$, we see that $\pi_1|_{\ker \pi_2}$ is surjetive. To see that $\pi_1|_{\ker \pi_2}$ is injective, suppose $\pi_1[u, v] = 0$ for some $[u, v] \in \ker \pi_2$. Then

$$\begin{aligned} 0 &= \pi_1[u, v] \\ &= u \end{aligned}$$

implies $u = 0$ and

$$\begin{aligned} 0 &= \pi_2[u, v] \\ &= v \end{aligned}$$

implies $v = 0$. Thus $[u, v] = [0, 0]$, hence $\pi_1|_{\ker \pi_2}$ is injective. □

Theorem 67.1. *Let (M, d) be an R-complex such that $M_i = 0$ for all $i < 0$. Then there exists a projective resolution of (M, d).*

Proof. We construct an R-complex (P, ∂) together with a chain map $\tau \colon P \to M$ which restricts to a surjection

$$\tau|_{\ker \partial} \colon \ker \partial \to \ker \mathrm{d}$$

by induction on homological degree as follows: for the base case $i = 0$, we choose a projective R-module P_0 together with a surjective R-linear map $\tau_0 \colon P_0 \to M_0$ and we set $\partial_0 \colon P_0 \to 0$ to be the zero map. Suppose for some $k > 0$, we have constructed R-linear maps $\tau_i \colon P_i \to M_i$ and $\partial_i \colon P_i \to P_{i-1}$ such that

$$\partial_{i-1} \circ \partial_i = 0 \quad \text{and} \quad \tau_{i-1} \circ \partial_i = \mathrm{d}_i \circ \tau_i$$

and such that τ_i restricts to a surjection

$$\tau_i|_{\ker \partial_i} \colon \ker \partial_i \to \ker \mathrm{d}_i$$

for all $0 < i < k$. We first construct the pullback:

$$\begin{tikzcd} P_k \arrow[dr, dashed, "\rho_k"] \arrow[drr, dashed, bend left, "\partial_k"] \arrow[ddr, dashed, bend right, "\tau_k"'] & & \\ & M_k \times_{\ker \mathrm{d}_{k-1}} \ker \partial_{k-1} \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & \ker \partial_{k-1} \arrow[d, "\tau_{k-1}|_{\ker \partial_{k-1}}"] \\ & M_k \arrow[r, "\mathrm{d}_k"] & \ker \mathrm{d}_{k-1} \end{tikzcd}$$

where the map $\tau_{k-1}|_{\ker \partial_{k-1}}$ lands in $\ker \mathrm{d}_{k-1}$ since the τ_i commute with the differentials. Now we choose a projective R-module P_k together with a surjective R-linear map

$$\rho_k \colon P_k \to M_k \times_{\ker \mathrm{d}_{k-1}} \ker \partial_{k-1}$$

and we set $\partial_k = \pi_2 \circ \rho_k$ and $\tau_k = \pi_1 \circ \rho_k$. Observe that $\operatorname{im} \partial_k \subseteq \ker \partial_{k-1}$ implies $\partial_{k-1} \circ \partial_k = 0$ and observe that

$$\begin{aligned} \tau_{k-1} \circ \partial_k &= \tau_{k-1} \circ \pi_2 \circ \rho_k \\ &= \mathrm{d}_k \circ \pi_1 \circ \rho_k \\ &= \mathrm{d}_k \circ \tau_k \end{aligned}$$

implies $\tau_{k-1} \circ \partial_k = \mathrm{d}_k \circ \tau_k$. Finally, observe that $\tau_k \colon \ker \partial_k \to \ker \mathrm{d}_k$ is surjective since it is a composition of surjective maps

$$\ker \partial_k = \ker(\pi_2 \circ \rho_k) \xrightarrow{\rho_k} \ker \pi_2 \xrightarrow[\cong]{\pi_1} \ker \mathrm{d}_k$$

where the isomorphism $\ker \pi_2 \cong \ker \mathrm{d}_k$ follows from Proposition (67.2). This completes the induction step. Therefore we have an R-complex (P, ∂) together with a chain map $\tau \colon P \to M$ which restricts to a surjection

$$\tau|_{\ker \partial} \colon \ker \partial \to \ker \mathrm{d}.$$

Moreover, Proposition (67.2) implies

$$\begin{aligned} \mathrm{H}_{k-1}(M) &= \ker \mathrm{d}_{k-1} / \operatorname{im} \mathrm{d}_k \\ &= \ker \mathrm{d}_{k-1} / \mathrm{d}_k(M_k) \\ &\cong \ker \partial_{k-1} / \operatorname{im} \pi_2 \\ &= \ker \partial_{k-1} / \operatorname{im} \partial_k \\ &= \mathrm{H}_{k-1}(P), \end{aligned}$$

It follows that τ is a quasi-isomorphism. □

Example 67.1. Let M be an $\mathbb{N}$-graded R-module. We want to calculate a semiprojective resolution of M in two ways:

1) We first compute a semiprojective resolution of M where we view it as an R-complex whose component in homologial degree i is M_i and whose differential is zero. We begin by choosing a surjection $\tau_0 \colon P_0 \twoheadrightarrow M_0$ where P_0 is a projective R-module. Next we choose a surjection $\rho_1 \colon P_1 \twoheadrightarrow M_1 \oplus K_0$ where P_1 is a projective R-module and where $K_0 = \ker \tau_0$. We define $\tau_1 = \pi_1 \circ \rho_1$ and we define $\partial_1 = \pi_2 \circ \rho_1$ where $\pi_1 \colon M_1 \oplus K_0 \twoheadrightarrow M_1$ and $\pi_2 \colon M_1 \oplus K_0 \twoheadrightarrow K_0$ are the obvious projection maps. Assuming we've constructed the semi-projection resolution up to some $k \geq 1$, we construct it at $k+1$ by choosing a surjection

$$\rho_{k+1} \colon P_{k+1} \twoheadrightarrow M_{k+1} \times_{M_k} Z_k = M_{k+1} \oplus (Z_k \cap K_k),$$

where P_{k+1} is a projective R-module, where $Z_k = \ker \partial_k$ and $K_k = \ker \tau_k$. We define $\tau_{k+1} = \pi_1 \circ \rho_{k+1}$ and we define $\partial_{k+1} = \pi_2 \circ \rho_{k+1}$ where $\pi_1 \colon M_{k+1} \oplus (Z_k \cap K_k) \twoheadrightarrow M_{k+1}$ and $\pi_2 \colon M_{k+1} \oplus (Z_k \cap K_k) \twoheadrightarrow Z_k \cap K_k$ are the obvious projection maps.

2) Next we compute a *graded* semiprojective resolution of M where we view M as a graded R-module but also as a trivial R-complex which sits in homological degree 0. To begin, we need to construct a surjection $\widetilde{\tau}_0 \colon \widetilde{P}_0 \to M$ where $\widetilde{P}_0$ is a graded projective R-module and where $\widetilde{\tau}_0$ is a graded R-module homomorphism. In fact, we've already got a candidate for this, namely $\widetilde{P}_0 = P$ and $\widetilde{\tau}_0 = \tau$. Next we choose a surjection $\widetilde{\rho}_1 \colon \widetilde{P}_1 \twoheadrightarrow \widetilde{K}$ where $\widetilde{P}_1$ is a graded projective R-module and where $\widetilde{K}_0 = \ker \widetilde{\tau}_0 = \ker \tau = K$. Note that $\Sigma^{-1}P$ is graded projective, there exists a graded homomorphism $\phi \colon \Sigma^{-1}P \to \widetilde{P}_1$ such that $\widetilde{\rho}_1 \circ \phi = \partial$.

67.1.2 Existence of injective resolutions

Lemma 67.2. *Let M, N, and E be R-modules, let $\psi\colon M \to N$ be an R-linear map, and let $\varphi\colon M \to E$ be an R-linear map. Define the pushout of $\psi\colon M \to N$ and $\varphi\colon M \to E$ to be the R-module $E +_M N$ given by*

$$E +_M N = (E \times N)/\{(\varphi v, -\psi v) \mid v \in M\}$$

equipped with the R-linear maps $\iota_1\colon E \to E +_M N$ and $\iota_2\colon N \to E +_M N$ given by

$$\iota_1(u) = [u, 0] \quad \text{and} \quad \iota_2(w) = [0, w]$$

for all $u \in E$ and $w \in N$, where $[u, w]$ denotes the coset class in $E +_M N$ with (u, w) as a representative. Then the following diagram commutes

$$\begin{tikzcd} 0 \arrow[r] & \ker\iota_1 \arrow[r] & E \arrow[r, "\iota_1"] & E +_M N \arrow[r] & (E +_M N)/E \arrow[r] & 0 \\ 0 \arrow[r] & \ker\psi \arrow[r] \arrow[u, "\varphi|_{\ker\psi}"] & M \arrow[r, "\psi"] \arrow[u, "\varphi"] & N \arrow[r] \arrow[u, "\iota_2"] & N/M \arrow[r] \arrow[u, "\overline{\iota_2}"] & 0 \end{tikzcd}$$

where $\overline{\iota_2}\colon N/M \to (E +_M N)/E$ is defined by

$$\bar{\iota}_2(\overline{w}) = \overline{[0, w]}$$

for all $\overline{w} \in N/M$ and where $\varphi|_{\ker\psi}\colon \ker\psi \to \ker\iota_1$ is defined by

$$\varphi|_{\ker\psi}(v) = \varphi(v)$$

for all $v \in \ker\psi$. Moreover,

1. *$\varphi|_{\ker\psi}$ is surjective and $\bar{\iota}_2$ is an isomorphism.*
2. *if φ is injective, then ι_2 is injective and $\varphi|_{\ker\psi}$ is an isomorphism.*
3. *if φ is surjective, then ι_2 is surjective.*

Proof. We need to check that $\bar{\iota}_2$ is well-defined. Suppose $w + \psi(v)$ is another representative of $\overline{w}$ where $v \in M$. Then

$$\begin{aligned} \bar{\iota}_2(\overline{v + \psi(w)}) &= \overline{[0, w + \psi(v)]} \\ &= \overline{[0, w] + [0, \psi(v)]} \\ &= \overline{[0, w] + [\varphi(v), 0]} \\ &= \overline{[0, w]}. \end{aligned}$$

Thus $\bar{\iota}_2$ is well-defined. Similarly, it is straightforward to check that $\varphi|_{\ker\psi}$ lands in $\ker\iota_1$. Now we finish the remaining part of the lemma:

1. First we show $\varphi|_{\ker\psi}$ is surjective. Let $v \in \ker\iota_1$. Then $[v, 0] = 0$ means there exists a $u \in M$ such that $(v, 0) = (\varphi u, -\psi u)$, or in other words, $\varphi u = v$ and $\psi u = 0$. However this implies $u \in \ker\psi$ and $\varphi|_{\ker\psi} u = v$. Thus $\varphi|_{\ker\psi}$ is surjective. To see why $\bar{\iota}_2$ is surjective, note that every element in $(E +_M N)/E$ can be represented as $\overline{[0, w]}$ for some $w \in N$. In particular, $\bar{\iota}_2$ is surjective. Next we show $\bar{\iota}_2$ is injective. Let $\overline{w} \in N/M$ such that $\overline{[0, w]} = 0$ in $(E +_M N)/E$. Then there exists a $u \in E$ such that $[u, 0] = [0, w]$ in $E +_M N$, or in other words, $[-u, w] = 0$. However this implies there exists a $v \in M$ such that $\varphi v = -u$ and $\psi v = w$. In particular, $\overline{w} = 0$ in N/M, thus $\bar{\iota}_2$ is injective, hence an isomorphism.

2. Assume φ is injective. First we show ι_2 is injective. Let $v \in N$ such that $[0, v] = 0$ in $E +_M N$. Then there exists a $u \in M$ such that $\varphi u = 0$ and $\varphi u = v$. Since φ is injective, we must have $u = 0$ which implies $\varphi u = 0 = v$. Thus ι_2 is injective. Clearly $\varphi|_{\ker\psi}$ is injective since φ is injective, hence $\varphi|_{\ker\psi}$ is an isomorphism since we already know it is surjective by (1).

3. Assume φ is surjective. First we show ι_2 is surjective. Let $[u, w] \in E +_M N$. Since φ is surjective, we have $u = \varphi v$ for some $v \in M$. However this implies

$$[u, w] = [\varphi v, w] = [0, w + \psi v].$$

Since $w + \psi v \in N$, it follows that ι_2 is surjetive. Next we show $\bar{\iota}_2$ is injective (hence an isomorphism). Suppose $\overline{w} \in N/M$ such that $\overline{[0,w]} = 0$ in $(E +_M N)/E$. Then there exists some $u \in E$ such that $[0,w] = [u,0]$. Since φ is surjective, there exists some $v \in M$ such that $\varphi v = u$. Thus

$$[0,w] = [u,0] = [\varphi v, 0] = [0, -\psi v].$$

In particular, we see that $[0, w + \psi v] = 0$. Thus there $v' \in M$ such that $\varphi v' = 0$ and $\psi v' = w + \psi v$, or in other words $w = \psi(v' - v)$. It follows that $\overline{w} = 0$ in N/M, hence $\bar{\iota}_2$ is injective.

□

Theorem 67.3. *Let (M, d) be an R-complex such that $M_i = 0$ for all $i > 0$. Then there exists an injective resolution of (M, d).*

Proof. We construct an R-complex (E, ∂) together with an injective chain map $\varepsilon\colon M \to E$ which induces an injective map

$$\bar{\varepsilon}\colon C_M := M/\operatorname{im}\mathrm{d} \to E/\operatorname{im}\partial =: C_E$$

by induction on homological degree as follows: for $i > 0$, we set $E_i = 0$, $\partial_{i+1} = 0$, and $\varepsilon_i = 0$. For $i = 0$, we choose an injective R-module E_0 together with an injective R-linear map $\varepsilon_0\colon M_0 \to E_0$ and we set $\partial_1\colon E_1 \to E_0$ to be the zero map. Suppose for some $k < 0$, we have constructed R-linear maps $\varepsilon_i\colon M_i \to E_i$ and $\partial_{i+1}\colon E_{i+1} \to E_i$ such that

$$\partial_{i-1}\partial_i = 0 \quad \text{and} \quad \partial_{i+1}\varepsilon_{i+1} = \varepsilon_i \mathrm{d}_{i+1}$$

and such that ε_i induces an injective map

$$\bar{\varepsilon}_i\colon C_{M,i} := M_i/\operatorname{im}\mathrm{d}_{i+1} \to E_i/\operatorname{im}\partial_{i+1} := C_{E,i}$$

for all $i > k$. We first construct the pushout

$$\begin{tikzcd} C_{E,k} \arrow[r, "\iota_1"] & C_{E,k} +_{C_{M,k}} M_{k-1} \\ C_{M,k} \arrow[u, "\bar{\varepsilon}_k"] \arrow[r, "\mathrm{d}_k"] & M_{k-1} \arrow[u, "\iota_2"'] \end{tikzcd}$$

here the map $\bar{\varepsilon}_k$ is well-defined since ε_k commutes with the differentials. Now we choose an injective R-module E_{k-1} together with an injective R-linear map

$$\rho_k\colon C_{E,k} +_{C_{M,k}} M_{k-1} \to E_{k-1}.$$

and we set $\partial_k = \rho_k \circ \iota_1 \circ \pi$ and $\varepsilon_{k-1} = \rho_k \circ \iota_2$. Observe that $\partial_k \circ \partial_{k+1} = 0$ since ∂_k factors through $C_{E,k} = E_k/\operatorname{im}\partial_{k+1}$. Also observe that

$$\begin{aligned} \partial_k \circ \varepsilon_k &= \rho_k \circ \iota_1 \circ \pi_k \circ \varepsilon_k \\ &= \rho_k \circ \iota_1 \circ \bar{\varepsilon}_k \circ \pi_k \\ &= \rho_k \circ \iota_2 \circ \mathrm{d}_k \circ \pi_k \\ &= \varepsilon_{k-1} \circ \mathrm{d}_k \circ \pi_k \\ &= \varepsilon_{k-1} \circ \mathrm{d}_k \end{aligned}$$

Finally, observe that $\bar{\varepsilon}_{k-1}\colon C_{M,k-1} \to C_{E,k-1}$ is injective since it is a composition of injective maps.

$$\ker\partial_k = \ker(\pi_2 \circ \rho_k) \xrightarrow{\rho_k} \ker\pi_2 \underset{\cong}{\xrightarrow{\pi_1}} \ker\mathrm{d}_k$$

where the isomorphism $\ker\pi_2 \cong \ker\mathrm{d}_k$ follows from Proposition (67.2). This completes the induction step. Therefore we have an R-complex (P, ∂) together with a chain map $\tau\colon (P, \partial) \to (M, \mathrm{d})$ which restricts to a surjection

$$\tau|_{\ker\partial}\colon \ker\partial \to \ker\mathrm{d}.$$

Moreover, Proposition (67.2) implies

$$\begin{aligned} \mathrm{H}_{k-1}(M) &= \ker(C_{M,k} \to M_{k-1}) \\ &\cong \ker(C_{E,k} \to C_{E,k} +_{C_{M,k}} M_{k-1}) \\ &= \ker(C_{E,k} \to C_{E,k} +_{C_{M,k}} M_{k-1} \rightarrowtail E_{k-1}) \\ &= \mathrm{H}_{k-1}(E). \end{aligned}$$

It follows that ε is a quasi-isomorphism. □

67.1.3 Extra

Let (M, d) be an R-complex. We know wish to show how to construct a semiprojective resolution of M. That is, we will build an R-complex $(P^{-\infty}, \partial^{-\infty})$ together with a quasi-isomorphism $\tau^{-\infty}\colon (P^{-\infty}, \partial^{-\infty}) \to (M, \mathrm{d})$. We proceed as follows: for each $n \in \mathbb{Z}$, let $M^{(n)}$ be the R-complex whose component in homological degree i is given by

$$M_i^{(n)} = \begin{cases} M_i & \text{if } i \geq n \\ \mathrm{d}M_n & \text{if } i = n-1 \\ 0 & \text{if } i < n-1 \end{cases}$$

and let $\tau^{(n)}\colon P^{(n)} \to M^{(n)}$ be a semiprojective resolution of $M^{(n)}$. The obvious map $M^{(n)} \to M^{(n-1)}$ lifts to a chain map $\varphi^{(n)}\colon P^{(n)} \to P^{(n-1)}$ which has the property that it induces an isomorphism

$$\mathrm{H}_i(P^{(n)}) \cong \mathrm{H}_i(M) \cong \mathrm{H}_i(P^{(n-1)})$$

for all $i > n$. Now set $P = \varinjlim P^{(n)}$. Then P is a semiprojective resolution of $M = \varinjlim M^{(n)}$.

67.2 Semiprojective and semi-injective complexes

Definition 67.4. Let P be an R-complex of projective R-modules and let E be an R-complex of injective R-modules.

1. We say P is **semi-projective** if $\mathrm{Hom}_R^\star(P, -)$ respects quasi-isomorphisms. If $\tau\colon P \to X$ is a quasi-isomorphism, then we say P is a **semiprojective resolution** of X.

2. We say E is **semi-injective** if $\mathrm{Hom}_R^\star(-, E)$ respects quasi-isomorphisms. If $\varepsilon\colon X \to E$ is a quasi-isomorphism, then we say E is a **semi-injective resolution** of X.

Proposition 67.3. *Let P be an R-complex of projective modules and let E be an R-complex of injective modules. Then P is semiprojective if and only if $\mathrm{Hom}_R^\star(P, -)$ takes exact complexes to exact complexes. Similarly, E is semi-injective if and only if $\mathrm{Hom}_R^\star(-, E)$ takes exact complexes to exact complexes.*

Proof. First suppose that $\mathrm{Hom}_R^\star(P, -)$ is exact. Let $\varphi\colon A \to A'$ be a quasiisomorphism. Then

$$\begin{aligned} \varphi\colon A \to A' \text{ is a quasiisomorphism} &\implies \mathrm{C}(\varphi) \text{ is exact} \\ &\implies \mathrm{Hom}_R^\star(P, \mathrm{C}(\varphi)) \text{ is exact} \\ &\implies \mathrm{C}(\mathrm{Hom}_R^\star(P, \varphi)) \text{ is exact} \\ &\implies \mathrm{Hom}_R^\star(P, \varphi) \text{ is a quasiisomorphism.} \end{aligned}$$

Convsersely, suppose P is semiprojective. Let M be an exact R-complex. Then the zero map $M \to 0$ is a quasiisomorphism. Since P is semiprojective, the induced map $\mathrm{Hom}_R^\star(P, M) \to 0$ is a quasiisomorphism. This implies $\mathrm{Hom}_R^\star(P, M)$ is exact. Thus $\mathrm{Hom}_R^\star(P, -)$ is exact. The proof is similar for the injective case. □

67.2.1 Operations on semiprojective R-complexes

Proposition 67.4. *Let P and P' be semiprojective R-complexes.*

1. *ΣP is semiprojective;*

2. *if $\varphi\colon P \to P'$ is a chain map, then $\mathrm{C}(\varphi)$ is semiprojective;*

3. *$P \oplus P'$ is semiprojective;*

4. *if Q is a complex of projective R-modules, then $\mathrm{C}(1_Q)$ is semiprojective.*

5. *$P \otimes_R P'$ is semiprojective.*

Proof. 1. Let M be an exact R-complex. Then

$$\mathrm{Hom}_R^\star(\Sigma P, M) \cong \Sigma^{-1}\mathrm{Hom}_R^\star(P, M)$$

is exact. It follows that ΣP is semiprojective.

2. Let M be an exact R-complex. Observe that the exact sequence

$$0 \longrightarrow P' \xrightarrow{\iota} \mathrm{C}(\varphi) \xrightarrow{\pi} \Sigma P \longrightarrow 0$$

is degreewise split exact. Therefore the sequence

$$0 \longrightarrow \mathrm{Hom}_R^\star(\Sigma P, M) \xrightarrow{\pi^*} \mathrm{Hom}_R^\star(\mathrm{C}(\varphi), M) \xrightarrow{\iota^*} \mathrm{Hom}_R^\star(P, M) \longrightarrow 0$$

is exact. It follows from the fact that both $\mathrm{Hom}_R^\star(\Sigma P, M)$ and $\mathrm{Hom}_R^\star(P', M)$ are exact and from the long exact sequence in homology that $\mathrm{Hom}_R^\star(\mathrm{C}(\varphi), M)$ is exact.

3. This follows from 2 and the fact that

$$P \oplus P' \cong \mathrm{C}(\Sigma^{-1} P \xrightarrow{0} P').$$

4. Let M be an exact R-complex. Then

$$\begin{aligned} \mathrm{Hom}_R^\star(\mathrm{C}(1_Q), M) &\cong \Sigma^{-1}\mathrm{C}(\mathrm{Hom}_R^\star(1_Q, M)) \\ &= \Sigma^{-1}\mathrm{C}(1_{\mathrm{Hom}_R^\star(Q,M)}) \end{aligned}$$

is exact.

5. By hom tensor adjointness, $\mathrm{Hom}_R(P \otimes_R P', -) \cong \mathrm{Hom}_R(P, \mathrm{Hom}_R(P', -))$ is a composition of two exact functors.

□

Theorem 67.4. *Every R-complex has a semiprojective resolution and a semiinjective resolution.*

67.2.2 A bounded below complex of projective R-modules is semiprojective

Lemma 67.5. *Let (P, ∂) be a bounded below complex of projective R-modules and let (M, d) be an exact R-complex. Then*

$$\mathrm{H}_0(\mathrm{Hom}_R^\star(P, M)) \cong 0. \tag{291}$$

Proof. By reindexing if necessary, we may assume that $P_i = 0$ for all $i < 0$. Recall that

$$\mathrm{Hom}_R^\star(P, M) = \{\text{homotopy classes of chain maps } \varphi\colon P \to M\}.$$

Thus in order to obtain (291), we need to show that any two chain maps from P to M are homotopic to each other. Let $\varphi\colon P \to M$ and $\psi\colon P \to M$ be any two chain maps. The idea is to build the homotopy $h\colon P \to M$ using induction on $i \geq 0$. The homotopy equation that needs to be satisfied is

$$\varphi - \psi = \mathrm{d}h + h\partial, \tag{292}$$

First, for each $i < 0$, we set $h_i\colon P_i \to M_{i+1}$ to be the zero map. Next we observe that $\mathrm{im}(\varphi_0 - \psi_0) \subseteq \mathrm{im}\,\mathrm{d}_1$. Indeed,

$$\begin{aligned} \mathrm{d}_0(\varphi_0 - \psi_0) &= \mathrm{d}_0\varphi_0 - \mathrm{d}_0\psi_0 \\ &= \varphi_{-1}\partial_0 - \psi_{-1}\partial_0 \\ &= (\varphi_{-1} - \psi_{-1})\partial_0 \\ &= (\varphi_{-1} - \psi_{-1}) \circ 0 \\ &= 0 \end{aligned}$$

implies

$$\begin{aligned} \mathrm{im}(\varphi_0 - \psi_0) &\subseteq \ker \mathrm{d}_0 \\ &= \mathrm{im}\,\mathrm{d}_1. \end{aligned}$$

Thus since P_0 is projective, $\mathrm{d}_1\colon M_1 \to \mathrm{im}\,\mathrm{d}_1$ is surjective, and $\varphi_0 - \psi_0\colon P_0 \to M_0$ lands in $\mathrm{im}\,\mathrm{d}_1$, there exists an R-linear map $h_0\colon P_0 \to P_1$ such that

$$\varphi_0 - \psi_0 = \mathrm{d}_1 h_0. \tag{293}$$

In homological degree $i = 0$, the equation (292) becomes (293). Thus, we are on the right track.

Now we use induction. Suppose for some $i > 0$ we have constructed an R-module homomorphism $h_i\colon P_i \to P_{i+1}$ such that

$$\varphi_i - \psi_i = \mathrm{d}_{i+1} h_i + h_{i-1}\partial_i. \tag{294}$$

Observe that $\operatorname{im}(\varphi_{i+1} - \psi_{i+1} - h_i\partial_{i+1}) \subseteq \operatorname{im} \mathrm{d}_{i+2}$. Indeed,

$$\begin{aligned}
\mathrm{d}_{i+1}(\varphi_{i+1} - \psi_{i+1} - h_i\partial_{i+1}) &= \mathrm{d}_{i+1}\varphi_{i+1} - \mathrm{d}_{i+1}\psi_{i+1} - \mathrm{d}_{i+1}h_i\partial_{i+1} \\
&= \varphi_i\partial_{i+1} - \psi_i\partial_{i+1} - \mathrm{d}_{i+1}h_i\partial_{i+1} \\
&= (\varphi_i - \psi_i - \mathrm{d}_{i+1}h_i)\partial_{i+1} \\
&= h_{i-1}\partial_i\partial_{i+1} \\
&= h_{i-1} \circ 0 \\
&= 0
\end{aligned}$$

implies

$$\begin{aligned}
\operatorname{im}(\varphi_{i+1} - \psi_{i+1} - h_i\partial_{i+1}) &\subseteq \ker \mathrm{d}_{i+1} \\
&= \operatorname{im} \mathrm{d}_{i+2}.
\end{aligned}$$

Therefore since P_{i+1} is projective, $\mathrm{d}_{i+2} \colon M_{i+2} \to \operatorname{im} \mathrm{d}_{i+2}$ is surjective, and $\varphi_{i+1} - \psi_{i+1} - h_i\partial_{i+1} \colon P_{i+1} \to M_{i+1}$ lands in $\operatorname{im} \mathrm{d}_{i+2}$, there exists an R-linear map $h_{i+1} \colon P_{i+1} \to P_{i+2}$ such that

$$\varphi_{i+1} - \psi_{i+1} - h_i\partial_{i+1} = \mathrm{d}_{i+2}h_{i+1},$$

which is the homotopy equation in degree $i+1$. □

Corollary 68. *Let P be a bounded below complex of projective R-modules. Then $\operatorname{Hom}^\star_R(P, -)$ respects exact complexes. In particular, this implies P is semiprojective.*

Proof. Let M be an exact R-complex. Observe that $\Sigma^i P$ is a bounded below complex of projective R-modules for each $i \in \mathbb{Z}$. It follows from Lemma (67.5) that for each $i \in \mathbb{Z}$ we have

$$\begin{aligned}
\mathrm{H}_i(\operatorname{Hom}^\star_R(P, M)) &= \mathrm{H}_{0-(-i)}(\operatorname{Hom}^\star_R(P, M)) \\
&= \mathrm{H}_0(\Sigma^{-i}\operatorname{Hom}^\star_R(P, M)) \\
&= \mathrm{H}_0(\operatorname{Hom}^\star_R(\Sigma^i P, M)) \\
&= 0.
\end{aligned}$$

Therefore $\operatorname{Hom}^\star_R(P, -)$ takes exact complexes to exact complexes.

Now we show that this implies $\operatorname{Hom}^\star_R(P, -)$ takes quasiisomorphisms to quasiisomorphisms. Let $\varphi \colon A \to A'$ be a quasiisomorphism. Then

$$\begin{aligned}
\varphi \colon A \to A' \text{ is a quasiisomorphism} &\implies \mathrm{C}(\varphi) \text{ is exact} \\
&\implies \operatorname{Hom}^\star_R(P, \mathrm{C}(\varphi)) \text{ is exact} \\
&\implies \mathrm{C}(\operatorname{Hom}^\star_R(P, \varphi)) \text{ is exact} \\
&\implies \operatorname{Hom}^\star_R(P, \varphi) \text{ is a quasiisomorphism.}
\end{aligned}$$

Therefore P is semiprojective. □

67.2.3 Lifting Lemma

Lemma 67.6. *Let P be a semiprojective R-complex, let $\tau \colon A \to B$ be a quasiisomorphism of R-complexes, and let $\varphi \colon P \to B$ be a chain map. There exists a chain map $\widetilde{\varphi} \colon P \to A$ such that $\tau\widetilde{\varphi} \sim \varphi$. If $\widetilde{\varphi}' \colon P \to A$ is another homotopic lift of φ with respect to τ, then $\widetilde{\varphi} \sim \widetilde{\varphi}'$. If in addition τ is surjective, then we can choose $\widetilde{\varphi} \colon P \to A$ such that $\tau\widetilde{\varphi} = \varphi$.*

Proof. Since $\operatorname{Hom}^\star_R(P, -)$ preserves quasiisomorphisms, we see that

$$\tau_* \colon \operatorname{Hom}^\star_R(P, A) \to \operatorname{Hom}^\star_R(P, B)$$

is a quasiisomorphism. In particular, τ_* induces an isomorphism in the degree 0 part of homology:

$$\mathrm{H}_0(\tau_*) \colon \mathrm{H}_0(\operatorname{Hom}^\star_R(P, A)) \to \mathrm{H}_0(\operatorname{Hom}^\star_R(P, B)).$$

Now φ represents the the homology class $[\varphi]$ in $\mathrm{H}_0(\operatorname{Hom}^\star_R(P, B))$, and since $\mathrm{H}_0(\tau_*)$ is an isomorphism, there exists a homology class $[\widetilde{\varphi}]$ in $\mathrm{H}_0(\operatorname{Hom}^\star_R(P, A))$ such that $[\varphi] = [\tau\widetilde{\varphi}]$. In other words we have $\tau\widetilde{\varphi} \sim \varphi$ since

$$\mathrm{H}_0(\operatorname{Hom}^\star_R(P, A)) = \mathcal{C}(P, A)/\sim.$$

This shows the existence of a homotopic lift of φ with respect to τ. If $\widetilde{\varphi}' \colon P \to A$ is another homotopic lift of φ with respect to τ, then $[\widetilde{\varphi}'] = [\widetilde{\varphi}]$ since $\mathrm{H}_0(\tau_*)$ is an isomorphism, hence $\widetilde{\varphi} \sim \widetilde{\varphi}'$.

Now assume that τ is surjective. Choose a homotopic lift of φ with respect to τ, say $\widetilde{\varphi}\colon P \to A$, and choose a homotopy from $\tau\widetilde{\varphi}$ to φ, say $h\colon P \to B$. Thus if we set $\varphi_h = \varphi + \mathrm{d}h + h\mathrm{d}$, then we have $\tau\widetilde{\varphi} = \varphi_h$. Using the fact that P is a graded projective R-module and τ is surjective, we choose a graded lift of h with respect to τ, say $\widetilde{h}\colon P \to A$. So $\widetilde{h}$ is a graded homomorphism of degree 1 such that $\tau\widetilde{h} = h$. Thus if we set $\widetilde{\varphi}_{\widetilde{h}} := \widetilde{\varphi} - \mathrm{d}\widetilde{h} - \widetilde{h}\mathrm{d}$, then we have $\widetilde{\varphi} \sim \widetilde{\varphi}_{\widetilde{h}}$ and

$$\begin{aligned}
\tau\widetilde{\varphi}_{\widetilde{h}} &= \tau(\widetilde{\varphi} - \mathrm{d}\widetilde{h} - \widetilde{h}\mathrm{d}) \\
&= \tau\widetilde{\varphi} - \tau(\mathrm{d}\widetilde{h} + \widetilde{h}\mathrm{d}) \\
&= \varphi_h - (\mathrm{d}h + h\mathrm{d}) \\
&= \varphi.
\end{aligned}$$

□

67.2.4 When is an R-complex quasiisomorphic to its own homology?

Let P be a semiprojective R-complex. Set $Z = \ker \mathrm{d}$, $B = \operatorname{im} \mathrm{d}$, and $H = \mathrm{H}(P)$. Assume that B is semiprojective as well. Then the short exact sequence of graded R-modules

$$0 \longrightarrow Z \longrightarrow P \xrightarrow{\ \mathrm{d}\ } \Sigma B \longrightarrow 0 \tag{295}$$

splits (as graded R-modules), hence Z is also semiprojective and there exists a surjective graded homomorphism $\varphi\colon P \to Z$ which restricts to the identity on Z. In particular, the composite $\varphi'\colon P \to Z \to H$ is a chain map since $\varphi\mathrm{d} = \mathrm{d} = 0$ which induces identity $H \to H$ in homology. Thus φ' is a quasiisomorphism.

Definition 67.5. A ring R is called **hereditary** if all submodules of projective R-modules are again projective R-modules. If this is required only for finitely generated submodules, then we say R is **semiheritary**.

Example 67.2. R is hereditary if and only if all R-modules have projective resolutions of length at most 1.

Example 67.3. R is hereditary if and only if all ideals of R are projective modules. For instance, Dedekind domains are hereditary.

Example 67.4. The triangular matrix ring $\left(\begin{smallmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{smallmatrix}\right)$ is right hereditary and left semihereditary but not left hereditary.

67.3 Base Change in Tor

Let $R \to R'$ be a ring homomorphism, let M be an R-module, and let N' be an R'-module. Using the ring homomorphism $R \to R'$, we can transport the R-module M to an R'-modules $M \otimes_R R'$. It turns out that this induces an R'-module homomorphism in Tor:

$$\mathrm{Tor}^R(M, N') \to \mathrm{Tor}^{R'}(R' \otimes_R M, N'). \tag{296}$$

Indeed, let P be a projective resolution of M over R and let P' be a projective resolution of $R' \otimes_R M$ over R'. Choose a homotopy lift $\sigma\colon R' \otimes_R P \to P'$ of the chain map $R' \otimes_R P \to R' \otimes_R M$. Then we obtain (296) by applying the homology functor to the following sequence of maps:

$$P \otimes_R N' \simeq R' \otimes_{R'} (P \otimes_R N') \simeq (R' \otimes_R P) \otimes_{R'} N' \xrightarrow{\sigma \otimes 1} P' \otimes_{R'} N'. \tag{297}$$

Note that the choice of a homotopy lift $R' \otimes_R P \to P'$ is unique up to homotopy, so we get the same map in Tor no matter which homotopy lift we choose. This Tor map also doesn't depend on the choice of projective resolutions P and P' since they too are unique up to homotopy. In particular, if $R \to R'$ is flat, then already $R' \otimes_R P'$ is a projective resolution of $R' \otimes_R M'$ and thus we can choose the identity map $R' \otimes_R P \to R' \otimes_R P$ in (297), and in fact this shows that $P \otimes_R N'$ and $P' \otimes_{R'} N'$ are isomorphic as complexes, so in particular (296) would certainly be an isomorphism in this case. In general, let K

Not only do we get a R'-module homomorphism in Tor, but we also get an R'-module homomorphism in Ext:

$$\mathrm{Ext}_{R'}(R' \otimes_R M, N') \to \mathrm{Ext}_R(M, N'). \tag{298}$$

Indeed, we obtain (**??**) by applying the homology functor to this sequence of maps:

$$\mathrm{Hom}^\star_{R'}(P', N') \to \mathrm{Hom}^\star_{R'}(P \otimes_R R', N') \simeq \mathrm{Hom}^\star_R(P, \mathrm{Hom}_{R'}(R', N')) \simeq \mathrm{Hom}^\star_R(P, N').$$

67.4 Ext Functor

67.5 Base Change in Tor

Let S be an R-algebra, let M be an R-module and let N be an S-module. Then there exists a natural graded S-module homomorphism

$$\mathrm{Tor}^R(M,N) \to \mathrm{Tor}^S(S \otimes_R M, N).$$

Indeed, let F be an R-projective resolution of M (so in particular we have a surjective quasiisomorphism $\sigma\colon F \xrightarrow{\simeq} M$). Let G be an S-projective resolution of $S \otimes_R M$ (so in particular, we have a surjective quasiisomorphism $\tau\colon G \to S \otimes_R M$). Note that $S \otimes_R F$ is a semiprojective S-complex. Therefore by the homotopy lifting lemma, the chain map $1 \otimes \sigma\colon S \otimes_R F \to S \otimes_R M$ lifts to a chain map $\varphi\colon S \otimes_R F \to G$ such that $\tau\varphi = 1 \otimes \sigma$. The map φ is unique up to homotopy by the homotopy lifting lemma. Therefore φ induces a canonical map in homology:

$$\begin{aligned}\mathrm{Tor}^R(M,N) &:= \mathrm{H}(F \otimes_R N)\\ &\to \mathrm{H}(S \otimes_R F \otimes_R N)\\ &\to \mathrm{H}(G \otimes_R N)\\ &:= \mathrm{Tor}^S(S \otimes_R M, N).\end{aligned}$$

The map $\mathrm{H}(F \otimes_R N) \to \mathrm{H}(S \otimes_R F \otimes_R N)$ in induced by the map of S-complexes $F \otimes_R N \to S \otimes_R F \otimes_R N$ given by $a \otimes n \mapsto 1 \otimes a \otimes n$ for all $a \in F$ and $n \in N$. The map $\mathrm{H}(S \otimes_R F \otimes_R N) \to \mathrm{H}(G \otimes_R N)$ is induced by the map $\varphi \otimes 1$. In homological degree 0, this is none other than the usual base change in tensor products:

$$M \otimes_R N \to S \otimes_R M \otimes_R N$$

given by $m \otimes n \mapsto 1 \otimes m \otimes n$ for all $m \in M$ and $n \in N$.

67.6 Ext Functor

Definition 67.6. Let A and B be R-complexes. We define the graded R-module $\mathrm{Ext}_R(A,B)$ as follows: choose a semiprojective resolution $\tau\colon P \to A$. Then set

$$\mathrm{Ext}_R(A,B) := \mathrm{H}(\mathrm{Hom}^\star_R(P,B)).$$

The ith homogeneous component of $\mathrm{Ext}_R(A,B)$ is denoted

$$\mathrm{Ext}^i_R(A,B) := \mathrm{H}_{-i}(\mathrm{Hom}^\star_R(P,B)).$$

One might argue that this isn't well-defined since if we had chosen a different projective resolution $\tau'\colon P' \to A$, then $\mathrm{H}(\mathrm{Hom}_R(P',B))$ isn't literally the same as $\mathrm{H}(\mathrm{Hom}_R(P,B))$. However the key is that there is a canonical isomorphism from $\mathrm{H}(\mathrm{Hom}_R(P',B))$ to $\mathrm{H}(\mathrm{Hom}_R(P,B))$. This is why it's okay to write equal signs here:

$$\mathrm{Ext}_R(A,B) := \mathrm{H}(\mathrm{Hom}_R(P,B)) = \mathrm{H}(\mathrm{Hom}_R(P',B)).$$

Theorem 67.7. $\mathrm{Ext}_R(A,B)$ *is well-defined up to a canonical isomorphism.*

Proof. Suppose $\tau_1\colon P_1 \to A$ and $\tau_2\colon P_2 \to A$ are two semiprojective resolutions of A. Choose a homotopic lift $\widetilde{\tau}_1\colon P_1 \to P_2$ of τ_1 with respect to τ_2 (such a lift is unique up to homotopy). Similarly choose a homotopic lift $\widetilde{\tau}_2\colon P_2 \to P_1$ of τ_2 with respect to τ_1 (again this lift is unique up to homotopy). We claim that $\widetilde{\tau}_1\colon P_1 \to P_2$ is a homotopy equivalence with $\widetilde{\tau}_2\colon P_2 \to P_1$ being its homotopy inverse. Indeed, observe that

$$\begin{aligned}\tau_1\widetilde{\tau}_2\widetilde{\tau}_1 &\sim \tau_2\widetilde{\tau}_1\\ &\sim \tau_1\end{aligned}$$

implies $\widetilde{\tau}_2\widetilde{\tau}_1$ is a homotopic lift of τ_1 with respect to τ_1, but 1_{P_1} is also a homotopic lift of τ_1 with respect to τ_1. Therefore $\widetilde{\tau}_2\widetilde{\tau}_1 \sim 1_{P_1}$. A similar computation gives $\widetilde{\tau}_1\widetilde{\tau}_2 \sim 1_{P_2}$. Now $\mathrm{Hom}^\star_R(-,B)$ preserves homotopy equivalences, and thus $\mathrm{Hom}^\star_R(\widetilde{\tau}_1,B)\colon \mathrm{Hom}^\star_R(P_1,B) \to \mathrm{Hom}^\star_R(P_2,B)$ is a homotopy equivalence. Then since the homology functor takes homotopy equivalences to isomorphisms, we see that

$$\mathrm{H}(\mathrm{Hom}^\star_R(\widetilde{\tau}_1,B))\colon \mathrm{H}(\mathrm{Hom}^\star_R(P_1,B)) \to \mathrm{H}(\mathrm{Hom}^\star_R(P_2,B))$$

is an isomorphism. Furthermore, this isomorphism is canonical since $\widetilde{\tau}_1$ is unique up to homotopy (if $\widetilde{\tau}_1'\colon P_1 \to P_2$ were another homotopic lift of τ_1 with respect to τ_2, then we'd have $\mathrm{H}(\mathrm{Hom}^\star_R(\widetilde{\tau}_1{}',B)) = \mathrm{H}(\mathrm{Hom}^\star_R(\widetilde{\tau}_1,B))$) □

67.6.1 The functor $\mathrm{Ext}_R(A,-)$

Now that we've defined the module $\mathrm{Ext}_R(A,B)$, we want to define the covariant functor

$$\mathrm{Ext}_R(A,-)\colon \mathbf{Comp}_R \to \mathbf{Grad}_R.$$

Clearly, we want this functor to map an R-complex B to the graded R-module $\mathrm{Ext}_R(A,B)$. Let us show how it should act on chain maps:

Definition 67.7. Let $\psi\colon B \to B'$ be a chain map and let $\tau\colon P \to A$ be a semiprojective resolution of A. We define

$$\mathrm{Ext}_R(A,\psi)\colon \mathrm{Ext}_R(A,B) \to \mathrm{Ext}_R(A,B')$$

by $\mathrm{Ext}_R(A,\psi) := \mathrm{H}(\mathrm{Hom}_R^\star(A,\psi))$.

Again, in our definition of $\mathrm{Ext}_R(A,\psi)$, we *chose* a semiprojective resolution of A. Let us now show that had we chosen a different semiprojective resolution of A, we would get a *naturally isomorphic* functor which is *canonical*. Thus the functor $\mathrm{Ext}_R(A,-)$ is well-defined *up to a canonical natural isomorphism*.

Theorem 67.8. $\mathrm{Ext}_R(A,-)$ *is well-defined up to a canonical natural isomorphism.*

Proof. Suppose $\tau_1\colon P_1 \to A$ and $\tau_2\colon P_2 \to A$ are two semiprojective resolutions of A. Choose a homotopic lift $\widetilde{\tau}_2\colon P_2 \to P_1$ of τ_2 with respect to τ_1. Then $\widetilde{\tau}_2$ is a homotopy equivalence, by the same argument as in the proof of Theorem (67.10). Now observe that the diagram

$$\begin{tikzcd}
\mathrm{Hom}_R^\star(P_1,B) \arrow[r, "\mathrm{Hom}_R^\star(\widetilde{\tau}_2,B)"] \arrow[d, "\mathrm{Hom}_R^\star(P_1,\psi)"'] & \mathrm{Hom}_R^\star(P_2,B) \arrow[d, "\mathrm{Hom}_R^\star(P_2,\psi)"] \\
\mathrm{Hom}_R^\star(P_1,B') \arrow[r, "\mathrm{Hom}_R^\star(\widetilde{\tau}_2,B')"'] & \mathrm{Hom}_R^\star(P_2,B')
\end{tikzcd}$$

is commutative. Therefore we obtain a commutative diagram after apply homology:

$$\begin{tikzcd}
\mathrm{H}(\mathrm{Hom}_R^\star(P_1,B)) \arrow[r, "\mathrm{H}(\mathrm{Hom}_R^\star(\widetilde{\tau}_2,B))"] \arrow[d, "\mathrm{H}(\mathrm{Hom}_R^\star(P_1,\psi))"'] & \mathrm{H}(\mathrm{Hom}_R^\star(P_2,B)) \arrow[d, "\mathrm{H}(\mathrm{Hom}_R^\star(P_2,\psi))"] \\
\mathrm{H}(\mathrm{Hom}_R^\star(P_1,B')) \arrow[r, "\mathrm{H}(\mathrm{Hom}_R^\star(\widetilde{\tau}_2,B'))"'] & \mathrm{H}(\mathrm{Hom}_R^\star(P_2,B'))
\end{tikzcd}$$

Since the rows are isomorphisms, we see that $\mathrm{H}(\mathrm{Hom}_R^\star(\widetilde{\tau}_2,-))$ is a natural isomorphism. This natural isomorphism is canonical since different choices of homotopic lifts are all homotopic to each other. □

67.6.2 The functor $\mathrm{Ext}_R(-,B)$

Next we want to define the contravariant functor

$$\mathrm{Ext}_R(-,B)\colon \mathbf{Comp}_R \to \mathbf{Grad}_R.$$

Again, we want this functor to send and an R-complex A to the graded R-module $\mathrm{Ext}_R(A,B)$. This time, the way it acts on chain maps will be a little more involved than in the covariant case.

Definition 67.8. Let $\varphi\colon A \to A'$ be a chain map, let $\tau\colon P \to A$ be a semiprojective resolution of A, let $\tau'\colon P' \to A'$ be a semiprojective resolution of A', and let $\widetilde{\varphi}\colon P \to P'$ be a homotopic lift of $\varphi\tau$ with respect to τ'. We define

$$\mathrm{Ext}_R(\varphi,B)\colon \mathrm{Ext}_R(A',B) \to \mathrm{Ext}_R(A,B).$$

by $\mathrm{Ext}_R(\varphi,B) := \mathrm{H}(\mathrm{Hom}_R^\star(\widetilde{\varphi},B))$.

This time our definition of the functor $\mathrm{Ext}_R(-,B)$ involves *three choices*; namely, the semiprojective resolutions $\tau\colon P \to A$ and $\tau'\colon P' \to A'$ as well as the homotopic lift $\widetilde{\varphi}\colon P \to P'$. Even though we made three choices, we shall still see that $\mathrm{Ext}_R(-,B)$ is well-defined up to a canonical natural isomorphism.

Theorem 67.9. $\mathrm{Ext}_R(-,B)$ *is well-defined up to a canonical natural isomorphism.*

Proof. Suppose $\tau_1\colon P_1 \to A$ and $\tau_2\colon P_2 \to A$ are two semiprojective resolutions of A, suppose $\tau_1'\colon P_1' \to A'$ and $\tau_2'\colon P_2' \to A'$ are two semiprojective resolutions of A', and suppose $\widetilde{\varphi_1}\colon P_1 \to P_1'$ is a homotopic lift of $\varphi\tau_1$ with respect to τ_1' and $\widetilde{\varphi_2}\colon P_2 \to P_2'$ is a homotopic lift of $\varphi\tau_2$ with respect to τ_2'. So altogether we have the diagrams

$$\begin{tikzcd} P_1 \arrow[r, "\widetilde{\varphi_1}"] \arrow[d, "\tau_1"'] & P_1' \arrow[d, "\tau_1'"] \\ A \arrow[r, "\varphi"'] & A' \end{tikzcd} \qquad \begin{tikzcd} P_2 \arrow[r, "\widetilde{\varphi_2}"] \arrow[d, "\tau_2"'] & P_2' \arrow[d, "\tau_2'"] \\ A \arrow[r, "\varphi"'] & A' \end{tikzcd}$$

which commute up to homotopy.

Choose a homotopic lift $\widetilde{\tau}_2\colon P_2 \to P_1$ of τ_2 with respect to τ_1 and choose a homotopic lift $\widetilde{\tau}_2{}'\colon P_2' \to P_1'$ of τ_2' with respect to τ_1'. Then $\widetilde{\tau}_2$ and $\widetilde{\tau}_2{}'$ are both homotopy equivalences by the same argument as in the proof of Theorem (67.10). Now observe that

$$\begin{aligned} \tau_1'\widetilde{\tau}_2{}'\widetilde{\varphi_2} &\sim \tau_2'\widetilde{\varphi_2} \\ &\sim \varphi\tau_2 \\ &\sim \varphi\tau_1\widetilde{\tau}_2 \\ &\sim \tau_1'\widetilde{\varphi_1}\widetilde{\tau}_2. \end{aligned}$$

In particular, both $\widetilde{\tau}_2{}'\widetilde{\varphi_2}\colon P_2 \to P_1'$ and $\widetilde{\varphi_1}\widetilde{\tau}_2\colon P_2 \to P_1'$ are homotopic lifts of $\varphi\tau_2$ with respect to τ_1'. Therefore $\widetilde{\tau}_2{}'\widetilde{\varphi_2} \sim \widetilde{\varphi_1}\widetilde{\tau}_2$, which further implies

$$\begin{aligned} \mathrm{Hom}_R^\star(\widetilde{\varphi_2}, B)\mathrm{Hom}_R^\star(\widetilde{\tau}_2{}', B) &= \mathrm{Hom}_R^\star(\widetilde{\tau}_2{}'\widetilde{\varphi_2}, B) \\ &\sim \mathrm{Hom}_R^\star(\widetilde{\varphi_1}\widetilde{\tau}_2, B) \\ &= \mathrm{Hom}_R^\star(\widetilde{\tau}_2, B)\mathrm{Hom}_R^\star(\widetilde{\varphi_1}, B) \end{aligned}$$

since $\mathrm{Hom}_R^\star(-, B)$ respects homotopies. Therefore we have a diagram

$$\begin{tikzcd} \mathrm{Hom}_R^\star(P_1', B) \arrow[r, "\mathrm{Hom}_R^\star(\widetilde{\tau}_2{}', B)"] \arrow[d, "\mathrm{Hom}_R^\star(\widetilde{\varphi_1}, B)"'] & \mathrm{Hom}_R^\star(P_2', B) \arrow[d, "\mathrm{Hom}_R^\star(\widetilde{\varphi_2}, B)"] \\ \mathrm{Hom}_R^\star(P_1, B') \arrow[r, "\mathrm{Hom}_R^\star(\widetilde{\tau}_2, B)"'] & \mathrm{Hom}_R^\star(P_2, B) \end{tikzcd}$$

which commutes up to homotopy. Then since homology takes homotopic maps to equal maps, we see that the diagram

$$\begin{tikzcd} \mathrm{H}(\mathrm{Hom}_R^\star(P_1', B)) \arrow[r, "\mathrm{H}(\mathrm{Hom}_R^\star(\widetilde{\tau}_2{}', B))"] \arrow[d, "\mathrm{H}(\mathrm{Hom}_R^\star(\widetilde{\varphi_1}, B))"'] & \mathrm{H}(\mathrm{Hom}_R^\star(P_2', B)) \arrow[d, "\mathrm{H}(\mathrm{Hom}_R^\star(\widetilde{\varphi_2}, B))"] \\ \mathrm{H}(\mathrm{Hom}_R^\star(P_1, B)) \arrow[r, "\mathrm{H}(\mathrm{Hom}_R^\star(\widetilde{\tau}_2, B))"'] & \mathrm{H}(\mathrm{Hom}_R^\star(P_2, B)) \end{tikzcd}$$

is commutative. Since the rows are isomorphisms, we see that $\mathrm{H}(\mathrm{Hom}_R^\star(-, B))$ is a natural isomorphism. □

67.6.3 Properties of Ext

Proposition 67.5. *Let A, B be R-complexes, let $\{A_\lambda\}$ and $\{B_\lambda\}$ be a collection of R-complexes indexed over a set Λ, and let $S \subseteq R$ be a multiplicatively closed set. Then*

1. $\mathrm{Ext}_R\left(\bigoplus_{\lambda\in\Lambda} A_\lambda, B\right) \cong \prod^\star_{\lambda\in\Lambda} \mathrm{Ext}_R\left(A_\lambda, B\right)$;
2. $\mathrm{Ext}_R\left(A, \prod^\star_{\lambda\in\Lambda} B_\lambda\right) \cong \prod^\star_{\lambda\in\Lambda} \mathrm{Ext}_R(A, B_\lambda)$
3. *If A is finitely presented, then* $\mathrm{Ext}_R(A, B)_S \cong \mathrm{Ext}_{R_S}(A_S, B_S)$.

Proof. Choose a semiprojective resolutions $\tau_\lambda\colon P_\lambda \to A_\lambda$ of A_λ for each $\lambda \in \Lambda$. Then $\oplus\tau_\lambda\colon \bigoplus_\lambda P_\lambda \to \bigoplus_\lambda A_\lambda$ is a semiprojective resolution of $\bigoplus_\lambda A_\lambda$. Indeed, the homogeneous piece in degree i of $\bigoplus_\lambda P_\lambda$ is given by $\bigoplus_\lambda P_{\lambda,i}$, where $P_{\lambda,i}$ is the homogeneous piece in degree i of P_λ for all $\lambda \in \Lambda$, and $\bigoplus_\lambda P_{\lambda,i}$ is a projective R-module since each $P_{\lambda,i}$ is a projective R-module. Also, $\oplus\tau_\lambda$ is a quasiisomorphism since each τ_λ is a quasiisomorphism and since homology commutes with direct sums.

Therefore

$$\begin{aligned}
\operatorname{Ext}_R\left(\bigoplus_{\lambda\in\Lambda} A_\lambda, B\right) &= \mathrm{H}\left(\operatorname{Hom}_R^\star\left(\bigoplus_{\lambda\in\Lambda} A_\lambda, B\right)\right)\\
&= \mathrm{H}\left(\prod_{\lambda\in\Lambda}^{\star} \operatorname{Hom}_R^\star(A_\lambda, B)\right)\\
&= \prod_{\lambda\in\Lambda}^{\star} \mathrm{H}(\operatorname{Hom}_R^\star(A_\lambda, B))\\
&= \prod_{\lambda\in\Lambda}^{\star} \operatorname{Ext}_R(A_\lambda, B)
\end{aligned}$$

Similarly, choose a semiprojective resolution $\tau\colon P \to A$ of A. Then we have

$$\begin{aligned}
\operatorname{Ext}_R\left(A, \prod_{\lambda\in\Lambda}^{\star} B_\lambda\right) &= \mathrm{H}\left(\operatorname{Hom}_R^\star\left(P, \prod_{\lambda\in\Lambda}^{\star} B_\lambda\right)\right)\\
&= \mathrm{H}\left(\prod_{\lambda\in\Lambda}^{\star} \operatorname{Hom}_R^\star(P, B_\lambda)\right)\\
&= \prod_{\lambda\in\Lambda}^{\star} \mathrm{H}(\operatorname{Hom}_R^\star(P, B_\lambda))\\
&= \prod_{\lambda\in\Lambda}^{\star} \operatorname{Ext}_R(A, B_\lambda).
\end{aligned}$$

For the final equality, observe that $\tau_S\colon P_S \to A_S$ is a semiprojective resolution of A_S. Thus

$$\begin{aligned}
\operatorname{Ext}_{R_S}(A_S, B_S) &= \mathrm{H}\left(\operatorname{Hom}_{R_S}^\star(P_S, B_S)\right)\\
&= \mathrm{H}\left(\operatorname{Hom}_R^\star(P, B)_S\right)\\
&= \mathrm{H}(\operatorname{Hom}_R^\star(P, B))_S\\
&= \operatorname{Ext}_R(A, B)_S.
\end{aligned}$$

□

67.7 Semiflat complexes

Definition 67.9. Let M be an R-complex of flat R-modules. We say M is **semiflat** if $-\otimes_R M$ respects quasiisomorphisms. If $\tau\colon M \to X$ is a quasiisomorphism, then we say M is a **semiflat resolution** of X.

Remark 121. Since $-\otimes_R M$ is naturally isomorphic to $M \otimes_R -$, we see that M is semiflat if and only if $M \otimes_R -$ respects quasiisomorphisms.

Proposition 67.6. *Let M be an R-complex of flat R-modules. Then M is semiflat if and only if $M \otimes_R -$ is exact.*

Proof. First suppose that $-\otimes_R M$ is exact. Let $\varphi\colon A \to A'$ be a quasiisomorphism. Then

$$\begin{aligned}
\varphi\colon A \to A' \text{ is a quasiisomorphism} &\implies \mathrm{C}(\varphi) \text{ is exact}\\
&\implies \mathrm{C}(\varphi)\otimes_R M \text{ is exact}\\
&\implies \mathrm{C}(\varphi\otimes_R M) \text{ is exact}\\
&\implies \varphi\otimes_R M \text{ is a quasiisomorphism.}
\end{aligned}$$

Therefore $-\otimes_R M$ respects quasiisomorphisms.

Conversely, suppose M is semiflat. Let A be an exact R-complex. Then the zero map $M \to 0$ is a quasiisomorphism. Since M is semiflat, the induced map $A \otimes_R M \to 0$ is a quasiisomorphism. This implies $A \otimes_R M$ is exact. Therefore $-\otimes_R M$ is exact. □

67.7.1 Semiprojective complexes are semiflat

Proposition 67.7. *Let P be a semiprojective R-complex. Then P is semiflat.*

Proof. Since projective R-modules are flat, we see that P_i is flat for all $i \in \mathbb{Z}$. Now let A be an exact R-complex and let $\varepsilon\colon P \otimes_R A \to E$ be a semiinjective resolution. Then

$$\begin{aligned} P \otimes_R A \text{ is exact} &\iff \operatorname{Hom}^\star_R(P \otimes_R A, E) \text{ is exact} \\ &\iff \operatorname{Hom}^\star_R(P, \operatorname{Hom}^\star_R(A, E)) \text{ is exact.} \end{aligned}$$

the last line follows from the fact that P is semiprojective and E is semiinjective. □

67.8 Tor Functor

Definition 67.10. Let A and B be R-complexes. We define the graded R-module $\operatorname{Tor}^R(A, B)$ as follows: choose a semiprojective resolution $\tau\colon P \to A$. Then

$$\operatorname{Tor}^R(A, B) := \mathrm{H}(P \otimes_R B).$$

The ith homogeneous component of $\operatorname{Tor}^R(A, B)$ is denoted

$$\operatorname{Tor}^R_i(A, B) := \mathrm{H}_i(P \otimes_R B)$$

In our definition of $\operatorname{Tor}^R(A, B)$, we *chose* a semiprojective resolution of A. Let us now show that had we chosen a different semiprojective resolution of A, we would get an isomorphic object. Thus $\operatorname{Tor}^R(A, B)$ is well-defined *up to isomorphism*.

Theorem 67.10. $\operatorname{Tor}^R(A, B)$ *is well-defined up to isomorphism.*

Proof. Suppose $\tau_1\colon P_1 \to A$ and $\tau_2\colon P_2 \to A$ are two semiprojective resolutions of A. Choose a homotopic lift $\widetilde{\tau}_1\colon P_1 \to P_2$ of τ_1 with respect to τ_2. Similarly, choose a homotopic lift $\widetilde{\tau}_2\colon P_2 \to P_1$ of τ_2 with respect to τ_1. As in the proof of Theorem (67.10), $\widetilde{\tau}_1\colon P_1 \to P_2$ is a homotopy equivalence with $\widetilde{\tau}_2\colon P_2 \to P_1$ being its homotopy inverse. Now $- \otimes_R B$ preserves homotopy equivalences, and thus $\widetilde{\tau}_1 \otimes_R B\colon P_1 \otimes_R B \to P_2 \otimes_R B$ is a homotopy equivalence. Then since the homology functor takes homotopy equivalences to isomorphisms, we see that

$$\mathrm{H}(\widetilde{\tau}_1 \otimes_R B))\colon \mathrm{H}(P_1 \otimes_R B) \to \mathrm{H}(P_2 \otimes_R B)$$

is an isomorphism. This isomorphism is unique in a sense. Indeed, if we had chosen another homotopic lift of τ_1 with respect to τ_2, say $\widetilde{\tau}_1'\colon P_1 \to P_2$, then $\widetilde{\tau}_1 \sim \widetilde{\tau}_1{}'$, which implies $\widetilde{\tau}_1 \otimes_R B \sim \widetilde{\tau}_1{}' \otimes_R B$, which implies $\mathrm{H}(\widetilde{\tau}_1 \otimes_R B)) = \mathrm{H}(\widetilde{\tau}_1{}' \otimes_R B))$. □

67.8.1 The functor $\operatorname{Tor}^R(A, -)$

Now that we've defined the module $\operatorname{Tor}^R(A, B)$, we want to define the covariant functor

$$\operatorname{Tor}^R(A, -)\colon \mathbf{Comp}_R \to \mathbf{Grad}_R.$$

Clearly, we want this functor to map an R-complex B to the graded R-module $\operatorname{Tor}^R(A, B)$. Let us show how it should act on chain maps:

Definition 67.11. Let $\psi\colon B \to B'$ be a chain map and let $\tau\colon P \to A$ be a semiprojective resolution of A. We define

$$\operatorname{Tor}^R(A, \psi)\colon \operatorname{Tor}^R(A, B) \to \operatorname{Tor}^R(A, B')$$

by $\operatorname{Tor}^R(A, \psi) := \mathrm{H}(A \otimes_R \psi)$.

Again, in our definition of $\operatorname{Tor}^R(A, \psi)$, we *chose* a semiprojective resolution of A. Let us now show that had we chosen a different semiprojective resolution of A, we would get a *naturally isomorphic* functor. Thus the functor $\operatorname{Tor}^R(A, -)$ is well-defined *up to natural isomorphism*.

Theorem 67.11. $\operatorname{Tor}^R(A, -)$ *is well-defined up to natural isomorphism.*

Proof. Suppose $\tau_1\colon P_1 \to A$ and $\tau_2\colon P_2 \to A$ are two semiprojective resolutions of A. Choose a homotopic lift $\widetilde{\tau}_1\colon P_1 \to P_2$ of τ_1 with respect to τ_2. Then $\widetilde{\tau}_1$ is a homotopy equivalence, by the same argument as in the proof of Theorem (67.10). Now observe that the diagram

$$\begin{tikzcd} P_1 \otimes_R B \arrow[r, "\widetilde{\tau}_1 \otimes_R B"] \arrow[d, "P_1 \otimes_R \psi"'] & P_2 \otimes_R B \arrow[d, "P_2 \otimes_R \psi"] \\ P_1 \otimes_R B' \arrow[r, "\widetilde{\tau}_2 \otimes_R B'"'] & P_2 \otimes_R B' \end{tikzcd}$$

is commutative where the rows are homotopy equivalences since $-\otimes_R B$ preserves homotopy equivalences. Therefore we obtain a commutative diagram after apply homology

$$\begin{tikzcd} \mathrm{H}(P_1\otimes_R B) \arrow[r, "\mathrm{H}(\widetilde{\tau}_1\otimes_R B)"] \arrow[d, "\mathrm{H}(P_1\otimes_R\psi)"'] & \mathrm{H}(P_2\otimes_R B) \arrow[d, "\mathrm{H}(P_2\otimes_R\psi)"] \\ \mathrm{H}(P_1\otimes_R B') \arrow[r, "\mathrm{H}(\widetilde{\tau}_2\otimes_R B')"'] & \mathrm{H}(P_2\otimes_R B') \end{tikzcd}$$

where the rows are isomorphisms since the $\mathrm{H}(-)$ takes homotopy equivalences to isomorphisms. Since the rows are isomorphisms and the diagram commutes, we see that $\mathrm{H}(\mathrm{Tor}^R(\widetilde{\tau}_1,-))$ is a natural isomorphism. $\square$

67.8.2 The functor $\mathrm{Tor}^R(-,B)$

Next we want to define the covariant functor

$$\mathrm{Tor}^R(-,B)\colon \mathbf{Comp}_R\to\mathbf{Grad}_R.$$

Again, we want this functor to send and an R-complex A to the graded R-module $\mathrm{Tor}^R(A,B)$.

Definition 67.12. Let $\varphi\colon A\to A'$ be a chain map, let $\tau\colon P\to A$ be a semiprojective resolution of A, let $\tau'\colon P'\to A'$ be a semiprojective resolution of A', and let $\widetilde{\varphi}\colon P\to P'$ be a homotopic lift of $\varphi\tau$ with respect to τ'. We define

$$\mathrm{Tor}^R(\varphi,B)\colon \mathrm{Tor}^R(A,B)\to\mathrm{Tor}^R(A',B).$$

by $\mathrm{Tor}^R(\varphi,B):=\mathrm{H}(\widetilde{\varphi}\otimes_R B)$.

This time our definition of the functor $\mathrm{Tor}^R(-,B)$ involves *three choices*; namely, the semiprojective resolutions $\tau\colon P\to A$ and $\tau'\colon P'\to A'$ as well as the homotopic lift $\widetilde{\varphi}\colon P\to P'$. Even though we made three choices, we shall still see that $\mathrm{Tor}^R(-,B)$ is well-defined up to natural isomorphism.

Theorem 67.12. *$\mathrm{Tor}^R(-,B)$ is well-defined up to natural isomorphism.*

Proof. Suppose $\tau_1\colon P_1\to A$ and $\tau_2\colon P_2\to A$ are two semiprojective resolutions of A, suppose $\tau_1'\colon P_1'\to A'$ and $\tau_2'\colon P_2'\to A'$ are two semiprojective resolutions of A', and suppose $\widetilde{\varphi_1}\colon P_1\to P_1'$ is a homotopic lift of $\varphi\tau_1$ with respect to τ_1' and $\widetilde{\varphi_2}\colon P_2\to P_2'$ is a homotopic lift of $\varphi\tau_2$ with respect to τ_2'. So altogether we have the diagrams

$$\begin{tikzcd} P_1 \arrow[r, "\widetilde{\varphi_1}"] \arrow[d, "\tau_1"'] & P_1' \arrow[d, "\tau_1'"] \\ A \arrow[r, "\varphi"'] & A' \end{tikzcd} \qquad \begin{tikzcd} P_2 \arrow[r, "\widetilde{\varphi_2}"] \arrow[d, "\tau_2"'] & P_2' \arrow[d, "\tau_2'"] \\ A \arrow[r, "\varphi"'] & A' \end{tikzcd}$$

which commute up to homotopy.

Choose a homotopic lift $\widetilde{\tau}_1\colon P_1\to P_2$ of τ_1 with respect to τ_2 and choose a homotopic lift $\widetilde{\tau}_1{}'\colon P_1'\to P_2'$ of τ_1' with respect to τ_2'. Then $\widetilde{\tau}_1$ and $\widetilde{\tau}_1{}'$ are both homotopy equivalences by the same argument as in the proof of Theorem (67.10). Now observe that

$$\begin{aligned} \tau_2'\widetilde{\varphi_2}\widetilde{\tau}_1 &\sim \varphi\tau_2\widetilde{\tau}_1 \\ &\sim \varphi\tau_1 \\ &\sim \tau_1'\widetilde{\varphi_1} \\ &\sim \tau_2'\widetilde{\tau}_1{}'\widetilde{\varphi_1}. \end{aligned}$$

In particular, both $\widetilde{\varphi_2}\widetilde{\tau}_1\colon P_1\to P_2'$ and $\widetilde{\tau}_1{}'\widetilde{\varphi_1}\colon P_1\to P_2'$ are homotopic lifts of $\varphi\tau_1$ with respect to τ_2'. Therefore

$$\widetilde{\varphi_2}\widetilde{\tau}_1\sim\widetilde{\tau}_1{}'\widetilde{\varphi_1},$$

and since $-\otimes_R B$ respects homotopies, we have a diagram

$$\begin{tikzcd} P_1\otimes_R B \arrow[r, "\widetilde{\tau}_1\otimes_R B"] \arrow[d, "\widetilde{\varphi_1}\otimes_R B"'] & P_2\otimes_R B \arrow[d, "\widetilde{\varphi_2}\otimes_R B"] \\ P_1'\otimes_R B \arrow[r, "\widetilde{\tau}_1{}'\otimes_R B"] & P_2'\otimes_R B \end{tikzcd}$$

which commutes up to homotopy. Finally, since $\mathrm{H}(-)$ takes homotopic maps to equal maps, we see that the diagram

$$\begin{tikzcd} \mathrm{H}(P_1 \otimes_R B) \arrow[r, "\mathrm{H}(\widetilde{\tau_1} \otimes_R B)"] \arrow[d, "\mathrm{H}(\widetilde{\varphi_1} \otimes_R B)"'] & \mathrm{H}(P_2 \otimes_R B) \arrow[d, "\mathrm{H}(\widetilde{\varphi_2} \otimes_R B)"] \\ \mathrm{H}(P_1' \otimes_R B) \arrow[r, "\mathrm{H}(\widetilde{\tau_1}' \otimes_R B)"] & \mathrm{H}(P_2' \otimes_R B) \end{tikzcd}$$

which is commutative. Since $\mathrm{H}(-)$ takes homotopy equivalences to isomorphisms, we see that the rows are isomorphisms, and thus $\mathrm{H}(\mathrm{Hom}_R^{\star}(-, B))$ is a natural isomorphism.

□

67.8.3 Balance of Tor

Proposition 67.8. *Let A and B be R-complexes and let $\sigma \colon P \to A$ and $\tau \colon Q \to B$ be semiprojective resolutions. Then*

$$\mathrm{Tor}^R(A, B) \cong \mathrm{H}(P \otimes_R Q) \cong \mathrm{H}(A \otimes_R Q).$$

Proof. Observe that $P \otimes_R -$ respects quasiisomorphisms since P is semiprojective (and hence semiflat). Therefore $P \otimes_R \tau \colon P \otimes_R Q \to P \otimes_R B$ is a quasiisomoprhism. Thus

$$\mathrm{H}(P \otimes_R \tau) \colon \mathrm{H}(P \otimes_R Q) \to \mathrm{H}(P \otimes_R B)$$

is an isomorphism. Similarly, $- \otimes_R Q$ respects quasiisomorphisms since Q is semiprojective (and hence semiflat). Therefore $\sigma \otimes_R Q \colon P \otimes_R Q \to A \otimes_R Q$ is a quasiisomorphism. Thus

$$\mathrm{H}(\sigma \otimes_R Q) \colon \mathrm{H}(P \otimes_R Q) \to \mathrm{H}(A \otimes_R Q)$$

is an isomorphism. Therefore we have balance of Tor:

$$\begin{aligned} \mathrm{Tor}^R(A, B) &= \mathrm{H}(P \otimes_R B) \\ &\cong \mathrm{H}(P \otimes_R Q) \\ &\cong \mathrm{H}(A \otimes_R Q). \end{aligned}$$

□

67.8.4 Commutativity of Tor

Proposition 67.9. *Let A and B be R-complexes. Then we have an isomorphism of graded R-modules*

$$\mathrm{Tor}^R(A, B) \cong \mathrm{Tor}^R(B, A),$$

which is natural in A and B.

Proof. Let $\sigma \colon P \to A$ be a semiprojective resolution of A and let $\tau \colon Q \to B$ be a semiprojective resolutions of B. We have

$$\begin{aligned} \mathrm{Tor}^R(A, B) &= \mathrm{H}(P \otimes_R B) \\ &\cong \mathrm{H}(P \otimes_R Q) \\ &\cong \mathrm{H}(Q \otimes_R P) \\ &\cong \mathrm{H}(Q \otimes_R A) \\ &= \mathrm{Tor}^R(B, A). \end{aligned}$$

□

67.8.5 Tor commutes with direct limits

Let $(B_\lambda, \varphi_{\lambda\mu})$ be a directed system of R-complexes and chain maps. We want to show

$$\begin{aligned} \mathrm{Tor}^R(A, \varinjlim B_\lambda) &= \varinjlim \mathrm{Tor}^R(A, B_\lambda) \\ &= \varinjlim \mathrm{H}(A \otimes_R P_\lambda) \\ &= \varinjlim \mathrm{H}(F \otimes_R B_\lambda) \end{aligned}$$

$$\mathrm{Tor}^R(A, \varinjlim B_\lambda) = \varinjlim \mathrm{Tor}^R(A,$$

67.9 Base Change in Tor

Let S be an R-algebra, let M be an R-module and let N be an S-module. Then there exists a natural graded S-module homomorphism

$$\mathrm{Tor}^R(M,N) \to \mathrm{Tor}^S(S\otimes_R M, N).$$

Indeed, let F be an R-projective resolution of M (so in particular we have a surjective quasiisomorphism $\sigma\colon F \xrightarrow{\simeq} M$). Let G be an S-projective resolution of $S\otimes_R M$ (so in particular, we have a surjective quasiisomorphism $\tau\colon G \to S\otimes_R M$). Note that $S\otimes_R F$ is a semiprojective S-complex. Therefore by the homotopy lifting lemma, the chain map $1\otimes\sigma\colon S\otimes_R F \to S\otimes_R M$ lifts to a chain map $\varphi\colon S\otimes_R F\to G$ such that $\tau\varphi = 1\otimes\sigma$. The map φ is unique up to homotopy by the homotopy lifting lemma. Therefore φ induces a canonical map in homology:

$$\begin{aligned}\mathrm{Tor}^R(M,N) &:= \mathrm{H}(F\otimes_R N)\\ &\to \mathrm{H}(S\otimes_R F\otimes_R N)\\ &\to \mathrm{H}(G\otimes_R N)\\ &:= \mathrm{Tor}^S(S\otimes_R M, N).\end{aligned}$$

The map $\mathrm{H}(F\otimes_R N)\to\mathrm{H}(S\otimes_R F\otimes_R N)$ in induced by the map of S-complexes $F\otimes_R N\to S\otimes_R F\otimes_R N$ given by $a\otimes n\mapsto 1\otimes a\otimes n$ for all $a\in F$ and $n\in N$. The map $\mathrm{H}(S\otimes_R F\otimes_R N)\to\mathrm{H}(G\otimes_R N)$ is induced by the map $\varphi\otimes 1$. In homological degree 0, this is none other than the usual base change in tensor products:

$$M\otimes_R N\to S\otimes_R M\otimes_R N$$

given by $m\otimes n\mapsto 1\otimes m\otimes n$ for all $m\in M$ and $n\in N$. Altogether, the map

$$\mathrm{Tor}^R(M,N)\to\mathrm{Tor}^S(S\otimes_R M,N)$$

is induced by the map of S-complexes $F\otimes_R N\to G\otimes_R N$ which is given by $a\otimes n\mapsto\varphi(1\otimes a)\otimes n$.

67.10 Functors from $\mathbf{Comp}_R$ to $\mathbf{HComp}_R$ and $\mathbf{HComp}_R$ to $\mathbf{HComp}_R$

67.10.1 Semiprojective Version

For every R-complex A we fix a semiprojective resolution $\mathrm{P}_R(A)\xrightarrow{\tau_A} A$ and for every chain map $\varphi\colon A\to B$ we fix a homotopic lift $\mathrm{P}_R(\varphi)\colon \mathrm{P}_R(A)\to\mathrm{P}_R(B)$ of $\varphi\tau_A$ with respect to τ_B. If the ring R is clear from context, then we write $\mathrm{P}(A)$ and $\mathrm{P}(\varphi)$ rather than $\mathrm{P}_R(A)$ and $\mathrm{P}_R(\varphi)$ in order to simplify notation.

Proposition 67.10. *We obtain a well-defined R-linear covariant functor $\mathbb{P}\colon \mathbf{Comp}_R\to\mathbf{HComp}_R$ which takes an R-complex A to the R-complex $\mathrm{P}(A)$ and which takes a chain map $\varphi\colon A\to B$ to the homotopy class $[\mathrm{P}(\varphi)]$.*

Proof. The well-definedness comes from the fact that we used fixed resolutions and lifts. The functor $\mathbb{P}$ respects identity maps. Indeed, given the identity morphism $1_A\colon A\to A$, we have $\tau_A 1_{\mathrm{P}(A)} = 1_A\tau_A$. In particular, $1_{\mathrm{P}(A)}$ is a homotopic lift of $1_A\tau_A$ with respect to τ_A. Thus $\mathrm{P}(1_A)\sim 1_{\mathrm{P}(A)}$, and thus $[\mathrm{P}(1_A)] = [1_{\mathrm{P}(A)}]$. The functor $\mathbb{P}$ also respects compositions. Indeed, let $\varphi\colon A\to B$ and $\psi\colon B\to C$ be two chain maps. Then

$$\begin{aligned}\tau_C\mathrm{P}(\psi)\mathrm{P}(\varphi) &\sim \psi\tau_B\mathrm{P}(\varphi)\\ &\sim \psi\varphi\tau_A.\end{aligned}$$

Thus $\mathrm{P}(\psi)\mathrm{P}(\varphi)$ is a homotopic lift of $\psi\varphi\tau_A$ with respect to τ_C. Since $\mathrm{P}(\psi\varphi)$ is also a homotopic lift of $\psi\varphi\tau_A$ with respect to τ_C, it follows that $\mathrm{P}(\psi\varphi)\sim\mathrm{P}(\psi)\mathrm{P}(\varphi)$, and thus $[\mathrm{P}(\psi\varphi)] = [\mathrm{P}(\psi)][\mathrm{P}(\varphi)]$.

Now we show that $\mathbb{P}$ is an R-linear functor. Let A and B be R-complexes. We want to show that if $\varphi,\psi\in\mathcal{C}(A,B)$ and $r,s\in R$ then

$$[\mathrm{P}(r\varphi+s\psi)] = [r\mathrm{P}(\varphi)+s\mathrm{P}(\psi)]. \tag{299}$$

To see this, note that $\mathrm{P}(\varphi)$ is a homotopic lift of $\varphi\tau_A$ with respect to τ_B and $\mathrm{P}(\psi)$ is a homotopic lift of $\psi\tau_A$ with respect to τ_B. Now observe that

$$\begin{aligned}\tau_B(r\mathrm{P}(\varphi)+s\mathrm{P}(\psi)) &= r\tau_B\mathrm{P}(\varphi)+s\tau_B\mathrm{P}(\psi)\\ &\sim r\varphi\tau_A+s\psi\tau_A\\ &= (r\varphi+s\psi)\tau_A.\end{aligned}$$

Thus $r\mathrm{P}(\varphi)+s\mathrm{P}(\psi)$ is a homotopic lift of $(r\varphi+s\psi)\tau_A$ with respect to τ_B. Since $\mathrm{P}(r\varphi+s\psi)$ is another homotopic lift of $(r\varphi+s\psi)\tau_A$ with respect to τ_B, it follows that $\mathrm{P}(r\varphi+s\psi)\sim r\mathrm{P}(\varphi)+s\mathrm{P}(\psi)$. In other words, we have (299). □

Definition 67.13. Define $\Omega_R \colon \mathbf{Comp}_R \to \mathbf{HComp}_R$ to be functor which sends the R-complex A to the R-complex A and which takes a chain map $\varphi \colon A \to B$ to the homotopy class $[\varphi]$.

Remark 122. If the ring R is clear from context, then we write Ω rather than Ω_R in order to simplify notation.

Proposition 67.11. *The functor Ω is a well-defined R-linear covariant functor. Moreover it transforms homotopy equivalences to isomorphisms. Furthermore, Ω satisfies the following universal mapping property: for every R-linear covariant functor $F \colon \mathbf{Comp}_R \to \mathcal{C}$ which takes homotopic maps to equal maps, there exists a unique R-linear functor $\widetilde{F} \colon \mathbf{HComp}_R \to \mathcal{C}$ such that $\widetilde{F}\Omega = F$.*

Proof. The first part of the propositions is straightforward. Let us address the universal mapping property. Given such an $F \colon \mathbf{Comp}_R \to \mathcal{C}$, we define $\widetilde{F} \colon \mathbf{HComp}_R \to \mathcal{C}$ to be the functor which takes an R-complex A to the object $F(A)$ and which takes the homotopy class $[\varphi]$ of a chain map $\varphi \colon A \to B$ to the morphism $F(\varphi) \colon F(A) \to F(B)$. Observe that this is well-defined by assumption of F (it takes homotopic chain maps to equal maps). Let us show that $\widetilde{F}$ is a functor. First we check that it respects identity maps. Let $[1_A]$ be the homotopy class of the identity map $1_A \colon A \to A$. Then

$$\begin{aligned} \widetilde{F}[1_A] &= F(1_A) \\ &= 1_{F(A)}. \end{aligned}$$

Thus $\widetilde{F}$ respects identity maps. Next let's check that it respects compositions. Let $[\varphi]$ and $[\psi]$ be the homotopy classes of the chain maps $\varphi \colon A \to B$ and $\psi \colon B \to C$ respectively. Then

$$\begin{aligned} \widetilde{F}[\psi\varphi] &= F(\psi\varphi) \\ &= F(\psi)F(\varphi) \\ &= \widetilde{F}[\psi]\widetilde{F}[\varphi]. \end{aligned}$$

Thus $\widetilde{F}$ respects compositions. Now let us check that $\widetilde{F}\Omega = F$. For any R-complex A, we have

$$\begin{aligned} \widetilde{F}\Omega(A) &= \widetilde{F}(A) \\ &= F(A) \end{aligned}$$

and for any chain map $\varphi \colon A \to B$, we have

$$\begin{aligned} \widetilde{F}\Omega(\varphi) &= \widetilde{F}[\mathrm{P}(\varphi)] \\ &= F(\varphi). \end{aligned}$$

Therefore $\widetilde{F}\Omega = F$. Finally, note that uniqueness of $\widetilde{F}$ follows from the fact that we were forced to define $\widetilde{F}$ in this way. Indeed, if $\widetilde{F}'$ was another such functor, then for any R-complex A, we have

$$\begin{aligned} \widetilde{F}'(A) &= \widetilde{F}'\Omega(A) \\ &= F(A) \\ &= \widetilde{F}\Omega(A) \\ &= \widetilde{F}(A), \end{aligned}$$

and for any chain map $\varphi \colon A \to B$, we have

$$\begin{aligned} \widetilde{F}'[\varphi] &= \widetilde{F}'\Omega(\varphi) \\ &= F(\varphi) \\ &= \widetilde{F}\Omega(\varphi) \\ &= \widetilde{F}[\varphi]. \end{aligned}$$

□

Remark 123. One should view Ω as some sort of "localization" functor. Indeed, recall that if S is a multilpicatively closed subset of a commutative ring A and $\rho_S \colon A \to A_S$ is the canonical localization map, then the pair (A_S, ρ_S) satisfies the following universal mapping property: for every ring homomorphism $\varphi \colon A \to B$ such that $\varphi(S) \subseteq B^\times$, there exists a unique ring homomorphism $\widetilde{\varphi} \colon A_S \to B$ such that $\widetilde{\varphi}\rho_S = \varphi$.

Theorem 67.13. *Let $\widetilde{\mathbb{P}} \colon \mathbf{HComp}_R \to \mathbf{HComp}_R$ be the functor which takes an R-complex A to the R-complex $\mathrm{P}(A)$ and which takes a homotopy class $[\varphi]$ of the chain map $\varphi \colon A \to B$ to the homotopy class $[\mathrm{P}(\varphi)]$ of the chain map $\mathrm{P}(\varphi) \colon \mathrm{P}(A) \to \mathrm{P}(B)$. Then $\widetilde{\mathbb{P}}$ is a well-defined R-linear functor.*

Proof. Note that $\mathbb{P}$ takes homotopic chain maps to equal maps. Thus we may apply Proposition (67.11) to $\mathbb{P} \colon \mathbf{Comp}_R \to \mathbf{HComp}_R$ (where $\mathcal{C} = \mathbf{HComp}_R$) to get $\widetilde{\mathbb{P}} \colon \mathbf{HComp}_R \to \mathbf{HComp}_R$. □

67.10.2 Semiinjective Version

For every R-complex A we fix a semiinjective resolution $A \xrightarrow{\varepsilon_A} \mathrm{E}_R(A)$ and for every chain map $\varphi\colon A \to B$ we fix a homotopic lift $\mathrm{E}_R(\varphi)\colon \mathrm{E}_R(A) \to \mathrm{E}_R(B)$ of $\varepsilon_B\varphi$ with respect to ε_A. If the ring R is clear from context, then we write $\mathrm{E}(A)$ and $\mathrm{E}(\varphi)$ rather than $\mathrm{E}_R(A)$ and $\mathrm{E}_R(\varphi)$ in order to simplify notation.

Just like in the semiprojective case, we will denote we obtain a well-defined R-linear covariant functor $\mathbb{E}\colon \mathbf{Comp}_R \to \mathbf{HComp}_R$ which takes an R-complex A to the R-complex $\mathrm{E}(A)$ and which takes a chain map $\varphi\colon A \to B$ to to the homotopy class $[\mathrm{E}(\varphi)]$ of the chain map $\mathrm{E}(\varphi)\colon \mathrm{E}(A) \to \mathrm{E}(B)$. Similarly, we obtain a well-defined R-linear covariant functor $\widetilde{\mathbb{E}}\colon \mathbf{HComp}_R \to \mathbf{HComp}_R$ which takes an R-complex A to the R-complex $\mathrm{E}(A)$ and which takes the homotopy class $[\varphi]$ of a chain map $\varphi\colon A \to B$ to the homotopy class $[\mathrm{E}(\varphi)]$ of the chain map $\mathrm{E}(\varphi)\colon \mathrm{E}(A) \to \mathrm{E}(B)$.

67.10.3 Covariant Hom

Theorem 67.14. *Let A be an R-complex. Then the following are well-defined R-linear functors*

1. $\mathbb{H}\mathrm{om}^\star_R(A,-)\colon \mathbf{Comp}_R \to \mathbf{HComp}_R$ *which takes an R-complex B to the R-complex $\mathrm{Hom}^\star_R(A,B)$ and which takes a chain map $\varphi\colon B \to B'$ to the homotopy class $[\mathrm{Hom}^\star_R(A,\varphi)]$ of the chain map $\mathrm{Hom}^\star_R(A,\varphi)\colon \mathrm{Hom}^\star_R(A,B) \to \mathrm{Hom}^\star_R(A,B')$.*

2. $\widetilde{\mathbb{H}\mathrm{om}}^\star_R(A,-)\colon \mathbf{HComp}_R \to \mathbf{HComp}_R$ *which takes an R-complex B to the R-complex $\mathrm{Hom}^\star_R(A,B)$ and which takes a homotopy class $[\varphi]$ of a chain map $\varphi\colon B \to B'$ to the homotopy class $[\mathrm{Hom}^\star_R(A,\varphi)]$ of the chain map $\mathrm{Hom}^\star_R(A,\varphi)\colon \mathrm{Hom}^\star_R(A,B) \to \mathrm{Hom}^\star_R(A,B')$.*

Proof. 1. Observe that $\mathbb{H}\mathrm{om}^\star_R(A,-) = \Omega\mathrm{Hom}^\star_R(A,-)$. The composition of two R-linear covariant functors is a well-defined R-linear covariant functor.

2. Observe that $\mathbb{H}\mathrm{om}^\star_R(A,-)$ takes homotopic maps to equal maps. Indeed, if $\varphi\colon B \to B'$ and $\psi\colon B \to B'$ are two chain maps such that $\varphi \sim \psi$, then $\mathrm{Hom}^\star_R(A,\varphi) \sim \mathrm{Hom}^\star_R(A,\psi)$. Therefore $[\mathrm{Hom}^\star_R(A,\varphi)] = [\mathrm{Hom}^\star_R(A,\psi)]$. Thus we may apply the universal mapping property in Proposition (67.11) to $\mathbb{H}\mathrm{om}^\star_R(A,-)\colon \mathbf{Comp}_R \to \mathbf{HComp}_R$ (where $\mathcal{C} = \mathbf{HComp}_R$) to get $\widetilde{\mathbb{H}\mathrm{om}}^\star_R(A,-)\colon \mathbf{HComp}_R \to \mathbf{HComp}_R$. □

67.10.4 Contravariant Hom

Theorem 67.15. *Let B be an R-complex. Then the following are well-defined R-linear functors*

1. $\mathbb{H}\mathrm{om}^\star_R(-,B)\colon \mathbf{Comp}_R \to \mathbf{HComp}_R$ *which takes an R-complex A to the R-complex $\mathrm{Hom}^\star_R(A,B)$ and which takes a chain map $\varphi\colon A \to A'$ to the homotopy class $[\mathrm{Hom}^\star_R(\varphi,B)]$ of the chain map $\mathrm{Hom}^\star_R(\varphi,B)\colon \mathrm{Hom}^\star_R(A',B) \to \mathrm{Hom}^\star_R(A,B)$.*

2. $\widetilde{\mathbb{H}\mathrm{om}}^\star_R(-,B)\colon \mathbf{HComp}_R \to \mathbf{HComp}_R$ *which takes an R-complex A to the R-complex $\mathrm{Hom}^\star_R(A,B)$ and which takes a homotopy class $[\varphi]$ of a chain map $\varphi\colon A \to A'$ to the homotopy class $[\mathrm{Hom}^\star_R(\varphi,B)]$ of the chain map $\mathrm{Hom}^\star_R(\varphi,B)\colon \mathrm{Hom}^\star_R(A,B) \to \mathrm{Hom}^\star_R(A,B')$.*

Proof. Proof is similar to the proof of Theorem (67.18). □

67.10.5 Tensor Product

Theorem 67.16. *Let A be an R-complex. Then the following are well-defined R-linear functors*

1. $A\underline{\otimes}_R-\colon \mathbf{Comp}_R \to \mathbf{HComp}_R$ *which takes an R-complex B to the R-complex $A \otimes_R B$ and which takes a chain map $\varphi\colon B \to B'$ to the homotopy class $[A \otimes_R \varphi]$ of the chain map $A \otimes_R \varphi\colon A \otimes_R B \to A \otimes_R B'$.*

2. $A\widetilde{\underline{\otimes}}_R-\colon \mathbf{HComp}_R \to \mathbf{HComp}_R$ *which takes an R-complex B to the R-complex $A \otimes_R B$ and which takes the homotopy class $[\varphi]$ of a chain map $\varphi\colon B \to B'$ to the homotopy class $[A \otimes_R \varphi]$ of the chain map $A \otimes_R \varphi\colon A \otimes_R B \to A \otimes_R B'$.*

Theorem 67.17. *Let B be an R-complex. Then the following are well-defined R-linear functors*

1. $-\underline{\otimes}_R B\colon \mathbf{Comp}_R \to \mathbf{HComp}_R$ *which takes an R-complex A to the R-complex $A \otimes_R B$ and which takes a chain map $\varphi\colon A \to A'$ to the homotopy class $[\varphi \otimes_R A]$ of the chain map $\varphi \otimes_R B\colon A \otimes_R B \to A' \otimes_R B$.*

2. $-\widetilde{\underline{\otimes}}_R B\colon \mathbf{HComp}_R \to \mathbf{HComp}_R$ *which takes an R-complex A to the R-complex $A \otimes_R B$ and which takes the homotopy class $[\varphi]$ of a chain map $\varphi\colon A \to A'$ to the homotopy class $[\varphi \otimes_R B]$ of the chain map $\varphi \otimes_R B\colon A \otimes_R B \to A' \otimes_R B$.*

Remark 124. (commutativity) Let A be an R-complex. Then $A\underline{\otimes}_R -$ is naturally isomorphic to $-\underline{\otimes}_R A$. Indeed, we have

$$\begin{aligned} A\underline{\otimes}_R - &= \Omega(A \otimes_R -) \\ &\cong \Omega(- \otimes_R A) \\ &= -\underline{\otimes}_R A, \end{aligned}$$

where the isomorphism at the second line is natural (as shown earlier). Note that this also implies $A\widetilde{\underline{\otimes}}_R -$ is naturally isomorphic to $-\widetilde{\underline{\otimes}}_R A$.

67.10.6 Natural Transformation of Functors

Proposition 67.12. *Let A be an R-complex. The natural chain maps*

$$\mathrm{P}(A) \xrightarrow[\simeq]{\tau_A} A \xrightarrow[\simeq]{\varepsilon_A} \mathrm{E}(A)$$

induce the following natural transformations

1. $\mathbb{P} \xrightarrow{[\tau]} \Omega \xrightarrow{[\varepsilon]} \mathbb{E}$ *of functors from* $\mathbf{Comp}_R$ *to* $\mathbf{HComp}_R$.

2. $\widetilde{\mathbb{P}} \xrightarrow{[\tau]} \mathrm{id} \xrightarrow{[\varepsilon]} \widetilde{\mathbb{E}}$ *of functors from* $\mathbf{HComp}_R$ *to* $\mathbf{HComp}_R$.

Proof. We focus $\Omega \xrightarrow{[\varepsilon]} \mathbb{E}$ and $\mathrm{id} \xrightarrow{[\varepsilon]} \widetilde{\mathbb{E}}$ since the proof that the other maps are natural transformations is a similar argument. We first consider $\Omega \xrightarrow{[\varepsilon]} \mathbb{E}$. We need to check that for every chain map $\varphi\colon A \to B$, the following diagram commutes in $\mathbf{HComp}_R$:

$$\begin{tikzcd} A \arrow[r, "{[\varepsilon_A]}"] \arrow[d, "{[\varphi]}"'] & \mathrm{E}(A) \arrow[d, "{[\mathrm{E}(\varphi)]}"] \\ B \arrow[r, "{[\varepsilon_B]}"'] & \mathrm{E}(B) \end{tikzcd}$$

This is clear however since $\mathrm{E}(\varphi)$ is a homotopic lift of $\varepsilon_B\varphi$ with respect to ε_A. Thus $\varepsilon_B\varphi \sim \mathrm{E}(\varphi)\varepsilon_A$, which implies

$$\begin{aligned} [\varepsilon_B][\varphi] &= [\varepsilon_B\varphi] \\ &= [\mathrm{E}(\varphi)\varepsilon_A] \\ &= [\mathrm{E}(\varphi)][\varepsilon_A]. \end{aligned}$$

Now we consider $\mathrm{id} \xrightarrow{[\varepsilon]} \widetilde{\mathbb{E}}$. We need to check that for every homotopy class $[\varphi]$ of a chain map $\varphi\colon A \to B$, the following diagram commutes in $\mathbf{HComp}_R$:

$$\begin{tikzcd} A \arrow[r, "{[\varepsilon_A]}"] \arrow[d, "{[\varphi]}"'] & \mathrm{E}(A) \arrow[d, "{[\mathrm{E}(\varphi)]}"] \\ B \arrow[r, "{[\varepsilon_B]}"'] & \mathrm{E}(B) \end{tikzcd}$$

This was done above. □

Theorem 67.18. *Let A be an R-complex. Then the following are well-defined R-linear functors*

1. $\mathbb{H}\mathrm{om}^\star_R(A,-)\colon \mathbf{Comp}_R \to \mathbf{HComp}_R$ *which takes an R-complex B to the R-complex* $\mathrm{Hom}^\star_R(A,B)$ *and which takes a chain map $\varphi\colon B \to B'$ to the homotopy class* $[\mathrm{Hom}^\star_R(A,\varphi)]$ *of the chain map* $\mathrm{Hom}^\star_R(A,\varphi)\colon \mathrm{Hom}^\star_R(A,B) \to \mathrm{Hom}^\star_R(A,B')$.

2. $\widetilde{\mathbb{H}}\mathrm{om}^\star_R(A,-)\colon \mathbf{HComp}_R \to \mathbf{HComp}_R$ *which takes an R-complex B to the R-complex* $\mathrm{Hom}^\star_R(A,B)$ *and which takes a homotopy class $[\varphi]$ of a chain map $\varphi\colon B \to B'$ to the homotopy class* $[\mathrm{Hom}^\star_R(A,\varphi)]$ *of the chain map* $\mathrm{Hom}^\star_R(A,\varphi)\colon \mathrm{Hom}^\star_R(A,B) \to \mathrm{Hom}^\star_R(A,B')$.

67.11 Triangulated Categories

Exact sequences are useful for studying modules and complexes, but these are poorly behaved in $\mathbf{HComp}_R$. For instance, the natural chain $0 \xrightarrow{\simeq} \mathcal{K}(1)$ is a quasiisomorphism between semiprojective complexes and so thus must be a homotopy equivalence. Thus $\mathcal{K}(1)$ is isomorphic to 0 in the $\mathbf{HComp}_R$. Now the 0 complex fits into a really silly exact sequence, namely $0 \to 0 \to 0$, but it is not clear whether the sequence $0 \to \mathcal{K}(1) \to 0$ should be exact. To solve this, Grothendieck and Verdier introduced the notion of a **triangulated category**, where instead of considering exact sequences, one considers **distinguished triangles**.

67.11.1 Shift Functors, Triangles, and Morphisms of Triangles

Definition 67.14. Let $\mathcal{C}$ be an R-linear category.

1. A **shift functor** (or **translation functor**) on $\mathcal{C}$ is an R-linear functor $\Sigma\colon \mathcal{C} \to \mathcal{C}$ with a 2-sided inverse $\Sigma^{-1}\colon \mathcal{C} \to \mathcal{C}$. Sometimes ΣA will be denoted $A[1]$. More generally, $\Sigma^n A = A[n]$. Note that $\Sigma^0 = 1_{\mathcal{C}}$.

2. A **triangle** in $\mathcal{C}$ is a diagram in $\mathcal{C}$ of the form

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} \Sigma A \tag{300}$$

   of morphisms in $\mathcal{C}$. Sometimes we call these **pretriangles** or **candidate triangles**. We shall use the shorthand notation $(A, B, C)_{(\alpha,\beta,\gamma)}$ to denote the triangle in (300).

3. A **morphism** of triangles in $\mathcal{C}$ is a commutative diagram in $\mathcal{C}$ of the form

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "f"] & B \arrow[r, "\beta"] \arrow[d, "g"] & C \arrow[r, "\gamma"] \arrow[d, "h"] & \Sigma A \arrow[d, "\Sigma f"] \\ A' \arrow[r, "\alpha'"] & B' \arrow[r, "\beta'"] & C' \arrow[r, "\gamma'"] & \Sigma A' \end{tikzcd} \tag{301}$$

   Such a morphism is called an **isomorphism** if f, g, h are all isomorphisms, that is, the morphism has a 2-sided inverse. We shall use shorthand notation $(f, g, h)\colon (A, B, C)_{(\alpha,\beta,\gamma)} \to (A', B', C')_{(\alpha',\beta',\gamma')}$ to denote the morphism of triangles in (302).

67.11.2 Triangulated Categories

Definition 67.15. A **triangulated R-linear category** is an R-linear category $\mathcal{C}$ equipped with a shift functor Σ and a class of triangles called **distinguished triangles** (or **exact triangles**) such that the following axioms are satisfied.

1. For all objects A in $\mathcal{C}$, the triangle $A \xrightarrow{1_A} A \to 0 \to \Sigma A$ is distinguished.

2. For every morphism $\alpha \colon A \to B$, there exists a distinguished triangle $(A, B, C)_{(\alpha,-,-)}$ (where the $-$ means we aren't specifying that morphism). In this case we call C a **cone of** α (or a **cofiber** of α).

3. Given an isomorphism of triangles $(f, g, h) \colon (A, B, C)_{(\alpha,\beta,\gamma)} \to (A', B', C')_{(\alpha',\beta',\gamma')}$, then $(A, B, C)_{(\alpha,\beta,\gamma)}$ is distinguished if and only if $(A', B', C')_{(\alpha',\beta',\gamma')}$ is distinguished.

4. Given a distinguished triangle $(A, B, C)_{(\alpha,\beta,\gamma)}$, the following **rotated triangles**, $(B, C, \Sigma A)_{(\beta,\gamma,-\Sigma\alpha)}$ and $(\Sigma^{-1}C, A, B)_{(-\Sigma^{-1}\gamma,\alpha,\beta)}$, are both distinguished.

5. Given a diagram in $\mathcal{C}$,

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "f"] & B \arrow[r, "\beta"] \arrow[d, "g"] & C \arrow[r, "\gamma"] \arrow[d, dashed, "h"] & \Sigma A \arrow[d, "\Sigma f"] \\ A' \arrow[r, "\alpha'"] & B' \arrow[r, "\beta'"] & C' \arrow[r, "\gamma'"] & \Sigma A' \end{tikzcd} \tag{302}$$

   where the top and bottom rows are distinguished triangles, then there exists a morphism $h \colon C \to C'$ making diagram commutative.

6. (Octahedral axiom) Start with morphisms $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ in $\mathcal{C}$ and fix distinguished triangles $(A, B, C^\diamond)_{(\alpha,\beta,\gamma_\diamond)}$, $(B, C, A^\diamond)_{(\beta,\gamma^\diamond,\alpha_\diamond)}$, and $(A, C, B^\diamond)_{(\beta\alpha,\widetilde{\beta}_\diamond,\widetilde{\alpha}^\diamond)}$. Then there exists a distinguished triangle $(C^\diamond, B^\diamond, A^\diamond)_{(\widetilde{\beta},\widetilde{\alpha},\widetilde{\gamma})}$ which is compatible with the input data in the following sense

$$\begin{aligned} \gamma^\diamond &= \widetilde{\alpha}\widetilde{\beta}_\diamond \\ \gamma_\diamond &= \widetilde{\alpha}^\diamond\widetilde{\beta} \\ \widetilde{\gamma} &= (\Sigma\beta^\diamond)\alpha_\diamond \\ \alpha_\diamond\widetilde{\alpha} &= (\Sigma\alpha)\widetilde{\alpha}^\diamond \\ \widetilde{\beta}\beta^\diamond &= \widetilde{\beta}_\diamond\beta \end{aligned}$$

   We can visualize this axiom via the following diagram

$$\begin{tikzcd} & & B^\diamond \arrow[ddll] \arrow[drr] & & \\ C^\diamond \arrow[urr] \arrow[d] & & & & A^\diamond \arrow[llll] \arrow[ddll] \\ A \arrow[rrrr, no head] \arrow[drr] & & & & C \arrow[uull] \arrow[u] \\ & & B \arrow[uull] \arrow[urr] & & \end{tikzcd}$$

   Note that the octahedral axiom is very technical, but it can be interpreted in terms of the third isomorphiss theorem, pullbacks, pushouts, fiber products, and fiber coproducts.

67.11.3 Homotopy Category is a Triangulated Category

Theorem 67.19. $\mathbf{HComp}_R$ *is a triangulated R-linear category, where a triangle is distinguished if and only if it is isomorphic to one of the form $(A, B, \mathrm{C}(\varphi))_{([\varphi],[\iota],[\pi])}$, where $\iota \colon B \to \mathrm{C}(\varphi)$ and $\pi \colon \mathrm{C}(\varphi) \to \Sigma A$ are the natural inclusion and projection maps respectively.*

Proof. Partial proof of TR1: The identity triangle $(A, A, 0)_{([1_A],[0],[0])}$ is distinguished since

$$\begin{tikzcd}
A \arrow[r, "{[1_A]}"] \arrow[d, "{[1_A]}"] & A \arrow[r, "{[0]}"] \arrow[d, "{[1_A]}"] & 0 \arrow[r, "{[0]}"] \arrow[d, "{[0]}"] & \Sigma A \arrow[d, "{[0]}"] \\
A \arrow[r, "{[1_A]}"] & A \arrow[r, "{[\iota]}"] & \mathrm{C}(A) \arrow[r, "{[\pi]}"] & \Sigma A
\end{tikzcd}$$

is an isomorphism. The only thing to check is that the middle part of the diagram is commutative, that is $[\iota][1_A] = [0][0]$. This is equivalent to ι being null-homotopic, which is clear. $\square$

68 Special Complexes

There are many special complexes which show up in Mathematics. In this section, we want to discuss some of them.

68.1 Simplicial Complexes

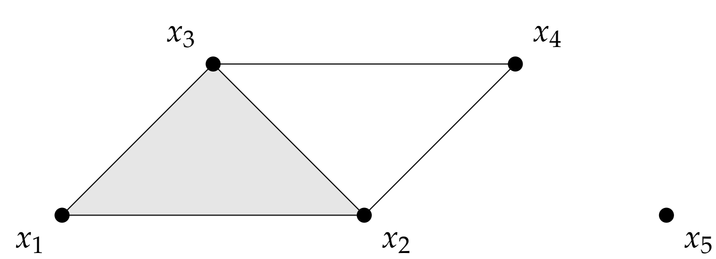
Definition 68.1. An (abstract) **simplicial complex** Δ on the set $\{x_1, \dots, x_n\}$ is a collection of subsets of $\{x_1, \dots, x_n\}$ which is closed under containment: if $\sigma \subseteq \{x_1, \dots, x_n\}$ and $\sigma \supseteq \tau$, then $\tau \in \Delta$. An element of a simplicial complex is called a **face** of Δ. A face of Δ which is not properly contained in another face in Δ is called a **facet** in Δ. A face $\sigma \in \Delta$ of cardinality $i+1$ is called an i**-dimensional face** or an i-face of Δ. For an i-dimensional face $\sigma \in \Delta$, we set

$$\dim \sigma = i = \#\sigma - 1,$$

where $\#\sigma$ denotes the cardinality of σ. The empty set $\emptyset$, is the unique face of dimension -1, as long as Δ is not the **void complex** $\{\}$ consisting of no subsets of $\{x_1, \dots, x_n\}$. The **dimension** of Δ, denoted $\dim \Delta$, is defined to be the maximum of the dimensions of its faces (or $-\infty$ if $\Delta = \{\}$).

The following example will help clarify some of the concepts introduced above.

Example 68.1. The simplicial complex Δ on $\{x_1, x_2, x_3, x_4, x_5\}$ consisting of all subsets of $\{x_1, x_2, x_3\}$, $\{x_2, x_4\}$, $\{x_3, x_4\}$, and $\{x_4\}$ is pictured below:



We often use squarefree monomial notation to denote faces of Δ. Thus, instead of $\{x_2, x_4\}$, we write x_2x_4, similarly instead of $\{x_1, x_2, x_3\}$, we write $x_1x_2x_3$. More generally, if $\sigma = \{x_{i_1}, \dots, x_{i_k} \mid 1 \le i_1 < \cdots < i_k \le n\}$, then the corresponding squarefree monomial is denoted $\boldsymbol{x}^\sigma = x_{i_1} \cdots x_{i_k}$.

68.1.1 Simplicial Homology

Definition 68.2. A **simplicial complex** $\Delta = (\mathcal{V}, \mathcal{F})$ consists of

1. A set $\mathcal{V}$ called the **vertex set** of Δ, whose elements are called **vertices** of Δ;
2. A set $\mathcal{F}$ of finite nonempty subsets of $\mathcal{F}$, whose elements are called **faces** of Δ, such that
   (a) if $v \in \mathcal{V}$, then $\{v\} \in F$;
   (b) if $\sigma \in \mathcal{F}$ and $\tau \subseteq \sigma$, then $\tau \in \mathcal{F}$.

If $\sigma \in \mathcal{F}$ and $\#\sigma = m+1$, then we say σ has **dimension** m and call it an m**-face** of Δ.

Definition 68.3. Let K be a field and let $\Delta = (\mathcal{V}, \mathcal{F})$ be a simplicial complex.. We define a K-complex, denoted $C = C_\Delta$, called the **reduced chain complex of Δ over K**, as follows: the homogeneous component of degree $i \in \mathbb{Z}$ of the underlying graded K-vector space C is given by

$$C_i := \begin{cases} \operatorname{span}_K\{\sigma \in \Delta \mid \dim \sigma = i\} & \text{if } -1 \leq i \leq \dim \Delta \\ 0 & \text{else} \end{cases}$$

and the differential ∂ is defined by $\partial(\emptyset) = 0$ and

$$\partial(\sigma) = \sum_{\lambda \in \sigma} \langle \lambda, \sigma \backslash \lambda \rangle \sigma \backslash \{\lambda\}.$$

for all $\sigma \in \Delta \backslash \{\emptyset\}$. The homology of $\mathcal{S}(\Delta)$ is called the **reduced simplicial homology** of Δ over K, and is commonly denoted as $\widetilde{H}(\Delta, K)$.

Example 68.2. For Δ as in Example (68.1), we have

$$\begin{aligned} S_2(\Delta) &= Kx_1x_2x_3 \\ S_1(\Delta) &= Kx_1x_2 + Kx_1x_3 + Kx_2x_3 + Kx_2x_4 + Kx_3x_4 \\ S_0(\Delta) &= Kx_1 + Kx_2 + Kx_3 + Kx_4 + Kx_5 \\ S_{-1}(\Delta) &= K \end{aligned}$$

Choosing bases for the $S_i(\Delta)$ as suggested by the ordering of the faces listed above, the chain complex for Δ becomes

$$0 \longrightarrow K \xrightarrow{\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}} K^5 \xrightarrow{\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}} K^5 \xrightarrow{\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}} K \longrightarrow 0$$

For example, $\partial_2(e_{\{1,2,3\}}) = e_{\{2,3\}} + e_{\{1,3\}} + e_{\{1,2\}}$, which we identify with the vector $(1,1,1,0,0)$. The mapping ∂_1 has rank 3, so $\widetilde{H}_0(\Delta; K) \cong \widetilde{H}_1(\Delta; K) \cong K$ and the other homology groups are 0. Geometrically, $\widetilde{H}_0(\Delta; K)$ is nontrivial since Δ is disconnected and $\widetilde{H}_1(\Delta; K)$ is nontrivial since Δ contains a triangle which is not the boundary of an element of Δ.

68.2 Monomial Resolution from a Labeled Simplicial Complex

Throughout this subsection, let $\boldsymbol{x} = x_1, \dots, x_n$, let $R = K[\boldsymbol{x}]$, and let $\boldsymbol{m} = m_1, \dots, m_r$ be monomials in R. For each nonempty subset $\sigma \subseteq [r]$, we set $m_\sigma := \operatorname{lcm}(m_\lambda \mid \lambda \in \sigma)$ and we set $\boldsymbol{a}_\sigma \in \mathbb{N}^n$ to be the exponent vector of m_σ. For completeness, we set $m_\emptyset = 1$ and $a_\emptyset = (0, \dots, 0)$. Let Re_σ be the free R-module generated by e_σ whose multidegree is $\boldsymbol{a}_\sigma$. Let Δ be a simplical complex on $[r]$. We label the vertices of Δ by $m_1, \dots, m_r$. More generally, if σ is a face of Δ, then we label it by m_σ. For each $\boldsymbol{a} \in \mathbb{N}^n$, let $\Delta_{\boldsymbol{a}}$ be the subcomplex of Δ defined by $\Delta_{\boldsymbol{a}} = \{\sigma \in \Delta \mid \boldsymbol{a}_\sigma \leq \boldsymbol{a}\}$. The differential on $\mathcal{S}(\Delta)$ is denoted ∂, and the differential on $\mathcal{S}(\Delta_{\boldsymbol{a}})$ is denoted $\partial_{\boldsymbol{a}}$. Note that $\partial_{\boldsymbol{a}}$ is just the restriction of ∂ to $\mathcal{S}(\Delta_{\boldsymbol{a}})$.

Definition 68.4. With the notation above, we define an R-complex, denoted F_Δ and called **R-complex induced by Δ** (or the **R-complex of Δ over R**), as follows: the homogeneous component in degree $i \in \mathbb{Z}$ of the underlying graded R-module of F_Δ is given by

$$F_{\Delta,i} := \begin{cases} \bigoplus_{\dim \sigma = i-1} Re_\sigma & \text{if } 0 \leq i \leq \dim \Delta + 1 \\ 0 & \text{else} \end{cases}$$

and the differential d_Δ is defined by $\mathrm{d}_\Delta(e_\emptyset) = 0$ and

$$\mathrm{d}_\Delta(e_\sigma) = \sum_{\lambda \in \sigma} \langle \lambda, \sigma \backslash \lambda \rangle \frac{m_\sigma}{m_{\sigma \backslash \lambda}} e_{\sigma \backslash \lambda}$$

for all $\sigma \in \Delta \backslash \{\emptyset\}$. In the case where Δ is the r-simplex, we call F_Δ the **Taylor complex** of $R/\boldsymbol{m}$ over R.

Let us check that $\mathrm{d}_\Delta^2 = 0$: it suffices to check this on the generators e_σ for all $\sigma \in \Delta$. If $|\sigma| \le 1$, then we clearly $\mathrm{d}_\Delta^2(e_\sigma) = 0$, thus assume that $|\sigma| > 1$. Then

$$\begin{aligned}
\mathrm{d}_\Delta^2(e_\sigma) &= \mathrm{d}_\Delta \mathrm{d}_\Delta(e_\sigma) \\
&= \mathrm{d}_\Delta\left(\sum_{\lambda\in\sigma} \langle \lambda, \sigma\backslash\lambda\rangle \frac{m_\sigma}{m_{\sigma\backslash\lambda}} e_{\sigma\backslash\lambda}\right) \\
&= \sum_{\lambda\in\sigma} \langle \lambda, \sigma\backslash\lambda\rangle \frac{m_\sigma}{m_{\sigma\backslash\lambda}} \mathrm{d}_\Delta(e_{\sigma\backslash\lambda}) \\
&= \sum_{\lambda\in\sigma} \langle \lambda, \sigma\backslash\lambda\rangle \frac{m_\sigma}{m_{\sigma\backslash\lambda}} \sum_{\mu\in\sigma\backslash\lambda} \langle \mu, \sigma\backslash\{\lambda,\mu\}\rangle \frac{m_{\sigma\backslash\lambda}}{m_{\sigma\backslash\{\lambda,\mu\}}} \mathrm{d}_\Delta(e_{\sigma\backslash\{\lambda,\mu\}}) \\
&= \sum_{\substack{\lambda,\mu\in\sigma \\ \lambda\neq\mu}} \langle \lambda, \sigma\backslash\lambda\rangle \langle \mu, \sigma\backslash\{\lambda,\mu\}\rangle \frac{m_\sigma}{m_{\sigma\backslash\{\lambda,\mu\}}} \mathrm{d}_\Delta(e_{\sigma\backslash\{\lambda,\mu\}}) \\
&= 0,
\end{aligned}$$

where the last part follows from symmetry in μ and λ and

$$\begin{aligned}
\langle \lambda, \sigma\backslash\lambda\rangle \langle \mu, \sigma\backslash\{\lambda,\mu\}\rangle &= \langle \lambda, \sigma\backslash\lambda\rangle \langle \mu, \sigma\backslash\{\lambda,\mu\}\rangle \\
&= \langle \lambda, \sigma\backslash\lambda\rangle \langle \mu, \sigma\backslash\lambda\rangle \langle \mu, \lambda\rangle \\
&= -\langle \lambda, \sigma\backslash\lambda\rangle \langle \lambda, \mu\rangle \langle \mu, \sigma\backslash\lambda\rangle \\
&= -\langle \lambda, \sigma\backslash\{\mu,\lambda\}\rangle \langle \mu, \sigma\backslash\lambda\rangle \\
&= -\langle \mu, \sigma\backslash\mu\rangle \langle \lambda, \sigma\backslash\{\mu,\lambda\}\rangle.
\end{aligned}$$

Observe that F_Δ also has the structure of a $\mathbb{N}^n$-graded K-complex. In other words, we have a decomposition of K-vector spaces

$$F_\Delta = \bigoplus_{\boldsymbol{a}\in\mathbb{N}^n} F_{\Delta,\boldsymbol{a}},$$

where the homogeneous component in multidegree $\boldsymbol{a} \in \mathbb{N}^n$ is given by

$$F_{\Delta,\boldsymbol{a}} = \bigoplus_{m_\sigma | \boldsymbol{x}^{\boldsymbol{a}}} K \frac{\boldsymbol{x}^{\boldsymbol{a}}}{m_\sigma} e_\sigma.$$

Moreover, for each $\boldsymbol{a} \in \mathbb{N}^n$, the differential d_Δ restricts to a differential on $F_{\Delta,\boldsymbol{a}}$ (which we denote by $\mathrm{d}_{\Delta,\boldsymbol{a}}$). Indeed, we have

$$\begin{aligned}
\mathrm{d}_{\Delta,\boldsymbol{a}}\left(\frac{\boldsymbol{x}^{\boldsymbol{a}}}{m_\sigma} e_\sigma\right) &= \frac{\boldsymbol{x}^{\boldsymbol{a}}}{m_\sigma} \mathrm{d}_\Delta(e_\sigma) \\
&= \frac{\boldsymbol{x}^{\boldsymbol{a}}}{m_\sigma} \sum_{\lambda\in\sigma} \langle \lambda, \sigma\backslash\lambda\rangle \frac{m_\sigma}{m_{\sigma\backslash\lambda}} e_{\sigma\backslash\lambda} \\
&= \sum_{\lambda\in\sigma} \langle \lambda, \sigma\backslash\lambda\rangle \frac{\boldsymbol{x}^{\boldsymbol{a}}}{m_\sigma} \frac{m_\sigma}{m_{\sigma\backslash\lambda}} e_{\sigma\backslash\lambda} \\
&= \sum_{\lambda\in\sigma} \langle \lambda, \sigma\backslash\lambda\rangle \frac{\boldsymbol{x}^{\boldsymbol{a}}}{m_{\sigma\backslash\lambda}} e_{\sigma\backslash\lambda} \\
&\in F_{\Delta,\boldsymbol{a}}.
\end{aligned}$$

Thus $F_{\Delta,\boldsymbol{a}}$ has the structure of a K-complex. In fact, letting $\varphi_{\boldsymbol{a}} \colon F_{\Delta,\boldsymbol{a}} \to \mathcal{S}(\Delta_{\boldsymbol{a}})$ be the unique graded K-linear isomorphism such that $\varphi_{\boldsymbol{a}}\left(\frac{\boldsymbol{x}^{\boldsymbol{a}}}{m_\sigma} e_\sigma\right) = \sigma$, then from the computation above, we see that $\mathrm{d}_{\Delta,\boldsymbol{a}} \partial_{\boldsymbol{a}} = \partial_{\boldsymbol{a}} \mathrm{d}_{\Delta,\boldsymbol{a}}$; hence $\varphi_{\boldsymbol{a}}$ is an isomorphism of K-complexes. In particular, we have

$$\begin{aligned}
\mathrm{H}(F_\Delta, \mathrm{d}_\Delta) &= \ker \mathrm{d}_\Delta / \operatorname{im} \mathrm{d}_\Delta \\
&= \left(\bigoplus_{\boldsymbol{a}\in\mathbb{N}^n} \ker \mathrm{d}_{\Delta,\boldsymbol{a}}\right) \Big/ \left(\bigoplus_{\boldsymbol{a}\in\mathbb{N}^n} \operatorname{im} \mathrm{d}_{\Delta,\boldsymbol{a}}\right) \\
&\cong \bigoplus_{\boldsymbol{a}\in\mathbb{N}^n} (\ker \mathrm{d}_{\Delta,\boldsymbol{a}} / \operatorname{im} \mathrm{d}_{\Delta,\boldsymbol{a}}) \\
&= \bigoplus_{\boldsymbol{a}\in\mathbb{N}^n} \mathrm{H}(F_{\Delta,\boldsymbol{a}}, \mathrm{d}_{\Delta,\boldsymbol{a}}) \\
&\cong \bigoplus_{\boldsymbol{a}\in\mathbb{N}^n} \mathrm{H}(\Delta_{\boldsymbol{a}}, K),
\end{aligned}$$

where the last homology is the simplicial homology of the simplicial complex $\Delta_{\boldsymbol{a}}$ over K. From this, we obtain the following theorem:

Theorem 68.1. *F_Δ is a free resolution of $R/\boldsymbol{m}$ over R if and only if the reduced simplicial homology $\widetilde{\mathrm{H}}(\Delta_{\boldsymbol{a}}, K)$ vanishes for all $\boldsymbol{a} \in \mathbb{N}^n$. In particular, the Taylor complex of $R/\boldsymbol{m}$ over R is a free resolution of $R/\boldsymbol{m}$ over R. Moreover, F_Δ is minimal if and only if $m_\sigma \neq m_{\sigma'}$ for every proper subface σ' of a face σ.*

68.2.1 Taylor Complex as a DG Algebra

Proposition 68.1. *Let $I = \langle m_1, \dots, m_r \rangle$ be a monomial ideal in $R = K[x_1, \dots, x_n]$. The Taylor resolution $(\mathcal{T}(\underline{m}), d^{\mathcal{T}(\underline{m})})$ is a DG algebra, with multiplication being uniquely determined on elementary tensors: for $\sigma, \tau \subseteq [n]$, we map $e_\sigma \otimes e_\tau \mapsto e_\sigma e_\tau$, where*

$$e_\sigma e_\tau = \begin{cases} \langle \sigma, \tau \rangle \frac{m_\sigma m_\tau}{m_{\sigma \cup \tau}} e_{\sigma \cup \tau} & \text{if } \sigma \cap \tau = \varnothing \\ 0 & \text{if } \sigma \cap \tau \neq \varnothing \end{cases} \tag{303}$$

Proof. Throughout this proof, denote $d := d^{\mathcal{T}(\underline{m})}$. We first note that $e_\varnothing$ serves as the identity for the multiplication rule (**??**). Indeed, let $\sigma \subseteq [n]$. Then since $\sigma \cap \varnothing = \varnothing$, we have

$$e_\sigma e_\varnothing = e_\sigma = e_\varnothing e_\sigma.$$

Moreover, multiplication by $e_\varnothing$ and e_σ given in (**??**) satisfies Leibniz law:

$$\begin{aligned} d(e_\sigma)e_\varnothing - e_\sigma d(e_\varnothing) &= d(e_\sigma)e_\varnothing \\ &= d(e_\sigma) \\ &= d(e_\sigma e_\varnothing), \end{aligned}$$

and similarly

$$\begin{aligned} d(e_\varnothing)e_\sigma + e_\varnothing d(e_\sigma) &= e_\varnothing d(e_\sigma) \\ &= d(e_\sigma) \\ &= d(e_\varnothing e_\sigma), \end{aligned}$$

Next, let $\lambda \in [n]$. Suppose $\tau \subseteq [n]$ and $\lambda \notin \tau$. Then

$$\begin{aligned} d(e_\lambda)e_\tau - e_\lambda d(e_\tau) &= m_\lambda e_\tau - e_\lambda \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle \frac{m_\tau}{m_{\tau \backslash \mu}} e_{\tau \backslash \mu} \\ &= m_\lambda e_\tau - \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle \frac{m_\tau}{m_{\tau \backslash \mu}} e_\lambda e_{\tau \backslash \mu} \\ &= m_\lambda e_\tau - \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle \langle \lambda, \tau \backslash \mu \rangle \frac{m_\tau}{m_{\tau \backslash \mu}} \frac{m_\lambda m_{\tau \backslash \mu}}{m_{\tau \backslash \mu \cup \lambda}} e_{\tau \backslash \mu \cup \lambda} \\ &= m_\lambda e_\tau - \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle \langle \lambda, \tau \rangle \langle \lambda, \mu \rangle \frac{m_\lambda m_\tau}{m_{\tau \backslash \mu \cup \lambda}} e_{\tau \backslash \mu \cup \lambda} \\ &= m_\lambda e_\tau + \sum_{\mu \in \tau} \langle \lambda, \tau \rangle \langle \mu, \tau \backslash \mu \rangle \langle \mu, \lambda \rangle \frac{m_\lambda m_\tau}{m_{\tau \backslash \mu \cup \lambda}} e_{\tau \backslash \mu \cup \lambda} \\ &= m_\lambda e_\tau + \sum_{\mu \in \tau} \langle \lambda, \tau \rangle \langle \mu, \tau \backslash \mu \cup \lambda \rangle \frac{m_\lambda m_\tau}{m_{\tau \backslash \mu \cup \lambda}} e_{\tau \backslash \mu \cup \lambda} \\ &= \langle \lambda, \tau \rangle \left(\langle \lambda, \tau \rangle m_\lambda e_\tau + \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \cup \lambda \rangle \frac{m_\lambda m_\tau}{m_{\tau \backslash \mu \cup \lambda}} e_{\tau \backslash \mu \cup \lambda} \right) \\ &= \langle \lambda, \tau \rangle \sum_{\mu \in \tau \cup \lambda} \langle \mu, \tau \backslash \mu \cup \lambda \rangle \frac{m_\lambda m_\tau}{m_{\tau \backslash \mu \cup \lambda}} e_{\tau \backslash \mu \cup \lambda} \\ &= \langle \lambda, \tau \rangle \frac{m_\lambda m_\tau}{m_{\tau \cup \lambda}} \sum_{\mu \in \tau \cup \lambda} \langle \mu, \tau \backslash \mu \cup \lambda \rangle \frac{m_{\tau \cup \lambda}}{m_{\tau \backslash \mu \cup \lambda}} e_{\tau \backslash \mu \cup \lambda} \\ &= \langle \lambda, \tau \rangle \frac{m_\lambda m_\tau}{m_{\tau \cup \lambda}} d(e_{\tau \cup \lambda}) \\ &= d(e_\lambda e_\tau), \end{aligned}$$

Next suppose $\tau \subseteq [n]$ and $\lambda \in \tau$. Then

$$\begin{aligned}
d(e_\lambda)e_\tau - e_\lambda d(e_\tau) &= m_\lambda e_\tau - e_\lambda \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle \frac{m_\tau}{m_{\tau \backslash \mu}} e_{\tau \backslash \mu} \\
&= m_\lambda e_\tau - \sum_{\mu \in \tau} \langle \mu, \tau \backslash \mu \rangle \frac{m_\tau}{m_{\tau \backslash \mu}} e_\lambda e_{\tau \backslash \mu} \\
&= m_\lambda e_\tau - \langle \lambda, \tau \backslash \lambda \rangle \langle \lambda, \tau \backslash \lambda \rangle \frac{m_\tau}{m_{\tau \backslash \lambda}} \frac{m_\lambda m_{\tau \backslash \lambda}}{m_\tau} e_\tau \\
&= m_\lambda e_\tau - m_\lambda e_\tau \\
&= 0 \\
&= d(0) \\
&= d(e_\lambda e_\tau).
\end{aligned}$$

Thus we have shown (**??**) satisfies the Leibniz law for all pairs (λ, τ) where $\lambda \in [n]$ and $\tau \subseteq [n]$. We prove by induction on $|\sigma| = i \geq 1$ that (**??**) satisfies the Leibniz law for all pairs (σ, τ) where $\sigma, \tau \subseteq [n]$. The base case $i = 1$ was just shown. Now suppose we have shown (**??**) satisfies the Leibniz law for all pairs (σ, τ) where $\sigma, \tau \subseteq [n]$ such that $|\sigma| = i < n$. Let $\sigma, \tau \subseteq [n]$ such that $|\sigma| = i + 1$. Choose $\lambda \in \sigma$. Then

$$\begin{aligned}
\frac{m_\lambda m_{\sigma \backslash \lambda}}{m_\sigma} d(e_\sigma e_\tau) &= d\left(\frac{m_\lambda m_{\sigma \backslash \lambda}}{m_\sigma} e_\sigma e_\tau \right) \\
&= d(e_\lambda e_{\sigma \backslash \lambda} e_\tau) \\
&= m_\lambda e_{\sigma \backslash \lambda} e_\tau - e_\lambda d(e_{\sigma \backslash \lambda} e_\tau) \\
&= m_\lambda e_{\sigma \backslash \lambda} e_\tau - e_\lambda (d(e_{\sigma \backslash \lambda}) e_\tau + (-1)^{|\sigma|-1} e_{\sigma \backslash \lambda} d(e_\tau)) \\
&= (m_\lambda e_{\sigma \backslash \lambda} - e_\lambda d(e_{\sigma \backslash \lambda})) e_\tau + (-1)^{|\sigma|} \frac{m_\lambda m_{\sigma \backslash \lambda}}{m_\sigma} e_\sigma d(e_\tau) \\
&= d(e_\lambda e_{\sigma \backslash \lambda}) e_\tau + (-1)^{|\sigma|} \frac{m_\lambda m_{\sigma \backslash \lambda}}{m_\sigma} e_\sigma d(e_\tau) \\
&= d\left(\frac{m_\lambda m_{\sigma \backslash \lambda}}{m_\sigma} e_\sigma \right) e_\tau + (-1)^{|\sigma|+1} \frac{m_\lambda m_{\sigma \backslash \lambda}}{m_\sigma} e_\sigma d(e_\tau), \\
&= \frac{m_\lambda m_{\sigma \backslash \lambda}}{m_\sigma} \left(d(e_\sigma) e_\tau + (-1)^{|\sigma|+1} e_\sigma d(e_\tau) \right)
\end{aligned}$$

where we used the base case on the pairs $(e_\lambda, e_{\sigma \backslash \lambda} e_\tau)$[13] and $(e_\lambda, e_{\sigma \backslash \lambda})$ and where we used the induction hypothesis on the pair $(e_{\sigma \backslash \lambda}, e_\tau)$. and where we used the base case on the pair $(e_\lambda, e_{\sigma \backslash \lambda})$. Canceling $\frac{m_\lambda m_{\sigma \backslash \lambda}}{m_\sigma}$ on both sides completes the proof. □

Lemma 68.2. *(DG Algebra Criterion) Let (A, d) be an R-complex such that A is an associative and unital graded R-algebra. Let G be a set of generators for the graded R-algebra A. Suppose the Leibniz law is true for all pairs (a, b) where $a, b \in G$ such that* $\deg(a) = 1$. *Further suppose that each $a \in G$ is divisible by some $a_1 \in G$ such that* $\deg(a_1) = 1$. *Then (A, d) is a DG algebra.*

Proof. It suffices to check that the Leibniz law holds for all pairs (a, b) where $a, b \in G$. Indeed, if $x \in A_k$ and $y \in A_l$ and

$$x = \sum_i r_i a_i \quad \text{and} \quad y = \sum_j s_j b_j,$$

then

$$\begin{aligned}
d(xy) &= d\left(\sum r_i a_i \sum s_j b_j\right) \\
&= \sum \sum r_i s_j d(a_i b_j) \\
&= \sum \sum r_i s_j (d(a_i) b_j + (-1)^{\deg(a_i)} a_i d(b_j)) \\
&= \sum \sum r_i s_j d(a_i) b_j + \sum \sum r_i s_j (-1)^{\deg(a_i)} a_i d(b_j)) \\
&= d\left(\sum r_i a_i\right) \sum s_j b_j + (-1)^{\deg(x)} \sum r_i a_i d\left(\sum s_j b_j\right) \\
&= d(x) y + (-1)^{\deg(x)} x d(y).
\end{aligned}$$

[13] If $e_{\sigma \backslash \lambda} e_\tau = 0$, then obviously Leibniz law holds for the pair $(e_\lambda, e_{\sigma \backslash \lambda} e_\tau)$.

First observe that the Leibniz law is satisfied for all pairs $(1, a)$ where $1 \in A$ is the identity and $a \in A$. Indeed, we have

$$\begin{aligned} d(1)a + 1d(a) &= 0 \cdot a + 1 \cdot d(a) \\ &= d(a) \\ &= d(1 \cdot a). \end{aligned}$$

Similarly, the Leibniz law is satisfied for all pairs $(a, 1)$ where $1 \in A$ is the identity and $a \in A$. Indeed, we have

$$\begin{aligned} d(a) \cdot 1 + (-1)^{\deg(a)} ad(1) &= d(a) + (-1)^{\deg(a)} a \cdot 0 \\ &= d(a) \\ &= d(a \cdot 1). \end{aligned}$$

Now we want to show that the Leibniz law holds for all pairs (a, b) where $a, b \in A$ such that $\deg(a) \geq 1$ by using induction on $\deg(a)$. The base case ($\deg(a) = 1$) is the assumption in the lemma. Now assume that the Leibniz law is satisfied for all pairs (a, b) where $\deg(a) = i \geq 1$. Let $a, b \in A$ such that $\deg(a) = i + 1$. Choose $a_1 \in A_1$ such that $a_1 | a$. Then $a = a_1 a_i$, for some $a_i \in A_i$. Then

$$\begin{aligned} d(ab) &= d(a_1 a_i b) \\ &= d(a_1) a_i b - a_1 d(a_i b) \\ &= d(a_1) a_i b - a_1 (d(a_i) b + (-1)^i a_i d(b)) \\ &= d(a_1) a_i b - a_1 d(a_i) b + (-1)^{i+1} a_1 a_i d(b)) \\ &= (d(a_1) a_i - a_1 d(a_i)) b + (-1)^{i+1} a_1 a_i d(b)) \\ &= d(a_1 a_i)) b + (-1)^{i+1} a_1 a_i d(b)), \\ &= d(a) b + (-1)^{i+1} ad(b). \end{aligned}$$

□

69 Cell Complexes and Cellular Resolutions

A finite regular cell complex $X \subseteq \mathbb{R}^n$ is obtained by starting with a finite set of vertices $X_0 \subseteq \mathbb{R}^n$ and connecting some vertices by curves to get a graph $X_1 \subseteq \mathbb{R}^n$ and then glue some shaded regions nicely to get $X_2 \subseteq \mathbb{R}^n$ then glue some solid regions an dso on until $X_n = X$ for some n.

70 Local Cohomology

Let A be a ring and let J be an ideal in A. We say J is generated **up to radical** by n elements if there exist $x_1, \dots, x_n \in J$ such that $\sqrt{J} = \sqrt{\langle x_1, \dots, x_n \rangle}$ (note that this condition is equivalent to $\dim(J / \langle x_1, \dots, x_n \rangle) = 0$). For example, the ideal $\langle x^2, xy, y^2 \rangle \subseteq K[x, y]$ is generated up to radical by the two elements x^2, y^2 since

$$\sqrt{\langle x^2, xy, y^2 \rangle} = \langle x, y \rangle = \sqrt{\langle x^2, y^2 \rangle}.$$

Given an ideal I, what is the least number of elements needed to generate it up to radical? A particular example of this problem is the follwoing: let $R = K[x, y, u, v]$ be a polynomial ring in four variables over the field K Consider the ideal $I = \langle xu, xv, yu, yv \rangle$. This ideal is its own nilradial, i.e. $I = \sqrt{I}$. The four generators of I are minimal. On the other hand, it can be generated not on the nose, but up to radical, by the three elements $xu, yv, xv + yu$. This holds since

$$(xv)^2 = xv(xv + yu) - (xu)(yv) \in \langle xu, yv, xv + yu \rangle.$$

Are there two elements which generate it up to radical? It turns out that this is not the case. We shall see that local cohomology provides an obstruction to this ideal being generated up to radical by two elements. In particular, to a ring A and ideal J, we'll associate for $i \geq 0$ modules $H^i_J(A)$ with the properties that

1. $H^i_J(A) = H^i_{\sqrt{J}}(A)$,
2. If J is generated by k-elements, then $H^i_J(A) = 0$ for all $i > k$.

Finally, for $I = \langle xu, xv, yu, yv \rangle$, we'll prove that $H^3_I(R) \neq 0$, and therefore I cannot be generated up to radical by two elements.

70.1 Defining $\Gamma_I(M)$

Definition 70.1. Let R be a ring, let $I \subseteq R$ be an ideal, and let M an R-module. We define the I-**torsion submodule** of M to be

$$\Gamma_I(M) = \bigcup_{n \geq 0} (0 :_M I^n) = \{u \in M \mid \text{there exists } n \in \mathbb{N} \text{ such that } I^n u = 0\}.$$

This is also called the submodule of M **supported on** I (an element in $\Gamma_I(M)$ is said to have **support on** I) in the sense that if $\mathfrak{p} \in \mathrm{D}(I)$, then $\Gamma_I(M)_{\mathfrak{p}} = 0$. Indeed, if $u/1 \in \Gamma_I(M)_{\mathfrak{p}}$, then $u \in \Gamma_I(M)$ so there exists an $n \in \mathbb{N}$ such that $I^n u = 0$. Furthermore, we can't have $\mathfrak{p} \supseteq I^n$ (otherwise $\mathfrak{p} \supseteq I$), thus there exists an $x_n \in I^n$ such that $x_n \notin \mathfrak{p}$ and $x_n u = 0$. This implies $u/1 = 0$ in $\Gamma_I(M)_{\mathfrak{p}}$ which implies $\Gamma_I(M)_{\mathfrak{p}} = 0$ since $u/1$ was arbitrary. On the other hand, suppose $\mathfrak{p} \in \mathrm{V}(I) \cap \operatorname{Supp} M$. Thus $\mathfrak{p} \supseteq I$ and $M_{\mathfrak{p}} \neq 0$. Then we have

$$\begin{aligned} \Gamma_I(M)_{\mathfrak{p}} &= \left(\varinjlim \operatorname{Hom}_R(R/I^n, M) \right)_{\mathfrak{p}} \\ &= \bigcup_{n \geq 1} \operatorname{Hom}_R(R/I^n, M)_{\mathfrak{p}} \\ &= \bigcup_{n \geq 1} \operatorname{Hom}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}/I_{\mathfrak{p}}^n, M_{\mathfrak{p}}) \\ &= \Gamma_{I_{\mathfrak{p}}}(M_{\mathfrak{p}}). \end{aligned}$$

Thus we have

$$\begin{aligned} \mathfrak{p} \in \operatorname{Supp}(\Gamma_I(M)) &\iff \Gamma_I(M)_{\mathfrak{p}} \neq 0 \\ &\iff \Gamma_{I_{\mathfrak{p}}}(M_{\mathfrak{p}}) \neq 0 \\ &\iff \operatorname{Hom}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}/I_{\mathfrak{p}}, M_{\mathfrak{p}}) \neq 0 \\ &\iff \operatorname{Hom}_R(R/I, M)_{\mathfrak{p}} \neq 0 \\ &\iff \mathfrak{p} \in \operatorname{Supp}(\operatorname{Hom}_R(R/I, M)) \end{aligned}$$

$\Gamma_{I_{\mathfrak{p}}}(M_{\mathfrak{p}}) \neq 0$ if and only if $0 :_{I_{\mathfrak{p}}} M_{\mathfrak{p}} \neq 0$.

Remark 125. Assume $(R, \mathfrak{m}, \Bbbk)$ is a local noetherian ring. Let $I \subseteq \mathfrak{m}$ be an ideal of R and let M be a nonzero finitely generated R-module. Then we have

$$\begin{aligned} \Gamma_I M \neq 0 &\iff 0 :_{I^n} M \neq 0 \text{ for all } n \in \mathbb{N} \\ &\iff \operatorname{depth}(I^n, M) \neq 0 \text{ for all } n \in \mathbb{N} \\ &\iff \operatorname{depth}(I, M) \neq 0 \\ &\iff 0 :_I M \neq 0 \\ &\iff \operatorname{Hom}_R(R/I, M) \neq 0 \end{aligned}$$

where the third if and only if follows from the fact that $\operatorname{depth}(J, M) = \operatorname{depth}(\sqrt{J}, M)$ for all ideals J of R.

Proposition 70.1. *Let R be a ring, let $I \subseteq R$ be an ideal, and let M an R-module. We have*

$$\operatorname{Supp}(\Gamma_I(M)) = \operatorname{Supp}(\operatorname{Hom}_R(R/I, M)) \subseteq \mathrm{V}(I) \cap \operatorname{Supp} M.$$

Proof. To ease notation in what follows, set $X = \operatorname{Supp}(\Gamma_I(M))$, set $Y = \operatorname{Supp}(M)$, and set $Z = \mathrm{V}(I)$. We are trying to show that $X = Y \cap Z$. Suppose $\mathfrak{p} \in X$ $\square$

Remark 126. Let $J = \sqrt{I}$ denote the radical of I. Since J is finitely generated, there exists some $n \in \mathbb{N}$ such that $J^n \subseteq I$. It follows that $\Gamma_I(M) = \Gamma_J(M)$. Indeed, this follows from the fact that if $I^k u = 0$, then $J^{kn} u = 0$.

1. Since J is finitely generated, there exists some $n \in \mathbb{N}$ such that $J^n \subseteq I$. To see this, suppose $\sqrt{I} = \langle x_1, x_2 \rangle$. Then there exists $n_1, n_2 \in \mathbb{N}$ such that $x_1^{n_1}, x_2^{n_2} \in I$. Let $n = n_1 + n_2$. Then $\sqrt{I}^n \subset I$. To see this, note that $\sqrt{I}$ is generated by the terms $x_1^{m_1} x_2^{m_2}$ where $m_1 + m_2 = n$. By the pigeonhole principle, either $m_1 \geq n_1$ or $n_2 \geq m_2$. In either case, we have $x_1^{m_1} x_2^{m_2} \in I$.

2. Since there exists some $n \in \mathbb{N}$ such that $\sqrt{I}^n \subset I$, we have $\Gamma_I(M) = \Gamma_{\sqrt{I}}(M)$. To see this, suppose $m \in \Gamma_I(M)$. Then there exists $k \in \mathbb{N}$ such that $I^k m = 0$. Since $\sqrt{I}^n \subset I$, this means $\left(\sqrt{I}^n\right)^k m = \sqrt{I}^{nk} = 0$. Therefore $m \in \Gamma_{\sqrt{I}}(M)$. The converse is obvious.

3. Identify $(0 :_M I^n) = \mathrm{Hom}_A(A/I^n, M)$. Then

$$\Gamma_I(M) = \bigcup_{n \geq 0} (0 :_M I^n) = \bigcup_{n \geq 0} \mathrm{Hom}_A(A/I^n, M) = \varinjlim \mathrm{Hom}_A(A/I^n, M).$$

Remark 127. Let $\sqrt{I}$ denote the radical of I.

1. Since $\sqrt{I}$ is finitely generated, there exists some $n \in \mathbb{N}$ such that $\sqrt{I}^n \subset I$. To see this, suppose $\sqrt{I} = \langle x_1, x_2 \rangle$. Then there exists $n_1, n_2 \in \mathbb{N}$ such that $x_1^{n_1}, x_2^{n_2} \in I$. Let $n = n_1 + n_2$. Then $\sqrt{I}^n \subset I$. To see this, note that $\sqrt{I}$ is generated by the terms $x_1^{m_1} x_2^{m_2}$ where $m_1 + m_2 = n$. By the pigeonhole principle, either $m_1 \geq n_1$ or $n_2 \geq m_2$. In either case, we have $x_1^{m_1} x_2^{m_2} \in I$.

2. Since there exists some $n \in \mathbb{N}$ such that $\sqrt{I}^n \subset I$, we have $\Gamma_I(M) = \Gamma_{\sqrt{I}}(M)$. To see this, suppose $m \in \Gamma_I(M)$. Then there exists $k \in \mathbb{N}$ such that $I^k m = 0$. Since $\sqrt{I}^n \subset I$, this means $\left(\sqrt{I}^n\right)^k m = \sqrt{I}^{nk} = 0$. Therefore $m \in \Gamma_{\sqrt{I}}(M)$. The converse is obvious.

3. Identify $(0 :_M I^n) = \mathrm{Hom}_A(A/I^n, M)$. Then

$$\Gamma_I(M) = \bigcup_{n \geq 0} (0 :_M I^n) = \bigcup_{n \geq 0} \mathrm{Hom}_A(A/I^n, M) = \varinjlim \mathrm{Hom}_A(A/I^n, M).$$

Example 70.1. Let $A = K[x, y]$, $I = \langle x, y \rangle$, and $M = K[x, y]/\langle x^3, xy \rangle$. Then $\overline{x} \in \Gamma_I(M)$ since $I^2 \overline{x} = 0$. Thus,

$$K\overline{x} + K\overline{x}^2 = A\overline{x} \subset \Gamma_I(M).$$

To see the reverse inclusion, suppose $m \in \Gamma_I(M)$. Then for some $n \in \mathbb{N}$, we have $I^n m = 0$. Since $m \in M$, we can express it as $m = a_0 + a_1\overline{x} + a_2\overline{x}^2 + a_3\overline{y} + a_4\overline{y}^2 + a_5\overline{y}^3 + \cdots$, where $a_i \in K$. We must have $0 = a_3 = a_4 = a_5 = \cdots$ since no power of y can kill any of the $\overline{y}^k$. Similarly, we must have $a_0 = 0$ since no power of y can kill $\overline{1}$. Therefore $m = a_1\overline{x} + a_2\overline{x}^2$, which implies $A\overline{x} \supset \Gamma_I(M)$. Thus, we have $\Gamma_I(M) = A\overline{x}$. On the other hand, if we set $J = \langle x \rangle$, then we have $\Gamma_I(M) = M$. This is because $J^3 \subset \mathrm{Ann}(M)$.

Let A be a ring, $I_1, I_2 \subset A$ ideals in A. Then for all $n \in \mathbb{N}$, we have

$$\begin{aligned} 0 :_{A/I_1} I_2^n &= \{\overline{a} \in A/I_1 \mid I_2^n \overline{a} = 0\} \\ &= \{\overline{a} \in A/I_1 \mid I_2^n a \in I_1\} \\ &= (I_1 :_A I_2^n)/I_1. \end{aligned}$$

Therefore $\Gamma_{I_2}(A/I_1) = (I_1 :_A I_2^\infty)/I_1$. Now assume A is Noetherian. Then since

$$J : I \subset J : I^2 \subset J : I^3 \subset \cdots,$$

forms an ascending chain of ideals. There exists an s such that $J : I^s = J : I^{s+i}$ for all $i \geq 0$. The minimal such s is called the **saturation exponent**.

We briefly recall the geometric interpretation of the ideal quotient and the saturation. In a Noetherian ring, each radical ideal I_1 has a prime decomposition $I_1 = \bigcap_{i=1}^r \mathfrak{p}_i$. This implies

$$\begin{aligned}
\mathbf{V}(I_1 : I_2) &= \mathbf{V}\left(\left(\bigcap_{i=1}^r \mathfrak{p}_i\right) : I_2\right) \\
&= \mathbf{V}\left(\bigcap_{i=1}^r (\mathfrak{p}_i : I_2)\right) \\
&= \mathbf{V}\left(\bigcap_{I_2 \not\subset \mathfrak{p}_i} \mathfrak{p}_i\right) \\
&= \bigcup_{\mathbf{V}(\mathfrak{p}_i) \not\subset \mathbf{V}(I_2)} \mathbf{V}(\mathfrak{p}_i).
\end{aligned}$$

In other words, if I_1 is a radical ideal, then $\mathbf{V}(I_1 : I_2)$ is the Zariski closure of $\mathbf{V}(I_1) \backslash \mathbf{V}(I_2)$. More generally, if I_1 is not radical, then one can easily show that $\mathbf{V}(I_1 : I_2^\infty)$ is the Zariski closure of $\mathbf{V}(I_1) \backslash \mathbf{V}(I_2)$. Indeed, since A is Noetherian, we have $I_1 : I_2^\infty = I_1 : I_2^s$, where s is the saturation exponent. Express $\sqrt{I_1}$ in terms of its prime decomposition $\sqrt{I_1} = \bigcap_{i=1}^r \mathfrak{p}_i$. Then

$$\begin{aligned}
\mathbf{V}(I_1 : I_2^s) &= \mathbf{V}\left(\sqrt{I_1 : I_2^s}\right) \\
&= \mathbf{V}\left(\sqrt{I_1} : I_2\right) \\
&= \bigcup_{\mathbf{V}(\mathfrak{p}_i) \not\subset \mathbf{V}(I_2)} \mathbf{V}(\mathfrak{p}_i).
\end{aligned}$$

Proposition 70.2. *Let A be a ring, $I \subset A$ an ideal, and let Γ_I be the functor from the category of A-modules to itself, given by mapping an A-module M to the A-module $\Gamma_I(M)$. Then Γ_I is a left-exact covariant functor.*

Proof. It is clear that Γ_I is covariant. Let

$$0 \longrightarrow M_1 \xrightarrow{\varphi_1} M_2 \longrightarrow M_3 \xrightarrow{\varphi_2} 0$$

be a short exact sequence of A-modules. Then we are to show that

$$0 \longrightarrow \Gamma_I(M_1) \xrightarrow{\varphi_1} \Gamma_I(M_2) \xrightarrow{\varphi_2} \Gamma_I(M_3)$$

is exact. Let $x \in \Gamma_I(M_2)$ such that $\varphi_2(x) = 0$. Then there exists an $n \in \mathbb{N}$ such that $I^n x = 0$ and there exists $y \in M_1$ such that $\varphi_1(y) = x$. Then $I^n y = 0$ since

$$\begin{aligned}
\varphi_1(I^n y) &= I^n \varphi_1(y) \\
&= I^n x \\
&= 0,
\end{aligned}$$

and φ_1 is injective. Thus, we have exactness at $\Gamma_I(M_2)$. Now suppose $x \in \Gamma_I(M_1)$ such that $\varphi_1(x) = 0$. Then since φ_1 is injective, we have $x = 0$. Therefore we have exactness at $\Gamma_I(M_1)$. $\square$

Since the category of A-modules has enough injectives, we may define the **right derived functors** of the left-exact covariant functor Γ_I as follows: Let M be an A-module and let

$$0 \longrightarrow M \longrightarrow E^0 \longrightarrow E^1 \longrightarrow E^2 \longrightarrow \cdots$$

be an injective resolution of M. Then we define $H_I^i(M)$ to be the ith homology in the sequence given by

$$0 \longrightarrow \Gamma_I(E^0) \longrightarrow \Gamma_I(E^1) \longrightarrow \Gamma_I(E^2) \longrightarrow \cdots$$

Since Γ_I is left-exact, we have $H_I^0(M) = \Gamma_I(M)$. We call these **local cohomology modules**.

Remark 128.

1. An elementary, but important, property of local cohomology modules is that every element in $H^i_I(M)$ is killed by a power of I. This follows at once from the definition.

2. We often refer to the local cohomology modules as the local cohomology of M with support in I. This is an abuse of notation, but the justification is the following: the functor $\Gamma_I(M)$ identifies a submodule of M whose elements are supported on the closed set $\mathbf{V}(I) \subseteq \mathrm{Spec}(A)$. This means that if $\mathfrak{p} \in \mathrm{Spec}(A)$ and $\mathfrak{p}$ does not contain I, then $(\Gamma_I(M))_{\mathfrak{p}} = 0$. This holds since the elements in $\Gamma_I(M)$ are killed by powers of I, so that if we invert some element of I, they must become 0.

Proposition 70.3. *Let F^i and G^i be two cohomology functors which induce functorial long exact sequences given a short exact sequence of modules, which agree for $i = 0$, and such that $F^i(E) = G^i(E) = 0$ for all $i > 0$ whenever E is injective. Then we have $F^i(M) \cong G^i(M)$ functorially for all i.*

Proof. We will only sketch the proof here. The proof is by induction on i. Suppose we have proved it for $i > 0$. Let $M_0 = M$. From the short exact sequence

$$0 \longrightarrow M_0 \longrightarrow E_0 \longrightarrow M_1 \longrightarrow 0$$

we easily obtain

$$F^{i+1}(M_0) \cong F^i(M_1) \cong G^i(M_1) \cong G^{i+1}(M_0).$$

And so we have proved it for $i+1$. □

70.2 Koszul Complex

Let R be a ring and let $\boldsymbol{r} = r_1, \dots, r_m$ be a sequence of elements in R. The Koszul algebra $\mathbb{K} = \mathbb{K}^R(\boldsymbol{r})$ is defined to be the R-complex whose underlying graded R-module is given by

$$\mathbb{K} = \bigoplus_{\sigma \subseteq \{1,\dots,m\}} e_\sigma R,$$

where we use the notation $e_\sigma = \prod_{i \in \sigma} e_i$ and where e_σ is homogeneous with $|e_\sigma| = \#\sigma$. The differential d of $\mathbb{K}$ is defined on the homogeneous basis by $\mathrm{d}e_i = r_i$ and extended everywhere else using the Leibniz law. In particular, we have

$$\mathrm{d}e_\sigma = \sum_{i \in \sigma} (-1)^{\mathrm{pos}(i,\sigma)} r_i e_{\sigma \setminus i}.$$

For example, if $m = 3$ then we have

$$\begin{array}{llll} & \mathrm{d}e_1 = r_1 & \mathrm{d}e_{23} = e_3 r_2 - e_2 r_3 & \\ \mathrm{d}(1) = 0 & \mathrm{d}e_2 = r_2 & \mathrm{d}e_{13} = e_3 r_1 - e_1 r_3 & \mathrm{d}e_{123} = e_{23} r_1 - e_{13} r_2 + e_{12} r_3 \\ & \mathrm{d}e_3 = r_3 & \mathrm{d}e_{12} = e_2 r_1 - e_1 r_2 & \end{array}$$

An alternative description of $\mathbb{K}$ is the the iterated tensor product of complexes:

$$\mathbb{K}(\boldsymbol{r}) \simeq \mathbb{K}(r_1) \otimes_R \mathbb{K}(r_2) \otimes_R \cdots \otimes_R \mathbb{K}(r_m).$$

If M is an R-module, then we set $\mathbb{K}(\boldsymbol{r}, M) := \mathbb{K} \otimes_R M$ and we denote its homology by $\mathrm{H}(\boldsymbol{r}, M)$.

Another Koszul complex we are interested in is called the **dual Koszul complex**: it is given by $\mathbb{K}^\star := \mathrm{Hom}^\star_R(\mathbb{K}, R)$. The underlying graded R-module is given by

$$\mathbb{K}^\star = \bigoplus_{\sigma \subseteq \{1,\dots,m\}} R e^\star_\sigma.$$

Here $e^\star_\sigma \colon \mathbb{K} \to R$ is an R-linear map, graded of degree $-(\#\sigma)$, which is defined by

$$e^\star_\sigma(e_\tau) = \begin{cases} 1 & \text{if } \sigma = \tau \\ 0 & \text{else} \end{cases}$$

The differential $\mathrm{d}^\star$ of $\mathbb{K}^\star$ is defined by $\mathrm{d}^\star e^\star_\sigma = -(-1)^{\#\sigma} e^\star_\sigma \mathrm{d}$. In particular, we have

$$\mathrm{d}^\star e^\star_\sigma = (-1)^{\#\sigma+1} \sum_{i \in \sigma^\star} (-1)^{\mathrm{pos}(i,\sigma^\star)} r_i e^\star_{\sigma \cup i},$$

where $\sigma^\star := \{1,\dots,m\}\backslash\sigma$. For example, if $m=3$ then we have

$$
\begin{array}{llll}
 & \mathrm{d}^\star e_1^\star = r_3 e_{13}^\star + r_2 e_{12}^\star & \mathrm{d}^\star e_{23}^\star = r_1 e_{123}^\star & \\
\mathrm{d}^\star(1) = -r_1 e_1^\star - r_2 e_2^\star - r_3 e_3^\star & \mathrm{d}^\star e_2^\star = r_3 e_{23}^\star - r_1 e_{12}^\star & \mathrm{d}^\star e_{13}^\star = -r_2 e_{123}^\star & \mathrm{d}^\star e_{123}^\star = 0 \\
 & \mathrm{d}^\star e_3^\star = -r_2 e_{23}^\star - r_1 e_{13}^\star & \mathrm{d}^\star e_{12}^\star = r_3 e_{123}^\star &
\end{array}
$$

Note that the nonzero components of $\mathbb{K}^\star$ live in negative homological degree, that is, if $0<k<m$, then $\mathbb{K}_k^\star = 0$ and $\mathbb{K}_{-k}^\star \neq 0$. We often think of $\mathbb{K}^\star$ as a cochain complex using the upper sign convention $\mathbb{K}_{-k}^\star = \mathbb{K}^{\star,k}$ and $\mathrm{d}_{-k}^\star = \mathrm{d}^{\star,k}$. Note that the map $\varphi\colon \Sigma^n\mathbb{K}^\star \to \mathbb{K}$ defined by

$$\varphi(e_\sigma^\star) = \mathrm{sign}(\sigma^\star,\sigma)e_{\sigma^\star}$$

is an isomorphism of R-complexes. In particular we obtain $\mathrm{H}_i(\mathbb{K}) \simeq \mathrm{H}_{i-m}(\mathbb{K}^\star)$.

The **stable Koszul complex** $\widetilde{\mathbb{K}}$ is complex whose underlying graded R-module is given by

$$\widetilde{\mathbb{K}} = \bigoplus_{\sigma\subseteq\{1,\dots,m\}} \widetilde{e}_\sigma R_{r_\sigma}$$

For example, if $m=3$ then we have

$$
\begin{array}{llll}
 & \widetilde{\mathrm{d}}\widetilde{e}_1 = \widetilde{e}_{13} - \widetilde{e}_{12} & \widetilde{\mathrm{d}}\widetilde{e}_{23} = \widetilde{e}_{123} & \\
\widetilde{\mathrm{d}}(1) = \widetilde{e}_1 + \widetilde{e}_2 + \widetilde{e}_3 & \widetilde{\mathrm{d}}\widetilde{e}_2 = \widetilde{e}_{23} - \widetilde{e}_{12} & \widetilde{\mathrm{d}}e_{13} = -\widetilde{e}_{123} & \widetilde{\mathrm{d}}\widetilde{e}_{123} = 0 \\
 & \widetilde{\mathrm{d}}\widetilde{e}_3 = \widetilde{e}_{23} - \widetilde{e}_{13} & \widetilde{\mathrm{d}}\widetilde{e}_{12} = \widetilde{e}_{123} &
\end{array}
$$

Note that $\widetilde{\mathbb{K}} = \varinjlim \mathbb{K}^\star(\boldsymbol{r}^n)$, where $\boldsymbol{r}^n = r_1^n,\dots,r_m^n$. In particular, since taking filtered colimits is exact, we have

$$\mathrm{H}(\boldsymbol{r}^\infty, M) := \bigcup_{n\geq 0}\mathrm{H}(\boldsymbol{r}^n, M) = \varinjlim \mathrm{H}(\boldsymbol{r}^n, M).$$

Example 70.2. Let $X\subset \mathbb{A}^4$ be the variety defined by the equation $x_1x_4 = x_2x_3$ and let A be the coordinate ring of X, so

$$A := \Bbbk[x_1,x_2,x_3,x_4]/\langle x_1x_4 - x_2x_3\rangle.$$

The function x_1/x_2 is defined on $\mathrm{D}(x_2)$ and the function x_3/x_4 is defined on $\mathrm{D}(x_4)$. By the equation of X, these two functions coincide where they are both defined; in other word $x_1/x_2 = x_3/x_4$ on $\mathrm{D}(x_2x_4) = \mathrm{D}(x_2)\cap\mathrm{D}(x_4)$. So this gives rise to a regular function on $\mathrm{D}(x_2)\cup\mathrm{D}(x_4)$. But there is no representation of this function as a quotient of two polynomials in $\Bbbk[x_1,x_2,x_3,x_4]$ that works on all of $\mathrm{D}(x_2)\cup\mathrm{D}(x_4)$. This gives rise to a nontrivial element in $\mathrm{H}^1_{\langle x_2,x_4\rangle}(A)$. To see this, let's write down the stable Koszul complex:

$$0 \longrightarrow A \xrightarrow{\begin{pmatrix}1 & 1\end{pmatrix}} \begin{matrix}A_{x_2}\\ \oplus \\ A_{x_4}\end{matrix} \xrightarrow{\begin{pmatrix}1\\ -1\end{pmatrix}} A_{x_2x_4} \longrightarrow 0$$

The condition that $x_1/x_2 = x_3/x_4$ on $\mathrm{D}(x_2x_4)$ is equivalent to the condition that $(x_1/x_2, x_3/x_4)$ belongs to the kernel of the map from $A_{x_2}\oplus A_{x_4}$ to $A_{x_2x_4}$. The condition that there is no representation of this function as a quotient of two polynomials in $\Bbbk[x_1,x_2,x_3,x_4]$ that works on all of $\mathrm{D}(x_2)\cup\mathrm{D}(x_4)$ implies $(x_1/x_2, x_3/x_4)$ is not in the image of the map from A to $A_{x_2}\oplus A_{x_4}$. This means that $(x_1/x_2, x_3/x_4)$ represents a nontrivial element in $\mathrm{H}^1_{\langle x_2,x_4\rangle}(A)$.

Proposition 70.4. *Let A be a commutative Noetherian ring, I an ideal, and M an A-module. Suppose that $\sqrt{I} = \sqrt{\langle x_1,\dots,x_n\rangle}$. Then for all i,*

$$H_I^i(M) \cong H^i(\underline{x}^\infty; M),$$

and this isomorphism is functorial.

Proof. Since local cohomology depends on I only up to radical, without loss of generality, I can be assumed to be generated by the x_i. The Koszul cohomology does induce functorial long exact sequences given a short exact sequence of modules. We prove that $H^0(\underline{x}^\infty; M) = H_I^0(M)$. By definition, $H^0(\underline{x}^\infty; M)$ is the homology of the sequence

$$0 \longrightarrow M \longrightarrow M_{x_1}\oplus\cdots\oplus M_{x_n}.$$

An element $y \in M$ goes to zero if and only if it goes to zero in each localization, if and only if for each i there is an integer n_i such that $yx_i^{n_i} = 0$, if and only if there is an N such that $yI^N = 0$, if and only if $y \in H_I^0(M)$. To finish the proof, one needs to prove that $H^i(\underline{x}^\infty; E) = 0$ for all injective A-modules E, and for all $i > 0$. This follows because, as we shall see in the next section, on each indecomposable summand of E, each x_i acts either nilpotently or as a unit. This is easily seen to force the higher cohomology to be zero. $\square$

Proposition 70.5. *Let A be a Noetherian ring, I an ideal and M an A-module. Let $\varphi : A \to B$ be a homomorphism and let N be a B-module.*

1. *If φ is flat, then $H_I^j(M) \otimes_A B \cong H_{IB}^j(M \otimes_A B)$. In particular, local cohomology commutes with localization and completion.*

2. *(Independence of Base) $H_I^j(N) \cong H_{IB}^j(N)$, where the first local cohomology is computed over the base ring A.*

Proof.

1. Choose generators $x_1, \dots, x_n$ of I. The first claim follows at once from the fact that $K^\bullet(x_1, \dots, x_n; M) \otimes_A B = K^\bullet(\varphi(x_1), \dots, \varphi(x_n); M \otimes_A B)$, and that B is flat over A, so that the cohomology of $K^\bullet(x_1, \dots, x_n; M) \otimes_A B$ is the cohomology of $K^\bullet(x_1, \dots, x_n; M)$ tensored over A with B.

2. This follows from the fact that

$$\begin{aligned} K^\bullet(x_1, \dots, x_n; N) &= K^\bullet(x_1, \dots, x_n; A) \otimes_A N \\ &= K^\bullet(x_1, \dots, x_n; A) \otimes_A (B \otimes_B N) \\ &= (K^\bullet(x_1, \dots, x_n; A) \otimes_A B) \otimes_B N \\ &= K^\bullet(\varphi(x_1), \dots, \varphi(x_n); B) \otimes_A N \\ &= K^\bullet(\varphi(x_1), \dots, \varphi(x_n); N). \end{aligned}$$

$\square$

Proposition 70.6. *Let $(A, \mathfrak{m}, k, E)$ be a Noetherian local ring of dimension d, and let M be a finitely generated A-module. For all $i \geq 0$, we have*

$$H_{\mathfrak{m}}^i(M) \cong H_{\widehat{\mathfrak{m}}}^i\left(\widehat{M}\right).$$

Proof. We have

$$\begin{aligned} H_{\widehat{\mathfrak{m}}}^i\left(\widehat{M}\right) &\cong H_{\mathfrak{m} \otimes_A \widehat{A}}^i\left(\widehat{M}\right) \\ &\cong H_{\mathfrak{m}\widehat{A}}^i\left(M \otimes_A \widehat{A}\right) && (\widehat{A} \text{ is flat}) \\ &\cong H_{\mathfrak{m}}^i(M) \otimes_A \widehat{A} && (\widehat{A} \text{ is flat}) \\ &\cong \left(\varinjlim \operatorname{Ext}_A^i(A/\mathfrak{m}^n, M)\right) \otimes_A \widehat{A} \\ &\cong \varinjlim \left(\operatorname{Ext}_A^i(A/\mathfrak{m}^n, M) \otimes_A \widehat{A}\right) && \text{(tensor commutes with direct limits)} \\ &\cong \varinjlim \left(\operatorname{Ext}_A^i(A/\mathfrak{m}^n, M)\right) && \text{(ext modules are killed by a power of the maximal ideal)} \\ &\cong H_{\mathfrak{m}}^i(M). \end{aligned}$$

where the second to last isomorphism following as these Ext modules are killed by a power of the maximal ideal. $\square$

71 Free Resolutions and Fitting Invariants

71.1 Rank

Let R be a commutative ring. The **total quotient ring** $Q(R)$ of R is defined to be the localization of R with respect to the set of all nonzerodivisors, that is, $Q(R) := R_S$ where

$$S := R \setminus \left(\bigcup_{\mathfrak{p} \in \operatorname{WeakAss} R} \mathfrak{p} \right).$$

If R is noetherian, then the set of all zerodivisors of R is equal to the union of all associated primes of R.

Note that if $\mathfrak{p} \in \operatorname{Ass} R$, then $D \subseteq R \backslash \mathfrak{p}$ implies $Q(R)_{\mathfrak{p}Q(R)} \cong R_{\mathfrak{p}}$. The prime ideal of $Q(R)$ correspond to the prime ideals of R which are disjoint form D, that is, they are the prime ideals which only consist of nonzerodivisors. In particular, since R is Noetherian, we see that $Q(R)$ has only finitely many prime ideals.

Example 71.1. Let $R = \Bbbk[x,y]/\langle x^2, xy \rangle$. Then $\operatorname{Ass} R = \{\langle x \rangle, \langle x,y \rangle\}$. Therefore the set of all nonzerodivisors of R is given by $S = R \backslash \langle x,y \rangle$ and thus

$$Q(R) = \Bbbk[x,y]_{\langle x,y \rangle} / \langle x^2, xy \rangle.$$

Example 71.2. Let $R = \Bbbk[x,y]/I$ where $I = \langle x^2 - xy, xy^2 - xy \rangle$. A primary decomposition of I is given by $I = I_1 \cap I_2 \cap I_3$ where

$$\begin{aligned} I_1 &= \langle x \rangle & \sqrt{I_1} &= \langle x \rangle \\ I_2 &= \langle x^2, y \rangle & \sqrt{I_2} &= \langle x, y \rangle \\ I_3 &= \langle x-1, y-1 \rangle & \sqrt{I_3} &= \langle x-1, y-1 \rangle. \end{aligned}$$

Then $\operatorname{Ass} R = \{\langle x \rangle, \langle x,y \rangle, \langle x-1, y-1 \rangle\}$. Therefore the set of all nonzerodivisors of R is given by $S = R \backslash (\langle x,y \rangle \cup \langle x-1, y-1 \rangle)$ and thus

$$Q(R) = \Bbbk[x,y]_{\langle x,y \rangle} / \langle x^2, xy \rangle \oplus \Bbbk[x,y]_{\langle x-1, y-1 \rangle}.$$

Definition 71.1. Let M be a finitely generated R-module. We say that M has **rank** r if $M \otimes_R Q(R)$ is a free $Q(R)$-module of rank r. In this case, we denote the rank of M by $\operatorname{rank} M$.

Note that if R is an integral domain, then $Q(R) = K$ is a field (in fact, it is the field of fractions of R), hence in this case every finitely generated R-module M has a rank, namely

$$\operatorname{rank} M = \dim_K (M \otimes_R K).$$

Lemma 71.1. *Let M be a finitely generated R-module. Then M has rank r if and only if $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module of rank r for all prime ideals $\mathfrak{p} \in \operatorname{Ass} R$.*

Proof. Since $(M \otimes_A Q(A))_{\mathfrak{p}Q(A)} \cong M_{\mathfrak{p}}$ and $Q(A)_{\mathfrak{p}Q(A)} \cong A_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Ass}(A)$, we may assume that $A = Q(A)$. If M is a free A-module of rank r, then $M_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank r. Now suppose that $M_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank r for all prime ideals $\mathfrak{p} \in \operatorname{Ass}(A)$. If $r = 0$, then $M_{\mathfrak{p}} = \langle 0 \rangle$ for all $\mathfrak{p} \in \operatorname{Ass}(A)$, which implies $M = \langle 0 \rangle$. Therefore, we may assume $r > 0$. Choose $x \in M$ such that $x \notin \mathfrak{p}M_{\mathfrak{p}}$ for all $\mathfrak{p}$. Now x is an element of a minimal system of generators of $M_{\mathfrak{p}}$ for all $\mathfrak{p}$. Using Nakayama's Lemma, we obtain that x is an element of a basis of the free module $M_{\mathfrak{p}}$ for all $\mathfrak{p}$. This implies that $M_{\mathfrak{p}}/xA_{\mathfrak{p}} \cong (M/xA)_{\mathfrak{p}}$ is free of rank $r-1$ for all $\mathfrak{p}$. Using induction we may assume that M/xA is free of rank $r-1$. This implies $M \cong xA \oplus M/xA$ is free of rank r. $\square$

Lemma 71.2. *Let A be a Noetherian ring and M be a finitely generated A-module with a finite free presentation*

$$F_1 \xrightarrow{\varphi} F_0 \longrightarrow M \longrightarrow 0.$$

Then M has rank r if and only if $\operatorname{rank}(\operatorname{Im}(\varphi)) = \operatorname{rank}(F_0) - r$.

Proof. First assume M has rank r. Let $\mathfrak{p} \in \operatorname{Ass}(A)$. We have to show that $\operatorname{Im}(\varphi)_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module and $\operatorname{rank}(\operatorname{Im}(\varphi)_{\mathfrak{p}}) = \operatorname{rank}(F_0)_{\mathfrak{p}} - r$. Consider the exact sequence

$$0 \longrightarrow \operatorname{Im}(\varphi)_{\mathfrak{p}} \longrightarrow (F_0)_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow 0. \tag{304}$$

If $M_{\mathfrak{p}}$ is free, then $\operatorname{Im}(\varphi)_{\mathfrak{p}}$ must be free too. The converse is true too, since if $\mathfrak{p} \in \operatorname{Ass}(A)$, we can tensor (305) with $K := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ to get another exact sequence of K-vector spaces. Then $\operatorname{rank}(\operatorname{Im}(\varphi)_{\mathfrak{p}}) = \operatorname{rank}(F_0)_{\mathfrak{p}} - r$ follows from additivity of dimension and Nakayamma's Lemma.

$$0 \longrightarrow \operatorname{Im}(\varphi)_{\mathfrak{p}}/\mathfrak{p}\operatorname{Im}(\varphi)_{\mathfrak{p}} \longrightarrow (F_0)_{\mathfrak{p}}/(\mathfrak{p}F_0)_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \longrightarrow 0. \tag{305}$$

The converse is also true.

$\square$

Proposition 71.1. *Let A be a Noetherian ring and let*

$$0 \longrightarrow U \longrightarrow M \longrightarrow N \longrightarrow 0$$

be an exact sequence of finitely generated A-modules. If two of U, M, N have a rank, then so does the third, and $\operatorname{rank}(M) = \operatorname{rank}(U) + \operatorname{rank}(N)$.

Proof. In view of Lemma (71.2), we may assume that A is local and of depth 0. Then two of U, M, N are free. In each case, we get an isomorphism $M \cong U \oplus N$. $\square$

72 Fitting Ideals

Let $k \in \mathbb{Z}$ and let $\varphi\colon F \to G$ be a map of free R-modules. For $k \geq 1$, we set $I_k(\varphi)$ to be the image of the map

$$\wedge^k F \otimes \wedge^k G^* \to R \tag{306}$$

induced by $\wedge^k \varphi\colon \wedge^k F \to \wedge^k G$. We also make the convention that if $k \leq 0$, then we set $I_k(\varphi) = R$. To see what this image looks like, suppose $\beta = \{\beta_1, \dots, \beta_m\}$ is a basis for F and $\gamma = \{\gamma_1, \dots, \gamma_n\}$ is a basis for G and assume $1 \leq k \leq m \leq n$. Then

$$\wedge^k \beta \otimes \wedge^k \gamma^* := \{(\beta_{i_1} \wedge \cdots \wedge \beta_{i_k}) \otimes (\gamma^*_{j_1} \wedge \cdots \wedge \gamma^*_{j_k}) \mid 1 \leq i_1 \leq \cdots \leq i_k \leq m \text{ and } 1 \leq j_1 \leq \cdots \leq j_k \leq m\}$$

is a basis for the free R-module $\wedge^k F \otimes \wedge^k G^*$. In particular, to better understand $I_k(\varphi)$, it suffices to describe the images of the basis elements in $\wedge^k \beta \otimes (\wedge^k \gamma)^*$ under the map (306). For each $1 \leq i \leq m$ and $1 \leq j \leq n$ there exists unique $a_{ji} \in R$ such that

$$\varphi(\beta_i) = \sum_{j=1}^n a_{ji}\gamma_j.$$

Thus the matrix representation of φ with respect to β and γ is given by

$$[\varphi] = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}.$$

Given $1 \leq i_1 \leq \cdots \leq i_k \leq m$ and $1 \leq j_1 \leq \cdots \leq j_k \leq n$, we have

$$\begin{aligned}
(\beta_{i_1} \wedge \cdots \wedge \beta_{i_k}) \otimes (\gamma^*_{j_1} \wedge \cdots \wedge \gamma^*_{j_k}) &\mapsto (\varphi(\beta_{i_1}) \wedge \cdots \wedge \varphi(\beta_{i_k})) \otimes (\gamma^*_{j_1} \wedge \cdots \wedge \gamma^*_{j_k}) \\
&= \left(\left(\sum_{j=1}^n a_{ji_1}\gamma_j \right) \wedge \cdots \wedge \left(\sum_{j=1}^n a_{ji_k}\gamma_j \right) \right) \otimes (\gamma^*_{j_1} \wedge \cdots \wedge \gamma^*_{j_k}) \\
&= \left(\sum_{1 \leq j'_1 < \cdots < j'_k \leq n} \left(\sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) a_{j'_1 i_{\sigma(1)}} \cdots a_{j'_k i_{\sigma(k)}} \right) (\gamma_{j'_1} \wedge \cdots \wedge \gamma_{j'_k}) \right) \otimes (\gamma^*_{j_1} \wedge \cdots \wedge \gamma^*_{j_k}) \\
&= \left(\sum_{1 \leq j'_1 < \cdots < j'_k \leq n} \det([\varphi]_{\{j'_1,\dots,j'_k\},\{i_1,\dots,i_k\}})(\gamma_{j'_1} \wedge \cdots \wedge \gamma_{j'_k}) \right) \otimes (\gamma^*_{j_1} \wedge \cdots \wedge \gamma^*_{j_k}) \\
&\mapsto \det([\varphi]_{\{j_1,\dots,j_k\},\{i_1,\dots,i_k\}}),
\end{aligned}$$

where $[\varphi]_{\{j_1,\dots,j_k\},\{i_1,\dots,i_k\}}$ is the $k \times k$ submatrix of $[\varphi]$ whose rows correspond to the $j_1, \dots, j_k$ rows of $[\varphi]$ and whose columns correspond to the $i_1, \dots, i_k$ columns of $[\varphi]$. In particular, we see that $I_k(\varphi)$ is generated by the size k minors of $[\varphi]$. Note that if $m \geq n$, then $I_k(\varphi)$ would still be generated by the size k minors of $[\varphi]$ as long as $1 \leq k \leq n$. However if $k \leq 0$, then we set $I_k(\varphi) = R$, and if $k > \min(m, n)$, then we have $I_k(\varphi) = 0$. With these conventions in mind, notice that

$$I_k(\varphi) \supseteq I_{k+1}(\varphi)$$

for each $k \in \mathbb{Z}$. Indeed, the determinant of a $(k+1)$-minor of $[\varphi]$ can be calculated using determinants of k-minors of $[\varphi]$.

Example 72.1. Consider the case where $m = 4$ and $n = 3$, so the matrix representation of $\varphi\colon F \to G$ looks like this:

$$[\varphi] = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix}$$

Then we have

$$\begin{aligned}
&\vdots \\
I_{-1}(\varphi) &= R \\
I_0(\varphi) &= R \\
I_1(\varphi) &= \langle a_{11}, a_{12}, a_{13}, a_{14}, a_{21}, a_{22}, a_{23}, a_{24}, a_{31}, a_{32}, a_{33}, a_{34} \rangle \\
I_2(\varphi) &= \langle a_{11}a_{22} - a_{12}a_{21}, a_{11}a_{32} - a_{12}a_{31}, a_{21}a_{32} - a_{22}a_{31}, a_{11}a_{23} - a_{13}a_{21}, \dots \rangle \\
I_3(\varphi) &= \langle a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} - a_{12}a_{21}a_{33} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}, \dots \rangle \\
I_4(\varphi) &= 0 \\
I_5(\varphi) &= 0 \\
&\vdots
\end{aligned}$$

These ideal of minors turn out to define invariants of a module that generalize the usual invariants for finitely generated abelian groups:

Lemma 72.1. *(Fitting's Lemma) Let M be a finitely generated R-module and let*

$$F \xrightarrow{\varphi} G \to M \to 0 \quad \text{and} \quad F' \xrightarrow{\varphi'} G' \to M \to 0$$

be two presentations of M, with G and G' having ranks n and n' respectively. Then for each $0 \leq i < \infty$, we have $I_{n-i}(\varphi) = I_{n'-i}(\varphi')$. We define the ith ***Fitting invariant*** *of M to be the ideal*

$$\mathrm{Fitt}_i^R(M) := I_{n-i}(\varphi) = I_{n'-i}(\varphi').$$

We extend this defintion by setting $\mathrm{Fitt}_i^R(M) = 0$ if $i < 0$. If the base ring R is understood from context, then we just write $\mathrm{Fitt}_i(M)$ instead of $\mathrm{Fitt}_i^R(M)$. We often simplify notation even further by writing $\mathrm{F}_i(M)$ instead of $\mathrm{Fitt}_i(M)$.

Proof. We omit the immediate reduction to the case where F and F' are finitely generated which is the only case we shall be concerned with. Two ideals are equal if and only if they are equal in every localization of R, so we may harmlessly assume that R is local, and we must show that the Fitting ideals coming from a given presentation of M are the same as the ones coming from the minimal presentation. If φ is the map giving the minimal presentation, then any other presentation ψ may be put in the form

$$[\psi] = \begin{pmatrix} [\varphi] & 0 & 0 \\ 0 & 1_p & 0 \end{pmatrix}$$

where 1_p is a $p \times p$ identity matrix. We must show that $I_j(\varphi) = I_{j+p}(\psi)$. Any nonzero minor m of $[\psi]$ of size $j+p$ is made by taking, for some j', p' with $j' + p' = j + p$, a $j' \times j'$ minor m$'$ of $[\varphi]$ and a $p' \times p'$ minor of 1_p, and multiplying them. Since we must have $p' \leq p$, it follows that $j' \geq j$, and $\mathrm{m} = \mathrm{m}'$. Thus

$$\begin{aligned} I_{j+p}(\psi) &= \sum_{j \leq j' \leq j+p} I_{j'}(\varphi) \\ &= I_j(\varphi) \end{aligned}$$

where the equality on the right follows from the fact that $I_{j'}(\varphi) \subseteq I_j(\varphi)$ for all $j' \geq j$, we are done. □

Let's go over several examples to get a feel of what these fitting invariants look like:

Lemma 72.2. *(Fitting's Lemma) Let M be a finitely generated R-module and let*

$$F \xrightarrow{\varphi} G \to M \to 0 \quad \text{and} \quad F' \xrightarrow{\varphi'} G' \to M \to 0$$

be two presentations of M, with G and G' having ranks n and n' respectively. Then for each $0 \leq i < \infty$, we have $I_{n-i}(\varphi) = I_{n'-i}(\varphi')$. We define the ith ***Fitting invariant*** *of M to be the ideal*

$$\mathrm{Fitt}_i^R(M) := I_{n-i}(\varphi) = I_{n'-i}(\varphi').$$

We extend this defintion by setting $\mathrm{Fitt}_i^R(M) = 0$ if $i < 0$. If the base ring R is understood from context, then we just write $\mathrm{Fitt}_i(M)$ instead of $\mathrm{Fitt}_i^R(M)$. We often simplify notation even further by writing $\mathrm{F}_i(M)$ instead of $\mathrm{Fitt}_i(M)$.

Example 72.2. Suppose M has presentation matrix is $A = \left(\begin{smallmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{smallmatrix}\right)$. Then we have

$$\begin{aligned} &\mathrm{F}_0(M) = \langle \det \varphi \rangle = \langle a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} + \cdots + a_{13}a_{22}a_{31} \rangle \\ &\mathrm{F}_1(M) = \langle \{\text{entries of adj}\, \varphi\} \rangle = \langle a_{11}a_{22} - a_{12}a_{21}, a_{11}a_{32} - a_{12}a_{31}, \dots, a_{22}a_{33} - a_{23}a_{32} \rangle \\ &\mathrm{F}_2(M) = \langle \{\text{entries of } \varphi\} \rangle = \langle a_{11}, a_{12}, \dots, a_{33} \rangle \\ &\mathrm{F}_3(M) = R \end{aligned}$$

Example 72.3. Let $R = \Bbbk[x, y, z, w]$ and let M be an R-module with presentation matrix $A = \left(\begin{smallmatrix} x & y & z \\ 0 & z & w \\ y & z & 0 \end{smallmatrix}\right)$. Then we have

$$\begin{aligned} \mathrm{F}_0(M) &= \langle (y^2 - xz)w - yz^2 \rangle \\ \mathrm{F}_1(M) &= \langle xz, xw, yz, zw, yw, z^2, y^2 - xz \rangle \\ \mathrm{F}_1(M) &= \langle x, y, z, w \rangle \\ \mathrm{F}_2(M) &= R. \end{aligned}$$

Example 72.4. Suppose $R = K[x,y,z,w]$ and suppose M has presentation matrix $A = \left(\begin{smallmatrix} x & y & z \\ y & z & w \end{smallmatrix}\right)$ (so this presentation of M looks like $R^3 \xrightarrow{A} R^2 \to M$). Then we have

$$\begin{aligned} \mathrm{F}_0^R(M) &= \langle xz - y^2, xw - yz, yw - z^2 \rangle \\ \mathrm{F}_1^R(M) &= \langle x, y, z, w \rangle \\ \mathrm{F}_2^R(M) &= R. \end{aligned}$$

Next let $S = R/\mathrm{F}_0(M)$ and let $N = M \otimes_R S \simeq M/\mathrm{F}_0(M)M$. Then N has presentation matrix $\left(\begin{smallmatrix} \overline{x} & \overline{y} & \overline{z} \\ \overline{y} & \overline{z} & \overline{w} \end{smallmatrix}\right)$, and we have

$$\begin{aligned} \mathrm{F}_0^S(M) &= 0 \\ \mathrm{F}_1^S(M) &= \langle \overline{x}, \overline{y}, \overline{z}, \overline{w} \rangle \\ \mathrm{F}_2^S(M) &= S \end{aligned}$$

Example 72.5. Suppose $R = K[x,y,z,w]$ and suppose M has presentation matrix $\varphi = \left(\begin{smallmatrix} x & y \\ y & z \\ z & w \end{smallmatrix}\right)$ (so this presentation of M looks like $R^2 \xrightarrow{\varphi} R^3 \to M$). Then we have

$$\begin{aligned} \mathrm{F}_0(M) &= 0 \\ \mathrm{F}_1(M) &= \langle xz - y^2, xw - yz, yw - z^2 \rangle \\ \mathrm{F}_2(M) &= \langle x, y, z, w \rangle \\ \mathrm{F}_3(M) &= R \end{aligned}$$

Things get a little more interesting in the local situation as the following example shows:

Example 72.6. Suppose $R = \mathbb{Q}[x,y,z]_{\langle x,y,z \rangle}$ and suppose M has the following presentation

$$R^2 \xrightarrow{\begin{pmatrix} 0 & y \\ xy-1 & xz \\ xy+1 & xz \end{pmatrix}} R^3 \longrightarrow M \longrightarrow 0.$$

Using this presentation of M, we calculate

$$\begin{aligned} \mathrm{F}_0(M) &= 0 \\ \mathrm{F}_1(M) &= \langle y - xy^2, y + xy^2, xz \rangle = \langle y, xz \rangle \\ \mathrm{F}_2(M) &= \langle y, xz, xy - 1, xy + 1 \rangle = R \end{aligned}$$

Let's find a smaller presentation of M and use it to calculate the Fitting invariants of M: since $xy - 1$ is a unit in R, we can perform the following sequence of elementary row and column operations to φ:

$$\begin{pmatrix} 0 & y \\ xy-1 & xz \\ xy+1 & xz \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & y \\ xy-1 & xz \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & y \\ xy-1 & 0 \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & y \\ 1 & 0 \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix} \to \begin{pmatrix} y & 0 \\ \frac{-2xz}{xy-1} & 0 \\ 0 & 1 \end{pmatrix} := \begin{pmatrix} \psi & 0 \\ 0 & 1 \end{pmatrix}$$

where we set $\psi = \left(\begin{smallmatrix} y \\ \frac{-2xz}{xy-1} \end{smallmatrix}\right)$. These correspond to the following change of ordered bases of R^3 and R^2:

$$(e_1, e_2, e_3) \to (e_1, e_3, (xy-1)e_2 + (xy+1)e_3) = (\widetilde{e}_1, \widetilde{e}_2) \qquad \text{and} \qquad (e_1, e_2) \to (\frac{-xz}{xy-1}e_1 + e_2, e_1) = (\widetilde{e}_1, \widetilde{e}_2).$$

In particular, we obtain another presentation of M:

$$R^2 \xrightarrow{\begin{pmatrix} \psi & 0 \\ 0 & 1 \end{pmatrix}} R^3 \longrightarrow M \longrightarrow 0.$$

The entry 1 in the presentation gives us a trivial relation, so we prune it to obtain the following minimal presentation of M:

$$R \xrightarrow{\psi} R^2 \longrightarrow M \longrightarrow 0$$

Using this minimal presentation of M, we calculate

$$\begin{aligned}
\mathrm{F}_0(M) &= 0 \\
\mathrm{F}_1(M) &= \langle y, -2xz/(xy-1)\rangle = \langle y, xz\rangle \\
\mathrm{F}_2(M) &= R.
\end{aligned}$$

Thus we obtain the same ideals.

Finally, we consider the following silly example:

Example 72.7. Suppose $R = K[x]$ and suppose M has presentation matrix $\varphi = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ (so this presentation of M looks like $R^2 \xrightarrow{\varphi} R^2 \to M$). Then it's easy to see that M is free of rank 2 (that is, $M \cong R^2$), and we calculate

$$\begin{aligned}
\mathrm{F}_0(M) &= 0 \\
\mathrm{F}_1(M) &= 0 \\
\mathrm{F}_2(M) &= R
\end{aligned}$$

Fitting ideals are also functorial:

Corollary 69. *The formation of Fitting ideals commutes with "base change"; that is, for any map of rings $R \to S$ we have*

$$\mathrm{F}_i^S(M \otimes_R S) = \mathrm{F}_i^R(M)S.$$

In particular, if $\mathfrak{p}$ is a prime ideal of R, then we have

$$\mathrm{F}_i^{R_\mathfrak{p}}(M_\mathfrak{p}) = (\mathrm{F}_i^R(M))_\mathfrak{p}.$$

Proof. Suppose $F \xrightarrow{\varphi} G \to M \to 0$ is a presentation of M with $\mathrm{rank}_R(G) = n$. Then it follows by right-exactness of $- \otimes_R S$ that $F \otimes_R S \xrightarrow{\varphi \otimes 1_S} G \otimes_R S \to M \otimes_R S$ is a presentation of $M \otimes_R S$ with $\mathrm{rank}_S(G \otimes_R S) = n$. Thus

$$\begin{aligned}
\mathrm{F}_i^S(M \otimes_R S) &= I_{n-k}(\varphi \otimes 1_S) \\
&= I_{n-k}(\varphi)S \\
&= \mathrm{F}_k^R(M)S.
\end{aligned}$$

□

Theorem 72.3. *Let A be a local ring and M be an A-module of finite presentation. The following conditions are equivalent:*

1. *M is a free module of rank r;*
2. *$F_r(M) = A$ and $F_{r-1}(M) = 0$.*

Proof. If M is a free module of rank r, then a presentation matrix of M is the $1 \times r$ matrix with entries zero. This gives us $F_r(M) = A$ and $F_{r-1}(M) = 0$. To prove (2) implies (1), let $F_r(M) = A$ and $F_{r-1}(M) = 0$, and choose a presentation

$$A^m \xrightarrow{\varphi} A^n \longrightarrow M \longrightarrow 0$$

with presentation matrix S. Then either $n = r$ and S is the zero matrix, or $n > r$, one $(n-r)$-minor of S is a unit and all $(n-r+1)$-minors of S vanish. If $n = r$ and S is the zero matrix, then, obviously M is free of rank r. In the second case, one $(n-r)$-minor is a unit (in a local ring, if an ideal is generated by non-units, then the ideal must be contained in the maximal ideal), so we can choose new bases of A^m and A^n such that the presentation matrix is of type $\left(\begin{smallmatrix} E_{n-r} & 0 \\ 0 & C \end{smallmatrix}\right)$, where E_{n-r} is the $(n-r)$-unit matrix. Because all $(n-r+1)$-minors are zero, we obtain, indeed, $C = 0$. This implies that M is free and isomorphic to the submodule of A^n generated by the vectors $e_{n-r+1}, \dots, e_n$. □

Corollary 70. *Let A be a ring and M an A-module of finite presentation. Then the following conditions are equivalent.*

1. *M is locally free of constant rank r;*
2. *$F_r(M) = A$ and $F_{r-1}(M) = 0$.*

Proof. For (1) implies (2), let $\mathfrak{p}$ be a prime ideal in A. Since $M_\mathfrak{p}$ is free of rank r, we have $A_\mathfrak{p} = F_r^{A_\mathfrak{p}}(M_\mathfrak{p}) = F_r^A(M)_\mathfrak{p}$ and $0 = F_{r-1}^{A_\mathfrak{p}}(M_\mathfrak{p}) = F_{r-1}^A(M)_\mathfrak{p}$. Since $\mathfrak{p}$ is arbitrary, this implies $F_r(M) = A$ and $F_{r-1}(M) = 0$. For (2) implies (1), we simply go backwards: Let $\mathfrak{p}$ be a prime ideal in A. Since $A = F_r(M)$ and $0 = F_{r-1}(M)$, we must have $A_\mathfrak{p} = F_r^A(M)_\mathfrak{p} = F_r^{A_\mathfrak{p}}(M_\mathfrak{p})$ and $0 = F_{r-1}^A(M)_\mathfrak{p} = F_{r-1}^{A_\mathfrak{p}}(M_\mathfrak{p})$. This implies $M_\mathfrak{p}$ is free. □

Corollary 71. *Let $\varphi : A^m \to A^n$ be a homomorphism, and let S be a matrix representation of φ with respect to some bases of A^m and A^n. Then φ is surjective if and only if there exists an n-minor of S which is a unit in A.*

Proof. $\mathrm{Coker}(\varphi)$ has finite presentation

$$A^m \xrightarrow{\varphi} A^n \longrightarrow \mathrm{Coker}(\varphi) \longrightarrow 0$$

If there exists an n-minor of S which is a unit in A, then $F_0(\mathrm{Coker}(\varphi)) = A$, and hence $\mathrm{Coker}(\varphi)$ is free of rank 0. This implies $A^m \cong A^n$. Conversely, if φ is surjective, then $\mathrm{Coker}(\varphi) \cong 0$ is free of rank 0, so $F_0(\mathrm{Coker}(\varphi)) = A$, which implies there exists an n-minor of S which is a unit in A. □

Corollary 72. *Let A be a Noetherian ring and M an A-module of finite presentation. Then the following conditions are equivalent.*

1. *M has rank r.*
2. *$F_r(M)_{\mathfrak{p}} = A_{\mathfrak{p}}$ and $F_{r-1}(M)_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in \mathrm{Ass}(A)$.*

Remark 129. Note that we have $F_r(M)_{\mathfrak{p}} = A_{\mathfrak{p}}$ whenever there exists an $(n-r)$-minor of S which does not belong to $\mathfrak{p}$.

72.1 Fitting Invariants of Resolution

Let $(R, \mathfrak{m}, \mathbb{k})$ be a local noetherian ring, let M be a finitely generated R-module, and let F be a free resolution of M over R, which we assume to be finite. Let $e_1, \dots, e_N$ be an ordered homogeneous basis of F as a graded R-module. Let $F^\star = \mathrm{Hom}_R^\star(F, R)$ and let $\varepsilon_1, \dots, \varepsilon_N$ denote the dual basis. The differential $\mathrm{d}\colon F \to F$ induces a map

$$\begin{array}{ccc} \mathrm{S}_k^k(F) \otimes_R \mathrm{S}_{k-1}^0(F^\star) & \longrightarrow & R \\ e^{\alpha} \otimes \varepsilon^{\beta} & \mapsto & \varepsilon^{\beta}(\mathrm{d}e)^{\alpha} \end{array}$$

We define $I_k(\mathrm{d}_1)$ to be the image of this map. More generally for $i \geq 2$, the differential $\mathrm{d}\colon F \to F$ induces a map

$$\begin{array}{ccc} \mathrm{S}_{ik}^k(F_{\leq i}) \otimes_R \mathrm{S}_{ik-1}^k(F_{\leq i}^\star) & \longrightarrow & R \\ e^{\alpha} \otimes \varepsilon^{\beta} & \mapsto & \varepsilon^{\beta}(\mathrm{d}e)^{\alpha} \end{array}$$

We define $I_k(\mathrm{d}_i)$ to be the image of this map. More generally for $i \geq 2$, the differential $\mathrm{d}\colon F \to F$ induces a map

$$\begin{array}{ccc} \mathrm{S}_i^m(F) \otimes_R \left(\mathrm{S}_{i-1}^m(F^\star) \oplus \mathrm{S}_{i-1}^{m-1}(F^\star)\right) & \longrightarrow & R \\ e^{\alpha} \otimes (\varepsilon^{\beta} + \varepsilon^{\gamma}) & \mapsto & \varepsilon^{\beta}(\mathrm{d}e)^{\alpha} + \varepsilon^{\gamma}(\mathrm{d}e)^{\alpha} \end{array}$$

We define $I_i^m(\mathrm{d})$ to be the image of this map.

Remark 130. When $i = m$, we recover the usual Fitting ideals $I_m(\mathrm{d}_1)$ of M where we view $\mathrm{d}_1\colon F_1 \to F_0$ as a presentation matrix for M. These ought to be invariants of M, and indeed they are! To see this,

72.2 What Makes a Complex Exact?

Theorem 72.4. *Let F be a finite R-complex such that each F_i is free. Then F is exact if and only if*

$$\mathrm{rank}\, F_i = \mathrm{rank}\, \mathrm{d}_i + \mathrm{rank}\, \mathrm{d}_{i+1} \quad \textit{and} \quad \mathrm{depth}(I(\mathrm{d}_i)) \geq i$$

for all i.

73 Some Category Theory

73.1 Preadditive and Additive Categories

73.1.1 Preadditive Categories

Definition 73.1. A category $\mathcal{A}$ is called **preadditive** if each morphism set $\mathrm{Mor}_{\mathcal{A}}(x, y)$ is endowed with the structure of an abelian group such that the compositions

$$\mathrm{Mor}(y, z) \times \mathrm{Mor}(x, y) \to \mathrm{Mor}(x, z)$$

are bilinear. A functor $F\colon \mathcal{A} \to \mathcal{B}$ of preadditive categories is called **additive** if and only if

$$F\colon \mathrm{Mor}(x, y) \to \mathrm{Mor}(F(x), F(y))$$

is a homomorphism of abelian groups for all $x, y \in \mathrm{Ob}(\mathcal{A})$.

Remark 131. In particular for every x, y there exists at least one morphism $x \to y$, namely the zero map.

Lemma 73.1. *Let $\mathcal{A}$ be a preadditive category. Let x be an object of $\mathcal{A}$. The following are equivalent:*

1. *x is an initial object;*
2. *x is a final object;*
3. $\mathrm{id}_x = 0$ *in* $\mathrm{Mor}(x, x)$.

Definition 73.2. In a preadditive category $\mathcal{A}$, we call **zero object**, and denote it by 0 any final and initial object as in the Lemma above.

Lemma 73.2. *Let $\mathcal{A}$ be a preadditive category and let $x, y \in \mathrm{Ob}(\mathcal{A})$. If the product $x \times y$ exists, then so does the coproduct $x \amalg y$. If the coproduct $x \amalg y$ exists, then so does the product $x \times y$. In this case also $x \amalg y \cong x \times y$.*

Proof. Suppose that $z = x \times y$ with projections $p\colon z \to x$ and $q\colon z \to y$. Denote $i\colon x \to z$ the morphism corresponding to $(1, 0)$. Denote $j\colon y \to z$ the morphism corresponding to $(0, 1)$. Thus we have a commutative diagram

$$\begin{tikzcd}
x \arrow[rr, "1"] \arrow[dr, "i"] & & x \\
& z \arrow[ur, "p"] \arrow[dr, "q"] & \\
y \arrow[rr, "1"] \arrow[ur, "j"] & & y
\end{tikzcd}$$

where the diagonal compositions are zero. It follows that $i \circ p + j \circ q\colon z \to z$ is the identity since it is a morphism which upon composing p gives p and upon composing q gives q. Suppose given morphisms $a\colon x \to w$ and $b\colon y \to w$. Then we can form the map $a \circ p + b \circ q\colon z \to w$. In this way we get a bijection $\mathrm{Mor}(z, w) = \mathrm{Mor}(x, w) \times \mathrm{Mor}(y, w)$ which show that $z = x \amalg y$. $\square$

Definition 73.3. Given a pair of objects x, y in a preadditive categore $\mathcal{A}$, the **direct sum** $x \oplus y$ of x and y is the direct product $x \times y$ endowed with the morphisms i, j, p, q as in Lemma (73.2).

Lemma 73.3. *Let $\mathcal{A}$ and $\mathcal{B}$ be preadditive categories. Let $F\colon \mathcal{A} \to \mathcal{B}$ be an additive functor. Then F transforms direct sums to direct sums and zero to zero.*

Proof. A direct sum z of x and y is characterized by having morphisms $i\colon x \to z$, $j\colon y \to z$, $p\colon z \to x$, and $q\colon z \to y$ such that $p \circ i = 1_x$, $q \circ j = 1_y$, $p \circ j = 0$, $q \circ i = 0$, and $i \circ p + j \circ q = 1_z$. Clearly $F(x)$, $F(y)$, $F(z)$ and the morphisms $F(i), F(j), F(p), F(q)$ satisfy exactly the same relations (by additivity) and we see that $F(z)$ is a direct sum of $F(x)$ and $F(y)$. Hence, F transforms direct sums to direct sums. $\square$

73.1.2 Additive Category

Definition 73.4. A category $\mathcal{A}$ is called **additive** if it is preadditive and finite products exist. In other words, it has a zero object and direct sums.

Definition 73.5. Let $\mathcal{A}$ be a preadditive category and let $f\colon x \to y$ be a morphism.

1. A **kernel** of f is an equalizer of $f\colon x \to y$ and $0\colon x \to y$. If it exists, then it is unique up to unique isomorphism. With this in mind, we talk about *the* kernel of f and denote it by $\iota\colon \ker f \to x$. Thus we have $f\iota = 0$ and if $\iota'\colon z \to x$ is an other morphism such that $f\iota' = 0$, then there exists a unique morphism $g\colon z \to \ker f$ such that $\iota' = \iota g$.

2. A **cokernel** of f is a coequalizer of $f\colon x \to y$ and $0\colon x \to y$. If it exists, then it is unique up to unique isomorphism. With this in mind, we talk about *the* cokernel of f and denote it by $\pi\colon y \to \operatorname{coker} f$. Thus we have $\pi f = 0$ and if $\pi'\colon y \to z$ is an other morphism such that $\pi' f = 0$, then there exists a unique morphism $g\colon \operatorname{coker} f \to z$ such that $\pi' = g\pi$.

3. If a kernel of f exists, then a **coimage** of f is a cokernel of the morphism $\ker f \to x$. If it exists, then it is unique up to unique isomorphism. With this in mind, we talk about *the* coimage of f and denote it by $x \to \operatorname{coim} f$.

4. If a cokernel of f exists, then a **image** of f is a kernel of the morphism $y \to \operatorname{coker} f$. If it exists, then it is unique up to unique isomorphism. With this in mind, we talk about *the* image of f and denote it by $\operatorname{im} f \to y$.

Lemma 73.4. *Let $\mathcal{C}$ be a preadditive category. Let $x \oplus y$ with morphisms i, j, p, q as in Lemma (73.2) be a direct sum in $\mathcal{C}$. Then $i\colon x \to x \oplus y$ is a kernel of $q\colon x \oplus y \to y$. Dually, p is a cokernel for j.*

Proof. Let $f\colon z' \to x \oplus y$ be a morphism such that $qf = 0$. We have to show taht there exists a unique morphism $g\colon z' \to x$ such that $f = ig$. SInce $ip + jq$ is the identity on $x \oplus y$ we see that

$$\begin{aligned} f &= (ip + jq)f \\ &= ipf \end{aligned}$$

and hence $g = pf$ works. Uniqueness holds because pi is the idenity on x. The proof of the second statement is dual. □

Lemma 73.5. *Let $\mathcal{C}$ be a preadditive category. Let $f\colon x \to y$ be a morphism in $\mathcal{C}$.*

1. *If a kernel of f exists, then this kernel is a monomorphism.*

2. *If a cokernel of f exists, then this cokernel is an epimorphism.*

3. *If a kernel and coimage of f exist, then the coimage is an epimorphism.*

4. *If a cokernel and image of f exist, then the image is a monomorphism.*

Lemma 73.6. *Let $f\colon x \to y$ be a morphism in a preadditive category such that the kernel, cokernel, image, and coimage all exist. Then f can be factored uniquely as*

$$x \to \operatorname{coim} f \to \operatorname{im} f \to y.$$

Proof. There is a canonical morphism $\operatorname{coim} f \to y$ because $\ker f \to x \to y$ is zero. The composition $\operatorname{coim} f \to y \to \operatorname{coker} f$ is zero, because it is the unique morphism which gives rise to the morphism $x \to y \to \operatorname{coker} f$ which is zero. Hence $\operatorname{coim} f \to y$ factors uniquely through $\operatorname{im} f \to y$, which gives us the desired map. □

73.2 Abelian Category

An abelian category is a category satisfying just enough axioms so the snake lemma holds.

Definition 73.6. A category $\mathcal{A}$ is called **abelian** if

1. it is additive;

2. all kernels and cokernels exist;

3. the natural map $\operatorname{coim} f \to \operatorname{im} f$ is an isomorphism for all morphisms f in $\mathcal{A}$.

Definition 73.7. Let $f\colon x \to y$ be a morphism in an abelian category.

1. We say f is **injective** if $\ker f = 0$.

2. We say f is **surjective** if $\operatorname{coker} f = 0$.

3. If $x \to y$ is injective, then we say that x is a **subobject** of y and we use the notation $x \subseteq y$ to denote this. If $x \to y$ is surjective, then we say y is a **quotient** of x.

Lemma 73.7. *Let $f\colon x \to y$ be a morphism in an abelian category $\mathcal{A}$. Then*

1. *f is injective if and only if f is a monomorphism.*

2. *f is surjective if and only if f is an epimorphism.*

Lemma 73.8. *Let $\mathcal{A}$ be an abelian category. All finite limits and finite colimits exist in $\mathcal{A}$.*

73.3 R-Linear Categories

Definition 73.8. An R-**linear category** $\mathcal{A}$ is a category where every morphism set is given the structure of an R-module and where $x, y, z \in \mathrm{Ob}(\mathcal{A})$ composition law

$$\mathrm{Hom}_{\mathcal{A}}(y,z) \times \mathrm{Hom}_{\mathcal{A}}(x,y) \to \mathrm{Hom}_{\mathcal{A}}(x,z)$$

is R-bilinear. Thus composition determines an R-linear map

$$\mathrm{Hom}_{\mathcal{A}}(y,z) \otimes_R \mathrm{Hom}_{\mathcal{A}}(x,y) \to \mathrm{Hom}_{\mathcal{A}}(x,z)$$

of R-modules. A functor $F\colon \mathcal{A} \to \mathcal{B}$ of R-linear categories is called R-**linear** if the map

$$F\colon \mathrm{Hom}_{\mathcal{A}}(x,y) \to \mathrm{Hom}_{\mathcal{A}}(F(x), F(y))$$

is an R-linear map.

Example 73.1. The category Mod_R of all R-modules and R-linear maps is an R-linear category. Indeed, for each R-module M and N, we have an R-module $\mathrm{Hom}_R(M, N)$. Composition

$$\mathrm{Hom}_R(M_2, M_3) \times \mathrm{Hom}_R(M_1, M_2) \to \mathrm{Hom}_R(M_1, M_3),$$

defined by $(\varphi_2, \varphi_1) \mapsto \varphi_2 \circ \varphi_1$, is easily checked to be R-bilinear.

73.3.1 Additive functor from Graded Modules Induces Functor on Complexes

Proposition 73.1. *Let $\mathcal{F}\colon \mathrm{Grad}_R \to \mathrm{Grad}_R$ be an additive functor. Then $\mathcal{F}$ induces a functor*

$$\mathcal{F}\colon \mathrm{Comp}_R \to \mathrm{Comp}_R,$$

where an R-complex (A, d) gets mapped to the R-complex $(\mathcal{F}(A), \mathcal{F}(\mathrm{d}))$.

Proof. Let (A, d) be an R-complex. We first need to show that $(\mathcal{F}(A), \mathcal{F}(\mathrm{d}))$ is an R-complex. Indeed, $\mathcal{F}(A)$ is a graded R-module and $\mathcal{F}(\mathrm{d})$ is a graded homomorphism of degree -1. Moreover,

$$\begin{aligned}\mathcal{F}(\mathrm{d})\mathcal{F}(\mathrm{d}) &= \mathcal{F}(\mathrm{dd}) \\ &= \mathcal{F}(0) \\ &= 0.\end{aligned}$$

Thus $(\mathcal{F}(A), \mathcal{F}(\mathrm{d}))$ is an R-complex.
Next, let $\varphi\colon A \to A'$ be a chain map of R-complexes. Then

$$\begin{aligned}\mathcal{F}(\varphi)\mathcal{F}(\mathrm{d}) &= \mathcal{F}(\varphi\mathrm{d}) \\ &= \mathcal{F}(\mathrm{d}\varphi) \\ &= \mathcal{F}(\mathrm{d})\mathcal{F}(\varphi).\end{aligned}$$

Thus $\mathcal{F}(\varphi)$ is also a chain map. □

73.4 Functors Which Preserve Homotopy

73.4.1 Tensor Product

Proposition 73.2. *Let N be an R-module, let $\varphi\colon M \to M'$ and $\psi\colon M \to M'$ be two chain maps of R-complexes and suppose $\varphi \sim \psi$. Then $\varphi \otimes N \sim \psi \otimes N$.*

Proof. Choose a homotopy $h\colon M \to M'$ from φ to ψ. So

$$\varphi - \psi = \mathrm{d}_{M'}h + h\mathrm{d}_M.$$

We claim that $h \otimes N\colon M \otimes_R N \to M' \otimes_R N$ is a homotopy from $\varphi \otimes N$ to $\psi \otimes N$. Indeed, let $u \otimes v \in M \otimes_R N$ with $u \in M_i$ and $v \in N_j$. Then we have

$$\begin{aligned}
(\mathrm{d}^{\otimes}_{(M',N)}(h \otimes N) + (h \otimes N)\mathrm{d}^{\otimes}_{(M,N)})(u \otimes v) &= \mathrm{d}^{\otimes}_{(M',N)}(h(u) \otimes v) + (h \otimes N)(\mathrm{d}_M(u) \otimes v + (-1)^i u \otimes \mathrm{d}_N(v)) \\
&= \mathrm{d}_{M'}h(u) \otimes v - (-1)^i h(u) \otimes \mathrm{d}_N(v) + h\mathrm{d}_M(u) \otimes v + (-1)^i h(u) \otimes \mathrm{d}_N(v)) \\
&= \mathrm{d}_{M'}h(u) \otimes v + h\mathrm{d}_M(u) \otimes v \\
&= (\mathrm{d}_{M'}h(u) + h\mathrm{d}_M(u)) \otimes v \\
&= ((\mathrm{d}_{M'}h + h\mathrm{d}_M)(u)) \otimes v \\
&= (\varphi - \psi)(u)) \otimes v \\
&= \varphi(u) \otimes v - \psi(u) \otimes v \\
&= (\varphi \otimes N)(u \otimes v) - (\psi \otimes N)(u \otimes v) \\
&= (\varphi \otimes N - \psi \otimes N)(u \otimes v).
\end{aligned}$$

It follows that

$$\varphi \otimes N - \psi \otimes N = \mathrm{d}^{\otimes}_{(M',N)}(h \otimes N) + (h \otimes N)\mathrm{d}^{\otimes}_{(M,N)}.$$

□

73.4.2 R-linear Functor Preserves Homotopy

Proposition 73.3. *Let $\varphi\colon A \to A'$ and $\psi\colon A \to A'$ be two chain maps of R-complexes which are homotopic to each other, and let $F\colon \mathrm{Comp}_R \to \mathrm{Comp}_R$ be an R-linear functor. Then $F(\varphi)$ is homotopic to $F(\psi)$.*

Proof. Choose a homotopy $h\colon A \to A'$ from φ to ψ. So

$$\varphi - \psi = \mathrm{d}_{A'}h + h\mathrm{d}_A.$$

We claim that $F(h)\colon F(A) \to F(A')$ is a homotopy from $F(\varphi)$ to $F(\psi)$. Indeed, let $a \in F(A)$ with $a \in F(A)_i$. Then we have

$$(\mathrm{d}_{F(A')}F(h) + F(h)\mathrm{d}_{F(A)})(a)$$

$$= (F(\varphi) - F(\psi))(a).$$

It follows that □

Proposition 73.4. *Let (A, d) and (A', d') be R-complexes and let $F\colon \mathbf{Grad}_R \to \mathbf{Grad}_R$ be an R-linear functor. Suppose A is homotopically equivalent to A'. Then $(F(A), F(\mathrm{d}))$ is homotopically equivalent to $(F(A'), F(\mathrm{d}'))$.*

Proof. Choose chain maps $\varphi\colon A \to A'$ and $\varphi'\colon A' \to A$ together with homotopies $h\colon A \to A'$ and $h'\colon A \to A'$ where

$$\varphi'\varphi - 1_A = \mathrm{d}h + h\mathrm{d} \qquad \text{and} \qquad \varphi\varphi' - 1_{A'} = \mathrm{d}'h' + h'\mathrm{d}'.$$

Then observe that

$$\begin{aligned}
F(\varphi')F(\varphi) - 1_{F(A)} &= F(\varphi')F(\varphi) - F(1_A) \\
&= F(\varphi'\varphi - 1_A) \\
&= F(\mathrm{d}h + h\mathrm{d}) \\
&= F(d)F(h) + F(h)F(d).
\end{aligned}$$

Thus $\mathcal{F}(\varphi')\mathcal{F}(\varphi) \sim 1_{\mathcal{F}(A)}$. A similar argument shows $\mathcal{F}(\varphi)\mathcal{F}(\varphi) \sim 1_{\mathcal{F}(A')}$. Therefore $\mathcal{F}(A)$ is homotopically equivalent to $\mathcal{F}(A')$. □

73.5 Epimorphisms and Monomorphisms

Definition 73.9. Let $\mathcal{C}$ be a category and let $f\colon x \to y$ be a morphism in $\mathcal{C}$.

1. We say f is an **epimorphism** if it is right-cancellative: $g_1 f = g_2 f$ implies $g_1 = g_2$ for all $g_1\colon y \to z$ and $g_2\colon y \to z$.
2. We say f is a **split epimorphism** if it has a right-sided inverse: there exists $g\colon y \to x$ such that $fg = 1_x$.
3. We say f is a **monomorphism** if it is left-cancellative: $fg_1 = fg_2$ implies $g_1 = g_2$ for all $g_1\colon w \to x$ and $g_2\colon w \to x$.
4. We say f is a **split monomorphism** if it has a left-sided inverse: there exists $g\colon y \to x$ such that $gf = 1_x$.
5. We say f is a **bimorphism** if it is both a monomorphism and an epimorphism.
6. We say f is an **isomorphism** if it is both a split monomomorphism and a split epimorphism.

73.5.1 Epimorphisms and Monomorphisms in $\mathbf{Comp}_R$

Proposition 73.5. *Let $\varphi\colon A \to B$ be a chain map. Then φ is an epimorphism if and only if φ is surjective*

73.6 Adjunctions

Definition 73.10. An **adjunction** between categories $\mathcal{C}$ and $\mathcal{D}$ consists of a pair of functors $F\colon \mathcal{C} \to \mathcal{D}$ and $G\colon \mathcal{D} \to \mathcal{C}$ such that for all objects x in $\mathcal{C}$ and y in $\mathcal{D}$ we have a bijection

$$\tau_{y,x}\colon \operatorname{Hom}_{\mathcal{C}}(Gy, x) \to \operatorname{Hom}_{\mathcal{D}}(y, Fx)$$

which is natural in x and y. We also say G is **left adjoint to** F and F is **right adjoint to** G.

Proposition 73.6. *Let $F\colon \mathcal{C} \to \mathcal{D}$ to left-adjoint to $G\colon \mathcal{D} \to \mathcal{C}$. Then F preserves colimits and G preserves limits.*

Proof. Let us show that F preserves colimits. Let (□

Proposition 73.7. *Let M be a graded R-module. The functor $- \otimes_R M\colon \mathbf{Grad}_R \to \mathbf{Grad}_R$ is left adjoint to the functor $\operatorname{Hom}_R(M, -)\colon \mathbf{Grad}_R \to \mathbf{Grad}_R$. In particular, $- \otimes_R M$ preserves direct limits and $\operatorname{Hom}^\star_R(M, -)$ preserves inverse limits.*

Proof. Let us show that $- \otimes_R M$ being left adjoint to $\operatorname{Hom}^\star_R(M, -)$ implies $- \otimes_R M$ preserves direct limits. Let $(M_\lambda, \varphi_{\lambda\mu})$ be a direct system of graded R-modules and graded R-linear maps indexed over a preordered set $(\Lambda, \leq)$. Since $- \otimes_R M$ is a covariant functor, $(M_\lambda \otimes_R M, \varphi_{\lambda\mu} \otimes 1_M)$ is a direct system of graded R-modules and graded R-linear maps indexed over a preordered set $(\Lambda, \leq)$. Furthermore, □

Part VII
Abstract Algebra Homework

74 Homework 1

74.1 Hom-cancellation

Proposition 74.1. *Let M be an R-module. Then*

$$\operatorname{Hom}_R(R, M) \cong M.$$

Proof. Define $\Psi\colon \operatorname{Hom}_R(R, M) \to M$ by

$$\Psi(\varphi) = \varphi(1)$$

for all $\varphi \in \operatorname{Hom}_R(R, M)$. We claim that Ψ is an R-module isomorphism. We first check that Ψ is an R-module homomorphism. Let $a, b \in R$ and let $\varphi, \psi \in \operatorname{Hom}_R(R, M)$, then

$$\begin{aligned}\Psi(a\varphi + b\psi) &= (a\varphi + b\psi)(1) \\ &= a\varphi(1) + b\psi(1) \\ &= a\Psi(\varphi) + b\Psi(\psi).\end{aligned}$$

Thus Ψ is an R-module homomorphism.

We next check that Ψ is injective. Suppose $\varphi \in \mathrm{Hom}_R(R, M)$ such that $\Psi(\varphi) = 0$. Then for all $a \in R$, we have

$$\begin{aligned} \varphi(a) &= a\varphi(1) \\ &= a\Psi(\varphi) \\ &= a \cdot 0 \\ &= 0. \end{aligned}$$

Thus $\varphi = 0$. It follows that $\ker \Psi = 0$, which implies Ψ is injective.

We next check that Ψ is surjective. Let $u \in M$. Define $\varphi \colon R \to M$ by setting $\varphi(1) = u$ and extending R-linearly:

$$\begin{aligned} \varphi(a) &= a\varphi(1) \\ &= au \end{aligned}$$

for all $a \in R$. Let us first check that the map φ defined above is indeed an R-module homomorphism. We already have R-scaling by construction, so it suffices to show that φ is additive. Let $a, b \in R$. Then

$$\begin{aligned} \varphi(a+b) &= (a+b)\varphi(1) \\ &= a\varphi(1) + b\varphi(1) \\ &= \varphi(a) + \varphi(b). \end{aligned}$$

Thus $\varphi \in \mathrm{Hom}_R(R, M)$. Finally note that $\Psi(\varphi) = u$, which implies Ψ is surjective. $\square$

74.2 Annihilator Ideals and Torsion

Problem 2.a

Proposition 74.2. *Let M be an R-module and let $u \in M$. Define*

$$0 : u = \{a \in R \mid au = 0\}.$$

Then the set $0 : u$ is an ideal in R.

Proof. First note that $0 : u$ is nonempty since $0 \cdot u = 0$ implies $0 \in 0 : u$. Let $x, y \in 0 : u$ and let $a \in R$. Then

$$\begin{aligned} (x+ay)u &= xu + ayu \\ &= 0 + a \cdot 0 \\ &= 0 \end{aligned}$$

implies $x + ay \in 0 : u$. This implies $0 : u$ is an ideal in R. $\square$

Problem 2.b

Proposition 74.3. *Suppose R is a domain. Then the set of torsion elements of M forms a submodule of M.*

Proof. Let M_{tor} denote the set of all torsion elements of M. Thus $u \in M_{\mathrm{tor}}$ implies there exists a nonzero $a \in R$ such that $au = 0$. Observe that M_{tor} is nonempty since $0 \in M_{\mathrm{tor}}$ (take $1 \in R$, then $1 \cdot 0 = 0$). Let $u, v \in M_{\mathrm{tor}}$ and let $a \in R$. Choose $c, d \in R \backslash \{0\}$ such that $cu = 0$ and $dv = 0$. Since R is a domain and both c and d are nonzero, we must have cd be nonzero too. Thus

$$\begin{aligned} cd(u+av) &= cdu + cdav \\ &= d(cu) + ac(dv) \\ &= d \cdot 0 + (ac) \cdot 0 \\ &= 0 \end{aligned}$$

implies $u + av \in M_{\mathrm{tor}}$. Thus M_{tor} is a submodule of M. $\square$

Remark 132. If R is not a domain, then it may not be the case that M_{tor} is a submodule of M. Indeed, consider the case where $R = K[x,y]/\langle xy \rangle$ and $M = R$ and K is a field. Note that R is not a domain since $\overline{xy} = \overline{0}$ even though $\overline{x} \neq \overline{0}$ and $\overline{y} \neq \overline{0}$. Also note that R_{tor} is not an ideal of R. Indeed, we have $\overline{x}, \overline{y} \in R_{\text{tor}}$ since $\overline{xy} = \overline{0}$ with $\overline{x}, \overline{y} \neq \overline{0}$, but $\overline{x} + \overline{y} \notin R_{\text{tor}}$. To see that $\overline{x} + \overline{y} \notin R_{\text{tor}}$, suppose we have

$$f(\overline{x}, \overline{y})(\overline{x} + \overline{y}) = \overline{0}. \tag{307}$$

where $f(\overline{x}, \overline{y})$ is the coset in R with $f(x,y) \in K[x,y]$ as a representative. The equation (9) tells us that we can find $g(x,y) \in K[x,y]$ such that

$$f(x,y)(x+y) = g(x,y)xy. \tag{308}$$

Choose such a $g(x,y) \in K[x,y]$. Since $K[x,y]$ is a UFD and $x \nmid (x+y)$ and $y \nmid (x+y)$, we must have $xy \mid f(x,y)$, which implies $f(\overline{x}, \overline{y}) = \overline{0}$ in R.

74.3 Isomorphism Criterion

Proposition 74.4. *Let $\varphi \colon M \to N$ be an R-module homomorphism. Then φ is an isomorphism if and only if there exists an R-module homomorphism $\psi \colon N \to M$ such that $\varphi\psi = \mathrm{id}_N$ and $\psi\varphi = \mathrm{id}_M$.*

Proof. One direction is clear, so suppose that $\varphi \colon N \to M$ is both an R-module homomorphism and a bijection. Let ψ denote the inverse of φ. We want to show that ψ is an R-module homomorphism. Let $a, b \in R$ and $u, v \in N$. Then

$$\begin{aligned} a\psi(u) + b\psi(v) &= \psi\varphi(a\psi(u) + b\psi(v)) \\ &= \psi(a(\varphi(\psi(u))) + b(\varphi(\psi(v)))) \\ &= \psi(au + bv). \end{aligned}$$

Thus ψ is an R-module homomorphism, and so φ is an isomorphism. $\square$

74.4 Projector Direct Sum

Proposition 74.5. *Let $\varphi \colon M \to M$ be an R-module homomorphism such that $\varphi(\varphi(u)) = \varphi(u)$ for all $u \in M$. Then*

$$M \cong \ker \varphi \oplus \operatorname{im} \varphi.$$

Proof. Define $\Psi \colon M \to \ker \varphi \oplus \operatorname{im} \varphi$ by

$$\Psi(u) = (u - \varphi(u), \varphi(u))$$

for all $u \in M$. Observe that $u - \varphi(u) \in \ker \varphi$ since

$$\begin{aligned} \varphi(u - \varphi(u)) &= \varphi(u) - \varphi(\varphi(u)) \\ &= \varphi(u) - \varphi(u) \\ &= 0. \end{aligned}$$

Thus we really do have $\Psi(u) \in \ker \varphi \oplus \operatorname{im} \varphi$ for all $u \in M$.

Let us check that Ψ is an R-module homomorphism. Let $a, b \in R$ and $u, v \in M$. Then

$$\begin{aligned} \Psi(au + bv) &= ((au + bv) - \varphi(au + bv), \varphi(au + bv)) \\ &= (au + bv - a\varphi(u) - b\varphi(v), a\varphi(u) + b\varphi(v)) \\ &= (a(u - \varphi(u)) + b(v - \varphi(v)), a\varphi(u) + b\varphi(v)) \\ &= (a(u - \varphi(u)), a\varphi(u)) + (b(v - \varphi(v)), b\varphi(v)) \\ &= a(u - \varphi(u), \varphi(u)) + b(v - \varphi(v), \varphi(v)) \\ &= a\Psi(u) + b\Psi(v). \end{aligned}$$

Thus Ψ is an R-module homomorphism.

We now show that Ψ is injective. Let $u \in M$ and suppose $\Psi(u) = (0,0)$. Then

$$\begin{aligned} (0,0) &= \Psi(u) \\ &= (u - \varphi(u), \varphi(u)) \end{aligned}$$

implies $\varphi(u) = 0$ and $u - \varphi(u) = 0$, which together implies $u = 0$. Thus $\ker \Psi = 0$, and so Ψ is injective.

Finally, we show that Ψ is surjective. Let $(u, \varphi(v)) \in \ker \varphi \oplus \operatorname{im} \varphi$. Then $u + \varphi(v) \in M$, and moreover we have

$$\begin{aligned}
\Psi(u+\varphi(v)) &= (u+\varphi(v)-\varphi(u+\varphi(v)), \varphi(u+\varphi(v))) \\
&= (u+\varphi(v)-\varphi(u)-\varphi(v)), \varphi(u)+\varphi(\varphi(v))) \\
&= (u, \varphi(\varphi(v))) \\
&= (u, \varphi(v)).
\end{aligned}$$

Thus Ψ is surjective. □

74.5 No (unitary) $\mathbb{Q}$-Module Structure on $\mathbb{Z}$

Proposition 74.6. *There is no (unitary) $\mathbb{Q}$-module structure on $\mathbb{Z}$.*

Proof. Suppose $\cdot : \mathbb{Q} \times \mathbb{Z} \to \mathbb{Z}$, denoted $(r, m) \mapsto r \cdot m$, gives us a $\mathbb{Q}$-module structure on $\mathbb{Z}$. Set $n = \frac{1}{2} \cdot 1$. Then

$$\begin{aligned}
2n &= n + n \\
&= \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 \\
&= \left(\frac{1}{2} + \frac{1}{2}\right) \cdot 1 \\
&= 1 \cdot 1 \\
&= 1
\end{aligned}$$

implies 2 divides 1, which is a contradiction. □

75 Homework 2

75.1 Five Lemma

Proposition 75.1. *Suppose the following diagram of R-modules and R-homomorphisms is commutative with exact rows*

$$\begin{tikzcd}
M_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "\psi_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "\psi_3"] & M_4 \arrow[r, "\varphi_4"] \arrow[d, "\psi_4"] & M_5 \arrow[d, "\psi_5"] \\
M_1' \arrow[r, "\varphi_1'"] & M_2' \arrow[r, "\varphi_2'"] & M_3' \arrow[r, "\varphi_3'"] & M_4' \arrow[r, "\varphi_4'"] & M_5'
\end{tikzcd}$$

1. *If ψ_2, ψ_4 are surjective and ψ_5 is injective, then ψ_3 is surjective.*
2. *If ψ_2, ψ_4 are injective and ψ_1 is surjective, then ψ_3 is injective.*

Proof.

1. Suppose ψ_2, ψ_4 are surjective and ψ_5 is injective and let $u_3' \in M_3'$. Since ψ_4 is surjective, we may choose a $u_4 \in M_4$ such that $\psi_4(u_4) = \varphi_3'(u_3')$. Observe that

$$\begin{aligned}
\psi_5\varphi_4(u_4) &= \varphi_4'\psi_4(u_4) \\
&= \varphi_4'\varphi_3'(u_3') \\
&= 0.
\end{aligned}$$

It follows that $\varphi_4(u_4) = 0$ since ψ_5 is injective. Therefore we may choose a $u_3 \in M_3$ such that $\varphi_3(u_3) = u_4$ (by exactness of the top row). Now observe that

$$\begin{aligned}
\varphi_3'(u_3' - \psi_3(u_3)) &= \varphi_3'(u_3') - \varphi_3'\psi_3(u_3) \\
&= \psi_4(u_4) - \psi_4\varphi_3(u_3) \\
&= \psi_4(u_4) - \psi_4(u_4) \\
&= 0.
\end{aligned}$$

Therefore we may choose a $u_2' \in M_2'$ such that $\varphi_2'(u_2') = u_3' - \psi_3(u_3)$ (by exactness of the bottom row). Since ψ_2 is surjective, we may choose a $u_2 \in M_2$ such that $\psi_2(u_2) = u_2'$. Finally we see that

$$\begin{aligned}
\psi_3(\varphi_2(u_2) + u_3) &= \psi_3\varphi_2(u_2) + \psi_3(u_3) \\
&= \varphi_2'\psi_2(u_2) + \psi_3(u_3) \\
&= \varphi_2'(u_2') + \psi_3(u_3) \\
&= u_3' - \psi_3(u_3) + \psi_3(u_3) \\
&= u_3'.
\end{aligned}$$

It follows that ψ_3 is surjective.

2. Suppose ψ_2, ψ_4 are injective and ψ_1 is surjective and let $u_3 \in \ker \psi_3$. Observe that

$$\begin{aligned}
\psi_4\varphi_3(u_3) &= \varphi_3'\psi_3(u_3) \\
&= \varphi_3'(0) \\
&= 0.
\end{aligned}$$

It follows that $\varphi_3(u_3) = 0$ since ψ_4 is injective. Therefore we may choose a $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ (by exactness of the top row). Now observe that

$$\begin{aligned}
\varphi_2'\psi_2(u_2) &= \psi_3\varphi_2(u_2) \\
&= \psi_3(u_3) \\
&= 0.
\end{aligned}$$

Therefore we may choose a $u_1' \in M_1'$ such that $\varphi_1'(u_1') = \psi_2(u_2)$ (by exactness of the bottom row). Since ψ_1 is surjective, we may choose a $u_1 \in M_1$ such that $\psi_1(u_1) = u_1'$. Now observe that

$$\begin{aligned}
\psi_2\varphi_1(u_1) &= \varphi_1'\psi_1(u_1) \\
&= \varphi_1'(u_1') \\
&= \psi_2(u_2).
\end{aligned}$$

It follows that $\varphi_1(u_1) = u_2$ since ψ_2 is injective. Therefore

$$\begin{aligned}
u_3 &= \varphi_2(u_2) \\
&= \varphi_2\varphi_1(u_1) \\
&= 0,
\end{aligned}$$

which implies $\ker \psi_3 = 0$. Thus ψ_3 is injective. □

75.2 3×3 Lemma

Proposition 75.2. *Consider the following diagram*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & M_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "\psi_2"] & M_3 \arrow[r] \arrow[d, "\psi_3"] & 0 \\
0 \arrow[r] & M_1' \arrow[r, "\varphi_1'"] \arrow[d, "\psi_1'"] & M_2' \arrow[r, "\varphi_2'"] \arrow[d, "\psi_2'"] & M_3' \arrow[r] \arrow[d, "\psi_3'"] & 0 \\
0 \arrow[r] & M_1'' \arrow[r, "\varphi_1''"] \arrow[d] & M_2'' \arrow[r, "\varphi_2''"] \arrow[d] & M_3'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

If the columns and top two rows are exact, then the bottom row is exact.

Proof. We first show φ_1'' is injective. Let $u_1'' \in \ker \varphi_1''$. Since ψ_1' is surjective (by exactness of first column) we may choose a $u_1' \in M_1'$ such that $\psi_1'(u_1') = u_1''$. Then

$$\begin{aligned}\psi_2'\varphi_1'(u_1') &= \varphi_1''\psi_1'(u_1') \\ &= \varphi_1''(u_1'') \\ &= 0\end{aligned}$$

implies $\varphi_1'(u_1') \in \ker \psi_2'$. Therefore there exists a unique $u_2 \in M_2$ such that $\psi_2(u_2) = \varphi_1'(u_1')$ (by exac Then

$$\begin{aligned}\psi_3\varphi_2(u_2) &= \varphi_2'\psi_2(u_2) \\ &= \varphi_2'\varphi_1'(u_1') \\ &= 0\end{aligned}$$

implies $\varphi_2(u_2) = 0$ since ψ_3 is injective (by exactness of third column). Thus $u_2 \in \ker \varphi_2$ and so there exists a unique $u_1 \in M_1$ such that $\varphi_1(u_1) = u_2$ (by exactness of first row). Therefore

$$\begin{aligned}\varphi_1'\psi_1(u_1) &= \psi_2\varphi_1(u_1) \\ &= \psi_2(u_2) \\ &= \varphi_1'(u_1')\end{aligned}$$

implies $\psi_1(u_1) = u_1'$ since φ_1' is injective (by exactness of second row). Thus

$$\begin{aligned}u_1'' &= \psi_1'(u_1') \\ &= \psi_1'\psi_1(u_1) \\ &= 0.\end{aligned}$$

Now we show $\ker \varphi_2'' = \operatorname{im} \varphi_1''$. Let $u_2'' \in \ker \varphi_2''$. Since ψ_2' is surjective (by exactness of second colunn), we may choose a $u_2' \in M_2'$ such that $\psi_2'(u_2') = u_2''$. Then

$$\begin{aligned}\psi_3'\varphi_2'(u_2') &= \varphi_2''\psi_2'(u_2') \\ &= \varphi_2''(u_2'') \\ &= 0\end{aligned}$$

implies $\varphi_2'(u_2') \in \ker \psi_3'$. Therefore there exists a unique $u_3 \in M_3$ such that $\psi_3(u_3) = \varphi_2'(u_2')$ (by exactness of third column). Since φ_2 is surjective, we may choose a $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$. Then

$$\begin{aligned}\varphi_2'(\psi_2(u_2) - u_2') &= \varphi_2'\psi_2(u_2) - \varphi_2'(u_2') \\ &= \psi_3\varphi_2(u_2) - \varphi_2'(u_2') \\ &= \psi_3(u_3) - \varphi_2'(u_2') \\ &= \varphi_2'(u_2') - \varphi_2'(u_2') \\ &= 0\end{aligned}$$

implies $\psi_2(u_2) - u_2' \in \ker \varphi_2'$. Therefore there exists a uniuqe $u_1' \in M_1'$ such that $\varphi_1'(u_1') = \psi_2(u_2) - u_2'$ (by exactness of second row). Therefore

$$\begin{aligned}\varphi_1''\psi_1'(u_1') &= \psi_2'\varphi_1'(u_1') \\ &= \psi_2'(\psi_2(u_2) - u_2') \\ &= \psi_2'\psi_2(u_2) - \psi_2'(u_2') \\ &= \psi_2'(u_2') \\ &= u_2''.\end{aligned}$$

It follows that $u_2'' \in \operatorname{im} \varphi_1''$. Thus $\ker \varphi_2'' \subseteq \operatorname{im} \varphi_1''$. For the reverse inclusion, let $u_2'' \in M_2''$. Choose $u_1'' \in M_1''$ such that $\varphi_1''(u_1'') = u_2''$. Since ψ_1' is surjective (by exactness of first column), we may choose a $u_1' \in M_1'$ such that $\psi_1'(u_1') = u_1''$. Then

$$\begin{aligned}0 &= \psi_3'\varphi_2'\varphi_1'(u_1') \\ &= \varphi_2''\psi_2'\varphi_1'(u_1') \\ &= \varphi_2''\varphi_1''\psi_1'(u_1') \\ &= \varphi_2''\varphi_1''(u_1'') \\ &= \varphi_2''(u_2'')\end{aligned}$$

implies $u_2'' \in \ker \varphi_2''$. Thus $\ker \varphi_2'' \supseteq \operatorname{im} \varphi_1''$.

The last step is to show φ_2'' is surjective. Let $u_3'' \in M_3''$. Since ψ_3' is surjective (by exactness of third column), we may choose a $u_3' \in M_3'$ such that $\psi_3'(u_3') = u_3''$. Since φ_2' is surjective (by exactness of second row), we may choose a $u_2' \in M_2'$ such that $\varphi_2'(u_2') = u_3'$. Then

$$\begin{aligned} \varphi_2''\psi_2'(u_2') &= \psi_3'\varphi_2'(u_2') \\ &= \psi_3'(u_3') \\ &= u_3'' \end{aligned}$$

implies φ_2'' is surjective. □

75.3 Snake Lemma

Proposition 75.3. *Consider the following commutative diagram with exact rows*

$$\begin{tikzcd} & M_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "\psi_2"] & M_3 \arrow[r] \arrow[d, "\psi_3"] & 0 \\ 0 \arrow[r] & M_1' \arrow[r, "\varphi_1'"] & M_2' \arrow[r, "\varphi_2'"] & M_3' & \end{tikzcd} \tag{309}$$

Then there exists an exact sequence

$$\ker \psi_1 \xrightarrow{\widetilde{\varphi_1}} \ker \psi_2 \xrightarrow{\widetilde{\varphi_2}} \ker \psi_3 \xrightarrow{\partial} \operatorname{coker} \psi_1 \xrightarrow{\overline{\varphi_1'}} \operatorname{coker} \psi_2 \xrightarrow{\overline{\varphi_2'}} \operatorname{coker} \psi_3. \tag{310}$$

Moreover, if φ_1 is injective, then $\widetilde{\varphi_1}$ is injective; and if φ_2' is surjective, then $\overline{\varphi_2'}$ is surjective.

Proof.

Step 1: We first define the maps in question. Define $\widetilde{\varphi_1}\colon \ker \psi_1 \to \ker \psi_2$ by

$$\widetilde{\varphi_1}(u_1) = \varphi_1(u_1)$$

for all $u_1 \in \ker \psi_1$. Note that $\widetilde{\varphi_1}$ lands in $\ker \psi_2$ by the commutativity of the diagram. Indeed,

$$\begin{aligned} \psi_2\widetilde{\varphi_1}(u_1) &= \psi_2\varphi_1(u_1) \\ &= \varphi_1'\psi_1(u_1) \\ &= \varphi_1'(0) \\ &= 0 \end{aligned}$$

implies $\widetilde{\varphi_1}(u_1) \in \ker \psi_2$ for all $u_1 \in \ker \psi_1$. Also note that $\widetilde{\varphi_1}$ is an R-module homomorphism since φ_1 is an R-module homomorphism. Similarly, we define $\widetilde{\varphi_2}\colon \ker \psi_2 \to \ker \psi_3$ by

$$\widetilde{\varphi_2}(u_2) = \varphi_2(u_2)$$

for all $u_2 \in \ker \psi_2$.

Next we define $\partial\colon \ker \psi_3 \to \operatorname{coker} \psi_1$ as follows: let $u_3 \in \ker \psi_3$. Choose $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ (such an element exists because φ_2 is surjective by exactness of the first row). By the commutativity of the diagram, we have

$$\begin{aligned} \varphi_2'\psi_2(u_2) &= \psi_3\varphi_2(u_2) \\ &= \psi_3(u_3) \\ &= 0. \end{aligned}$$

It follows that $\psi_2(u_2) \in \ker \varphi_2'$. Therefore there exists a unique $u_1' \in M_1'$ such that $\varphi_1'(u_1') = \psi_2(u_2)$ (by exactness of the second row). We set

$$\partial(u_3) = \overline{u_1'}$$

where $\overline{u_1'}$ is the coset in $\operatorname{coker} \psi_1$ with u_1' as a representative. We must check that ∂ defined in this is in fact a well-defined map. There was one choice that we made in our construction, namely the lift of u_3 under φ_2 to u_2. So let v_2 be another element in M_2 such that $\varphi_2(v_2) = u_3$. Denote by v_1' to be the unique element in M_1' such that

$\varphi_1'(v_1') = \psi_2(v_2)$. We must show that $\overline{u_1'} = \overline{v_1'}$ in $\operatorname{coker}\psi_1$. In other words, we must show that $v_1' - u_1' \in \operatorname{im}\psi_1$. Observe that

$$\begin{aligned}\varphi_2(v_2 - u_2) &= \varphi_2(v_2) - \varphi_2(u_2)\\ &= u_3 - u_3\\ &= 0\end{aligned}$$

implies $v_2 - u_2 \in \ker\varphi_2$. It follows that there exists a unique element $u_1 \in M_1$ such that $\varphi_1(u_1) = v_2 - u_2$ (by exactness of the first row). Then

$$\begin{aligned}\varphi_1'\psi_1(u_1) &= \psi_2\varphi_1(u_1)\\ &= \psi_2(v_2 - u_2)\\ &= \psi_2(v_2) - \psi_2(u_2)\\ &= \varphi_1'(v_1') - \varphi_1'(u_1')\\ &= \varphi_1'(v_1' - u_1')\end{aligned}$$

implies $\psi_1(u_1) = v_1' - u_1'$ since φ_1' is injective (by exactness of the second row). It follows that $v_1' - u_1' \in \operatorname{im}\psi_1$, and hence ∂ is well-defined.

Finally, we define $\overline{\varphi_1'}\colon \operatorname{coker}\psi_1 \to \operatorname{coker}\psi_2$ by

$$\overline{\varphi_1'}(\overline{u_1'}) = \overline{\varphi_1'(u_1')}$$

for all $\overline{u_1'} \in \operatorname{coker}\psi_1$. The map $\overline{\varphi_1'}$ is well-defined by the commutativity of the diagram. Indeed, let v_1' be another representative of the coset $\overline{u_1'}$ in $\operatorname{coker}\psi_1$. Choose $u_1 \in M_1$ such that $v_1' - u_1' = \psi_1(u_1)$. Then

$$\begin{aligned}\psi_2\varphi_1(u_1) &= \varphi_1'\psi_1(u_1)\\ &= \varphi_1'(v_1' - u_1')\\ &= \varphi_1'(v_1') - \varphi_1'(u_1').\end{aligned}$$

It follows that $\varphi_1'(v_1') - \varphi_1'(u_1') \in \operatorname{im}\psi_2$, and hence $\varphi_1'(v_1')$ and $\varphi_1'(u_1')$ represent the same coset in $\operatorname{coker}\psi_2$. Similarly, we define $\overline{\varphi_2'}\colon \operatorname{coker}\psi_2 \to \operatorname{coker}\psi_3$ by

$$\overline{\varphi_2'}(\overline{u_2'}) = \overline{\varphi_2'(u_2')}$$

for all $\overline{u_2'} \in \operatorname{coker}\psi_2$.

Step 2: Now that we've defined the maps in question, we will now show that the sequence (310) is exact as well as prove the "moreover" part of the proposition. First we show exactness at $\ker\psi_2$. Observe that

$$\begin{aligned}\widetilde{\varphi_2}\widetilde{\varphi_1}(u_1) &= \varphi_2\varphi_1(u_1)\\ &= 0\end{aligned}$$

for all $u_1 \in \ker\psi_1$. It follows that $\ker\widetilde{\varphi_2} \supseteq \operatorname{im}\widetilde{\varphi_1}$. Conversely, let $u_2 \in \ker\widetilde{\varphi_2}$. Thus $u_2 \in \ker\varphi_2 \cap \ker\psi_2$. By exactness of the top row in (309), we may choose a $u_1 \in M_1$ such that $\varphi_1(u_1) = u_2$. Moreover,

$$\begin{aligned}\varphi_1'\psi_1(u_1) &= \psi_2\varphi_1(u_1)\\ &= \psi_2(u_2)\\ &= 0\end{aligned}$$

implies $\psi_1(u_1) = 0$ since φ_1' is injective (by exactness of the bottom row in (309)). Therefore $u_1 \in \ker\psi_1$, and so $u_2 \in \operatorname{im}\widetilde{\varphi_1}$. Thus $\ker\widetilde{\varphi_2} \subseteq \operatorname{im}\widetilde{\varphi_1}$.

Next we show exactness at $\ker\psi_3$: let $u_3 \in \ker\partial$. Choose $u_2 \in M_2$ and $u_1' \in M_1'$ such that $\varphi_2(u_2) = u_3$ and $\varphi_1'(u_1') = \psi_2(u_2)$. Then

$$\begin{aligned}0 &= \partial(u_3)\\ &= \overline{u_1'}\end{aligned}$$

implies $u_1' \in \operatorname{im}\psi_1$. Choose $u_1 \in M_1$ such that $\psi_1(u_1) = u_1'$. Then

$$\begin{aligned}\psi_2(u_2 - \varphi_1(u_1)) &= \psi_2(u_2) - \psi_2\varphi_1(u_1)\\ &= \psi_2(u_2) - \varphi_1'\psi_1(u_1)\\ &= \psi_2(u_2) - \varphi_1'(u_1')\\ &= \psi_2(u_2) - \psi_2(u_2)\\ &= 0\end{aligned}$$

implies $u_2 - \varphi_1(u_1) \in \ker \psi_2$. Furthermore, we have

$$\begin{aligned}\varphi_2(u_2 - \varphi_1(u_1)) &= \varphi_2(u_2) - \varphi_2\varphi_1(u_1) \\ &= \varphi_2(u_2) \\ &= u_3.\end{aligned}$$

It follows that $u_3 \in \operatorname{im} \widetilde{\varphi_2}$. Thus $\ker \partial \subseteq \operatorname{im} \widetilde{\varphi_2}$. Convsersely, let $u_3 \in \operatorname{im} \widetilde{\varphi_2}$. Choose $u_2 \in \ker \psi_2$ such that $\varphi_2(u_2) = u_3$. Then $0 \in M_1'$ is the unique element in M_1' which maps to $\psi_2(u_2) = 0$. Thus $\partial(u_3) = \overline{0}$ which implies $\ker \partial \supseteq \operatorname{im} \widetilde{\varphi_2}$.

Next we show exactness at $\operatorname{coker} \psi_1$: let $\overline{u_1'} \in \ker \overline{\varphi_1'}$. Then $\varphi_1'(u_1') = \psi_2(u_2)$ for some $u_2 \in M_2$. Moreover,

$$\begin{aligned}\psi_3\varphi_2(u_2) &= \varphi_2'\psi_2(u_2) \\ &= \varphi_2'\varphi_1'(u_1') \\ &= 0\end{aligned}$$

implies $\varphi_2(u_2) \in \ker \psi_3$. Also we have $\partial(\varphi_2(u_2)) = \overline{u_1'}$, and so $\overline{u_1'} \in \operatorname{im}\partial$. Thus $\ker \overline{\varphi}_1' \subseteq \operatorname{im}\partial$. Conversely, let $\overline{u_1'} \in \operatorname{im}\partial$. Choose $u_3 \in M_3$ and $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ and $\psi_2(u_2) = \varphi_1'(u_1')$. It follows that

$$\begin{aligned}\overline{\varphi_1'}(\overline{u_1'}) &= \overline{\varphi_1'(u_1')} \\ &= \overline{\psi_2(u_2)} \\ &= \overline{0}\end{aligned}$$

in $\operatorname{coker} \psi_2$. Thus $\ker \overline{\varphi_1'} \supseteq \operatorname{im}\partial$.

Next we check exactness at $\operatorname{coker} \psi_2$: let $\overline{u_2'} \in \ker \overline{\varphi_2'}$. Choose $u_3 \in M_3$ such that $\psi_3(u_3) = \varphi_2'(u_2')$ and choose $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$. Since

$$\begin{aligned}\varphi_2'(u_2' - \psi_2(u_2)) &= \varphi_2'(u_2') - \varphi_2'\psi_2(u_2) \\ &= \varphi_2'(u_2') - \psi_3\varphi_2(u_2) \\ &= \varphi_2'(u_2') - \psi_3(u_3) \\ &= \varphi_2'(u_2') - \varphi_2'(u_2') \\ &= 0,\end{aligned}$$

it follows that $u_2' - \psi_2(u_2) \in \ker \varphi_2'$. Therefore there exists a unique $u_1' \in M_1'$ such that $\varphi_1'(u_1') = u_2' - \psi_2(u_2)$ (by exactness of the bottom row in (309)). Then

$$\begin{aligned}\overline{\varphi_1'}(\overline{u_1'}) &= \overline{\varphi_1'(u_1')} \\ &= \overline{u_2' - \psi_2(u_2)} \\ &= \overline{u_2'}\end{aligned}$$

in $\operatorname{coker} \psi_2$. It follows that $\overline{u_2'} \in \operatorname{im} \overline{\varphi_2'}$ and hence $\ker \overline{\varphi_2'} \subseteq \operatorname{im} \overline{\varphi_1'}$. Conversely, let $\overline{u_2'} \in \operatorname{im} \overline{\varphi_2'}$. Choose $u_1' \in M_1'$ such that $\varphi_1'(u_1') = u_2'$. Then

$$\begin{aligned}0 &= \varphi_2'\varphi_1'(u_1') \\ &= \varphi_2'(u_2')\end{aligned}$$

implies $u_2' \in \ker \varphi_2$. Therefore $\overline{\varphi_2'}(\overline{u_2'}) = \overline{0}$ in $\operatorname{coker} \psi_3$, and it follows that $\ker \overline{\varphi_2'} \supseteq \operatorname{im} \overline{\varphi_1'}$.

Finally, we prove the moreover part of this proposition. Suppose that φ_1 is injective. We want to show that $\widetilde{\varphi_1}$ is injective. Let $u_1 \in \ker \widetilde{\varphi_1}$. Then

$$\begin{aligned}0 &= \widetilde{\varphi_1}(u_1) \\ &= \varphi_1(u_1)\end{aligned}$$

implies $u_1 = 0$ since φ_1 is injective. It follows that $\widetilde{\varphi_1}$ is injective. Now suppose that φ_2' is surjective. We want to show that $\overline{\varphi_2'}$ is surjective. Let $\overline{u_3'} \in \operatorname{coker} \psi_3$. Since φ_2' is surjective, we may choose a $u_2' \in M_2'$ such that $\varphi_2'(u_2') = u_3'$. Then

$$\begin{aligned}\overline{\varphi_2'}(\overline{u_2'}) &= \overline{\varphi_2'(u_2')} \\ &= \overline{u_3'}.\end{aligned}$$

It follows that $\overline{\varphi_2'}$ is surjective. $\square$

75.4 Simple and Cyclic Modules

Definition 75.1. Let M be an R-module.

1. We say M is **simple** if the only submodules of M are itself and 0.
2. We say M is **cyclic** if there exists a $u \in M$ such that $M = Ru$.

Problem 4.a

Proposition 75.4. *Let M be a simple R-module. Then M is cyclic.*

Proof. If $M = 0$, then the proposition is clear, so assume $M \neq 0$. Choose any nonzero element u in M. Since M is simple, the submodule of M generated by u, given by

$$\langle u \rangle = \{au \mid a \in R\},$$

must either be the zero module or all of M. Since u was chosen to be nonzero, we cannot have $\langle u \rangle = 0$. Thus $\langle u \rangle = M$, which implies M is cyclic. □

Problem 4.b

Proposition 75.5. *Let M be a nonzero simple R-module and let $\varphi \colon M \to M$ be any nonzero R-module homomorphism. Then φ is an isomorphism. Moreover, assuming R is commutative, then we have*

$$\mathrm{Hom}_R(M, M) \cong M. \tag{311}$$

Proof. Since M is simple and φ is nonzero, we must have $\ker \varphi = 0$ and $\operatorname{im} \varphi = M$. Thus φ is an isomorphism.

Now let us show (311). Choose a nonzero element u in M (so $M = \langle u \rangle$). We define $\Psi \colon \mathrm{Hom}_R(M, M) \to M$ by the formula

$$\Psi(\varphi) = \varphi(u)$$

for all $\varphi \in \mathrm{Hom}_R(M, M)$.

Let us show that Ψ is an R-module homomorphism. Let $a, b \in R$ and $\psi, \varphi \in \mathrm{Hom}_R(M, M)$. Then we have

$$\begin{aligned}\Psi(a\varphi + b\psi) &= (a\varphi + b\psi)(u) \\ &= a\varphi(u) + b\psi(u) \\ &= a\Psi(\varphi) + b\Psi(\psi).\end{aligned}$$

It follows that Ψ is an R-module homomorphism.

Next we show that Ψ is injective. Suppose $\varphi \in \ker \Psi$ (so $\varphi(u) = 0$). Since $M = \langle u \rangle$, every element in M has the form au for some $a \in R$, so let au be an arbitary element in M. Then

$$\begin{aligned}\varphi(au) &= a\varphi(u) \\ &= a \cdot 0 \\ &= 0.\end{aligned}$$

This implies $\varphi = 0$ and thus Ψ is injective.

Lastly, we show that Ψ is surjective. Let $bu \in M$ where $b \in R$ and let $m_b \colon M \to M$ be the multiplication by b map, given by

$$m_b(v) = bv$$

for all $v \in M$. Then m_b is an R-module homomorphism (assuming that R is commutative) and moreover we have

$$\begin{aligned}\Psi(m_b) &= m_b(u) \\ &= bu.\end{aligned}$$

This implies Ψ is surjective. □

76 Homework 3

76.1 Non-split SES with Middle Term a Direct Sum

Proposition 76.1. *Define* $\varphi\colon \mathbb{Z} \to \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ *by*

$$\varphi(a) = (2a, 0)$$

for all $a \in \mathbb{Z}$ *and define* $\psi\colon \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ *by*

$$\psi(a, \overline{a_1}, \overline{a_2}, \dots) = (\overline{a}, \overline{a_1}, \overline{a_2}, \dots)$$

for all $(a, \overline{a_1}, \overline{a_2}, \dots) \in \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$*. Then*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \xrightarrow{\psi} (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \longrightarrow 0 \tag{312}$$

is a short exact sequence which does not split, even though we have $\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} = \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$*.*

Proof. The maps defined above are $\mathbb{Z}$-linear since each component map is $\mathbb{Z}$-linear. The map φ is injective since 2 is a nonzerodivisor in $\mathbb{Z}$, and the map ψ is surjective since the quotient map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is surjective. We also have exactness at $\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. Indeed, let $(a, \overline{a_1}, \overline{a_2}, \dots) \in \ker \psi$. Then

$$\begin{aligned} 0 &= \psi(a, \overline{a_1}, \overline{a_2}, \dots) \\ &= (\overline{a}, \overline{a_1}, \overline{a_2}, \dots) \end{aligned}$$

implies $\overline{a_n} = 0$ for all $n \geq 1$ and $a = 2b$ for some $b \in \mathbb{Z}$. Then

$$\begin{aligned} (a, \overline{a_1}, \overline{a_2}, \dots) &= (2b, 0) \\ &= \varphi(b) \end{aligned}$$

implies $(a, \overline{a_1}, \overline{a_2}, \dots) \in \operatorname{im} \varphi$. Therefore we have exactness at $\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$, and so (312) is a short exact sequence.

Now we show that (312) does not split. Assume for a contradiction that it did split. Then there exists an R-linear map

$$\widetilde{\psi}\colon (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$$

such that $\psi\widetilde{\psi} = 1$. Let

$$\pi_1\colon \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z} \quad \text{and} \quad \pi_2\colon \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$$

be the natural projection maps and denote $\widetilde{\psi}_1 = \pi_1 \circ \widetilde{\psi}$ and $\widetilde{\psi}_2 = \pi_2 \circ \widetilde{\psi}$ to be the component maps of $\widetilde{\psi}$. Note that $\widetilde{\psi}_1\colon (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z}$ must be the zero map since 2 is a nonzerodivisor on $\mathbb{Z}$ and $2 \in \operatorname{Ann}((\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. Indeed, we have

$$\begin{aligned} 2\widetilde{\psi}_1((\overline{a_n})) &= \widetilde{\psi}_1((\overline{2a_n})) \\ &= \widetilde{\psi}_1(\overline{0}) \\ &= 0, \end{aligned}$$

which implies $\widetilde{\psi}_1((\overline{a_n})) = 0$ for all $(\overline{a_n}) \in (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. Now let $(\overline{a_n}) \in (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ with $\overline{a_1} = \overline{1}$ and denote $(b_n) = \widetilde{\psi}_2((\overline{a_n}))$. Then

$$\begin{aligned} (\overline{a_n}) &= \psi\widetilde{\psi}((\overline{a_n})) \\ &= \psi(\widetilde{\psi}_1((\overline{a_n})), \widetilde{\psi}_2((\overline{a_n}))) \\ &= \psi(0, (b_n)) \\ &= (\overline{0}, \overline{b_1}, \overline{b_2}, \dots). \end{aligned}$$

This is a contradiction since $\overline{a_1} = \overline{1}$. $\square$

76.2 Splicing SES's

Proposition 76.2. *Suppose for each $i \in \mathbb{Z}$, suppose we are given short exact sequences of the form*

$$0 \longrightarrow K_i \xrightarrow{\phi_i} M_i \xrightarrow{\psi_i} K_{i-1} \longrightarrow 0 \tag{313}$$

Then we can splice these short exact sequences together to get a long exact sequence of the form

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots \tag{314}$$

where $\varphi_i = \phi_{i-1} \circ \psi_i$.

Proof. Let $i \in \mathbb{Z}$. It follows the short exact sequences (313) that

$$\begin{aligned} \ker \varphi_i &= \ker(\phi_{i-1} \circ \psi_i) \\ &= \ker \psi_i \\ &= \operatorname{im} \phi_i \\ &= \operatorname{im}(\phi_i \circ \psi_{i+1}) \\ &= \operatorname{im} \varphi_{i+1}. \end{aligned}$$

As i was arbitrary, it follows that (314) is exact. □

Corollary 73. *Every long exact of R-modules can be formed by splicing together suitable short exact sequences.*

Proof. Let

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots \tag{315}$$

be an exact sequence of R-modules. For each $i \in \mathbb{Z}$, we break (315) into short exact sequences of the form

$$0 \longrightarrow \ker \varphi_i \xrightarrow{\iota_i} M_i \xrightarrow{\widetilde{\varphi}_i} \operatorname{im} \varphi_i \longrightarrow 0 \tag{316}$$

where ι_i is the inclusion map and $\widetilde{\varphi}_i$ is just φ_i but with range $\operatorname{im} \varphi_i$ rather than M_{i-1}. In fact, since $\ker \varphi_{i-1} = \operatorname{im} \varphi_i$, we can rewrite (317) as

$$0 \longrightarrow \ker \varphi_i \xrightarrow{\iota_i} M_i \xrightarrow{\varphi_i} \ker \varphi_{i-1} \longrightarrow 0 \tag{317}$$

Since $\varphi_i = \iota_{i-1} \circ \widetilde{\varphi}_i$, it follows from Proposition (76.2) that splicing these short exact sequences together gives us our original long exact sequence (315) . □

76.3 A ring isomorphic to arbitrary direct sums of itself

Proposition 76.3. *Let K be a field, let V be a vector space of countably infinite dimension over K, and set $A = \operatorname{Hom}_K(V, V)$. Then A is a ring with identity where multiplication is given by function composition. Moreover, A is isomorphic (as an A-module over itself) to $\bigoplus_{i=1}^n A$ for every positive integer n.*

Proof. We first show that A is a ring with identity. First note that A has the structure of an abelian group where addition is defined pointwise: let $\varphi, \psi \in A$, then we define $\varphi + \psi \in A$ to be the K-linear map

$$(\varphi + \psi)(v) := \varphi(v) + \psi(v)$$

for all $v \in V$. Addition is associative and commutative since addition in V is associative and commutative. Moreover, the zero map $0 \colon V \to V$ defined by

$$0(v) = 0$$

for all $v \in V$ serves as the identity element. We claim that composition gives the abelian group A a ring structure. Indeed, let $\varphi, \psi, \phi \in A$ and let $v \in V$. Then

$$\begin{aligned} (\varphi \circ (\psi + \phi))(v) &= \varphi((\psi + \phi)(v)) \\ &= \varphi((\psi(v) + \phi(v)) \\ &= \varphi((\psi(v)) + \varphi(\phi(v)) \\ &= (\varphi \circ \psi)(v) + (\varphi \circ \phi)(v). \\ &= (\varphi \circ \psi + \varphi \circ \phi)(v) \end{aligned}$$

and

$$\begin{aligned}((\varphi+\psi)\circ\phi)(v) &= (\varphi+\psi)(\phi(v)) \\ &= \varphi(\phi(v))+\psi(\phi(v)) \\ &= (\varphi\circ\phi)(v)+(\psi\circ\phi)(v) \\ &= (\varphi\circ\phi+\psi\circ\phi)(v).\end{aligned}$$

and

$$\begin{aligned}(\varphi\circ(\psi\circ\phi))(v) &= \varphi((\psi\circ\phi)(v)) \\ &= \varphi(\psi(\phi(v))) \\ &= (\varphi\circ\psi)(\phi(v)) \\ &= ((\varphi\circ\psi)\circ\phi)(v)\end{aligned}$$

It follows that

$$\begin{aligned}\varphi\circ(\psi+\phi) &= \varphi\circ\psi+\varphi\circ\phi; \\ (\varphi+\psi)\circ\phi &= \varphi\circ\phi+\psi\circ\phi; \\ \varphi\circ(\psi\circ\phi) &= (\varphi\circ\psi)\circ\phi.\end{aligned}$$

Thus we have left and right distributivity as well as associativity. The identity map $1_V\colon V\to V$, given by $v\mapsto v$, serves as the identity element in A: all $v\in V$ and $\varphi\in A$, we have

$$\begin{aligned}(1_V\circ\varphi)(v) &= 1_V(\varphi(v)) \\ &= \varphi(v) \\ &= \varphi(1_V(v)) \\ &= (\varphi\circ 1_V)(v).\end{aligned}$$

It follows that

$$1_V\circ\varphi=\varphi=\varphi\circ 1_V$$

for all $\varphi\in A$, and hence 1_V is the identity element in A. This establishes our claim that A is a ring with identity.

Now we want to prove the "moreover" part of the proposition. First note that it suffices to show that $A\cong A\oplus A$. Indeed if this is the case, then an induction argument would gives us

$$\begin{aligned}A^n &= A\oplus A^{n-1} \\ &\cong A\oplus A \\ &\cong A.\end{aligned}$$

Let $\{e_i\}$ be a countable basis for V. Let $\psi_{\mathrm{o}}\colon V\to V$ and $\psi_{\mathrm{e}}\colon V\to V$ be the unique linear maps such that

$$\psi_{\mathrm{o}}(e_i)=\begin{cases}e_{(i+1)/2} & \text{if } i \text{ is odd.}\\ 0 & \text{if } i \text{ is even.}\end{cases} \qquad \text{and} \qquad \psi_{\mathrm{e}}(e_i)=\begin{cases}0 & \text{if } i \text{ is odd.}\\ e_{i/2} & \text{if } i \text{ is even.}\end{cases}$$

for all $i\in\mathbb{N}$. We claim that $\{\psi_{\mathrm{o}},\psi_{\mathrm{e}}\}$ is linearly independent and $\operatorname{span}\{\psi_{\mathrm{o}},\psi_{\mathrm{e}}\}=A$. This will imply $A\cong A\oplus A$.

Let us first show that $\{\psi_{\mathrm{o}},\psi_{\mathrm{e}}\}$ is linearly independent. Suppose we have the relation

$$\varphi_1\psi_{\mathrm{o}}+\varphi_2\psi_{\mathrm{e}}=0 \tag{318}$$

for some $\varphi_1,\varphi_2\in A$. If i is a positive odd integer, then applying e_i to both sides of (318) gives us

$$\varphi_1(e_{(i+1)/2})=0.$$

Similarly, if j is a positive even integer, then applying e_j to both sides of (318) gives us

$$\varphi_2(e_{j/2})=0.$$

Since every positive integer n can be expressed as $n=(i+1)/2$ and $n=j/2$ where i is a positive odd integer and j is a positive even integer, we see that

$$\varphi_1(e_n)=\varphi_2(e_n)=0$$

for all $n \in \mathbb{N}$. This implies $\varphi_1 = \varphi_2 = 0$. Thus $\{\psi_o, \psi_e\}$ is linearly independent.

Next we show that $\operatorname{span}\{\psi_o, \psi_e\} = A$. Let $\varphi \in A$ and define $\varphi_o \colon V \to V$ and $\varphi_e \colon V \to V$ be the unique linear maps such that

$$\varphi_o(e_n) = \varphi(e_{2n-1}) \qquad \text{and} \qquad \varphi_e(e_n) = \varphi(e_{2n})$$

for all $n \in \mathbb{N}$. Then if n is a positive odd integer, then we have

$$\begin{aligned}\varphi(e_n) &= \varphi_o(e_{(n+1)/2}) \\ &= \varphi_o(\psi_o(e_n)) \\ &= (\varphi_o\psi_o + \varphi_e\psi_e)(e_n),\end{aligned}$$

and if n is a positive even integer, then we have

$$\begin{aligned}\varphi(e_n) &= \varphi_e(e_{n/2}) \\ &= \varphi_e(\psi_e(e_n)) \\ &= (\varphi_o\psi_o + \varphi_e\psi_e)(e_n).\end{aligned}$$

Thus $\varphi = \varphi_o\psi_o + \varphi_e\psi_e$ since they agree on the basis $\{e_n\}$. □

76.4 Characterization of injective modules

Lemma 76.1. *Let E an R-module. The following statements are equivalent;*

1. *E is an injective R-module;*
2. *Every short exact sequence of the form*

$$0 \longrightarrow E \longrightarrow M \longrightarrow N \longrightarrow 0 \tag{319}$$

   splits.

3. *If E is a submodule of an R-module M, then E is a direct summand of M.*

Proof. ($2 \implies 1$) Assume that any short exact sequence of the form (363) splits. This means, equivalently, that any injective R-linear map out of E splits. Let $\varphi \colon M \to N$ be an injective R-linear map and let $\psi \colon M \to E$ be any R-linear map. We need to construct a map $\widetilde{\psi} \colon N \to E$ such that $\widetilde{\psi}\varphi = \psi$. To do this, consider the pushout module

$$E +_M N = (E \times N)/\{(\psi(u), -\varphi(u)) \mid u \in M\}$$

together its natural maps $\iota_1 \colon E \to E +_M N$ and $\iota_2 \colon N \to E +_M N$, given by

$$\iota_1(v) = [v, 0] \qquad \text{and} \qquad \iota_2(w) = [0, w]$$

for all $v \in E$ and $w \in N$ where $[v, w]$ denotes the equivalence class in $E +_M N$ with (v, w) as one of its representatives. Observe that

$$\begin{aligned}\iota_1(\psi(u)) &= [\psi(u), 0] \\ &= [0, \varphi(u)] \\ &= \iota_2(\varphi(u))\end{aligned}$$

for all $u \in M$. Therefore, we have a commutative diagram

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi"'] & N \arrow[d, "\iota_2"] \\ E \arrow[r, "\iota_1"'] & E +_M N \end{tikzcd}$$

We claim that ι_1 is injective. Indeed, suppose $v \in \ker \iota_1$. Then $[v, 0] = [0, 0]$ implies if $(v, 0) = (\psi(u), -\varphi(u))$ for some $u \in M$. Then $\varphi(u) = 0$ implies $u = 0$ since φ is injective, and therefore

$$\begin{aligned}v &= \psi(u) \\ &= \psi(0) \\ &= 0.\end{aligned}$$

Thus ι_1 is injective. Therefore by hypothesis the map $\iota_1 \colon E \to E +_M N$ splits, say by $\lambda \colon E +_M N \to E$, where $\lambda\iota_1 = 1_E$. Finally, we obtain a map $\widetilde{\psi} \colon N \to E$ by setting $\widetilde{\psi} := \lambda\iota_2$. Then

$$\begin{aligned} \widetilde{\psi}\varphi &= \lambda\iota_2\varphi \\ &= \lambda\iota_1\psi \\ &= \psi, \end{aligned}$$

shows that $\widetilde{\psi}$ has the desired property.

($1 \implies 2$) Assume that E is an injective R-module. Let $\varphi \colon E \to M$ be an injective homomorphism. Since E is an injective R-module and since $1_E \colon E \to E$ is an injective R-module homomorphism, there exists an R-linear map $\widetilde{\varphi} \colon M \to E$ such that $\widetilde{\varphi} \circ \varphi = 1_E$. That is, $\widetilde{\varphi}$ splits $\varphi \colon E \to M$.

($2 \implies 3$) Assume that any short exact sequence of the form (363) splits. Let M be an R-module such that $E \subseteq M$. Then the short exact sequence

$$0 \longrightarrow E \xrightarrow{\ \iota\ } M \xrightarrow{\ \pi\ } M/E \longrightarrow 0$$

splits, where $\iota \colon E \to M$ denotes the inclusion map and $\pi \colon M \to M/E$ denotes the quotient map. Therefore we may choose a $\widetilde{\pi} \colon M/E \to M$ such that $\pi\widetilde{\pi} = 1_{M/E}$. We claim that

$$M = E \oplus \widetilde{\pi}(M/E).$$

Indeed, they are both submodules of M. Furthermore, observe that we have $E \cap \widetilde{\pi}(M/E) = \{0\}$. Indeed, suppose $u \in E \cap \widetilde{\pi}(M/E)$. Then $u \in E$ implies $\pi(u) = 0$. Also $u \in \widetilde{\pi}(M/E)$ implies $u = \widetilde{\pi}(\overline{v})$ for some $\overline{v} \in M/E$. Therefore

$$\begin{aligned} 0 &= \widetilde{\pi}(0) \\ &= \widetilde{\pi}\pi(u) \\ &= \widetilde{\pi}\pi\widetilde{\pi}(\overline{v}) \\ &= \widetilde{\pi}(\overline{v}) \\ &= u. \end{aligned}$$

Finally, note that if $u \in M$, then we can write

$$u = u - \widetilde{\pi}\pi(u) + \widetilde{\pi}\pi(u),$$

where $\widetilde{\pi}\pi(u) \in \widetilde{\pi}(M/E)$ and where $u - \widetilde{\pi}\pi(u) \in E$ since

$$\begin{aligned} \pi(u - \widetilde{\pi}\pi(u)) &= \pi(u) - \pi\widetilde{\pi}\pi(u) \\ &= \pi(u) - \pi(u) \\ &= 0 \end{aligned}$$

implies $u - \widetilde{\pi}\pi(u) \in \ker \pi = E$. This implies $M = E + \widetilde{\pi}(M/E)$.

($3 \implies 2$) Assume that E satisfies the property that if E is a submodule of an R-module M, then it must be a direct summand of M. We show that any short exact sequence of the form (363) splits by showing that any injective R-linear map out of E splits.

Step 1: Before we show that any injective R-linear map out of E splits, we need to show that if $\varphi \colon E \to F$ is an isomorphism of R-modules, then F satisfies the same property as E; namely if N is an R-module such that $F \subseteq N$, then F is a direct summand of N. Let $\varphi \colon E \to F$ be an isomorphism, let $\psi \colon F \to E$ denote its inverse, and let N be an R-module such that $F \subseteq N$. We define an R-module $\psi(N)$, where as a set we have

$$\psi(N) = E \cup \{\psi(v) \mid v \in N \backslash F\},$$

where $\psi(v)$ is understood to be a formal symbol if $v \in N \backslash F$ and is understood to be an element in E if $v \in F$. Here, E is *literally* a subset of $\psi(N)$. We extend the R-linear structure on E to an R-linear structure on $\psi(N)$ by defining addition and scalar multiplication by

$$\psi(v_1) + \psi(v_2) = \psi(v_1 + v_2) \quad \text{and} \quad a\psi(v) = \psi(av).$$

for all $v, v_1, v_2 \in N \backslash F$ and $a \in R$. Defining the R-linear structure on $\psi(N)$ in this way makes it so that $\psi\colon F \to E$ and $\varphi\colon E \to F$ extends to an isomorphism $\psi\colon N \to \psi(N)$ with corresponding inverse $\varphi\colon \psi(N) \to N$.

With this construction in place, we see that E is *literally* a submodule of $\psi(N)$. Therefore $\psi(N)$ is an internal direct sum, say

$$\psi(N) = E \oplus K,$$

where K is another submodule of $\psi(N)$ such that $E \cap K = \{0\}$ and $E + K = \psi(N)$. Then since $\varphi\colon \psi(N) \to N$ is an isomorphism, we see that

$$\begin{aligned} N &= \varphi(E) \oplus \varphi(K) \\ &= F \oplus \varphi(K). \end{aligned}$$

Step 2: Now we will show that any injective R-linear map out of E splits. Let $\varphi\colon E \to M$ be any injective R-linear map. We claim that $\varphi\colon E \to M$ splits if and only if $\iota\colon \varphi(E) \to M$ splits, where ι denotes the inclusion map. Indeed, denote $\varphi^{-1}\colon E \to \varphi(E)$ to be the inverse of $\varphi\colon E \to \varphi(E)$. If $\varphi\colon E \to M$ splits, then there exists an R-linear map $\widetilde{\varphi}\colon M \to E$ such that $\widetilde{\varphi}\varphi = 1_E$. Then $\varphi\widetilde{\varphi}\colon M \to \varphi(E)$ splits $\iota\colon \varphi(E) \to M$ since

$$\begin{aligned} (\varphi\widetilde{\varphi}\iota)(\varphi(u)) &= \varphi\widetilde{\varphi}(\varphi(u)) \\ &= \varphi(\widetilde{\varphi}\varphi(u)) \\ &= \varphi(u) \end{aligned}$$

for all $\varphi(u) \in \varphi(E)$. Similarly, if $\iota\colon \varphi(E) \to M$ splits, then there exists an R-linear map $\widetilde{\iota}\colon M \to \varphi(E)$ such that $\widetilde{\iota}\iota = 1_{\varphi(E)}$. Then $\varphi^{-1}\widetilde{\iota}\colon M \to E$ splits $\varphi\colon E \to M$ since

$$\begin{aligned} (\varphi^{-1}\widetilde{\iota}\varphi)(u) &= (\varphi^{-1}\widetilde{\iota})(\varphi(u)) \\ &= (\varphi^{-1}\widetilde{\iota})(\iota\varphi(u)) \\ &= (\varphi^{-1}\widetilde{\iota}\iota)(\varphi(u)) \\ &= (\varphi^{-1})(\varphi(u)) \\ &= u \end{aligned}$$

for all $u \in E$.

Thus, to show that $\varphi\colon E \to M$ splits, it suffices to show that $\iota\colon \varphi(E) \to M$ splits. In this case, $\varphi(E)$ is a submodule of M, and by step 1, we see that M is an internal direct sum, say

$$M = \varphi(E) \oplus K$$

for some R-module $K \subseteq M$. The projection map $\pi_1\colon M \to \varphi(E)$ is easily seen to split the inclusion map $\iota\colon \varphi(E) \to M$. □

77 Homework 4

77.1 Divisible Modules

Definition 77.1. Let M be an R-module. We say M is **divisible** if $aM = M$ for every nonzerodivisor $a \in R$.

Problem 1.a

Proposition 77.1. *Let $\varphi\colon M \twoheadrightarrow N$ be a surjective map of R-modules and suppose M is divisible. Then N is divisible.*

Proof. Let $a \in R$ be a nonzerodivisor and let $v \in N$. We must find a $v' \in N$ such that $av' = v$. It will then follow that $aN = N$, which will imply N is divisible. Since φ is surjective, we may choose a $u \in M$ such that $\varphi(u) = v$. Since M is divisible, we may choose a $u' \in M$ such that $au' = u$. Then setting $v' = \varphi(u')$, we have

$$\begin{aligned} av' &= a\varphi(u') \\ &= \varphi(au') \\ &= \varphi(u) \\ &= v. \end{aligned}$$

Thus N is divisible. □

Problem 1.b

Proposition 77.2. *Assume that R is a PID and let M be any R-module. Then M may be decomposed as $M = D \oplus N$ where D is divisible and N has no nontrivial divisible subgroups.*

Proof. We first argue using Zorn's Lemma that M contains a maximal divisible submdoule. Consider the partially ordered set $(\mathscr{F}, \subseteq)$, where $\mathscr{F}$ is the family of all divisible submodules of M:

$$\mathscr{F} = \{D \subseteq M \mid D \text{ is divisible submodule of } M\},$$

and where the partial order $\subseteq$ is set inclusion. Note that $\mathscr{F}$ is nonempty since the zero module is divisible. Let $\{D_i \mid i \in I\}$ be a totally ordered subset of $\mathscr{F}$. We claim that

$$\bigcup_{i \in I} D_i$$

is a divisible submodule of M, and hence an upper bound of $\{D_i \mid i \in I\}$.

To see this, we first show that $\bigcup_{i \in I} D_i$ is a submodule of M. Indeed, it is nonempty since $0 \in \bigcup_{i \in I} D_i$. Also, if $a \in R$ and $u, v \in \bigcup_{i \in I} D_i$, then there exists an $i \in I$ such that $u, v \in D_i$ since $\{D_i \mid i \in I\}$ is totally ordered, and so

$$au + v \in D_i \subseteq \bigcup_{i \in I} D_i.$$

Thus $\bigcup_{i \in I} D_i$ is a submodule of M.

Now we show that $\bigcup_{i \in I} D_i$ is divisible. Let a be a nonzero divisor in R and let u be an element in $\bigcup_{i \in I} D_i$. Then there exists an $i \in I$ such that $u \in D_i$, and as D_i is divisible, there exists a

$$v \in D_i \in \bigcup_{i \in I} D_i$$

such that $av = u$. It follows that $\bigcup_{i \in I} D_i$ is divisible.

Thus the conditions for Zorn's Lemma are satisfied and so there exists a maximal divisible submodule of M, say $D \subseteq M$. Since every divisible module over a PID is injective[14], we see that D is injective, and thus we have a direct sum decomposition of M say

$$M = D \oplus N$$

where N is a submodule of M. To finish the proof, assume for a contradiction that N has a nontrivial divisible submodule, say $L \subseteq N$. We claim that $D + L$ is a divisible submodule of M which properly contains D. Indeed, it is divisible since if $a \in R$ is a nonzerodivisor and $x + y \in D + L$ where $x \in D$ and $y \in L$, then we can choose $u \in D$ and $v \in L$ such that $au = x$ and $av = y$ since D and L are divisible, and so

$$\begin{aligned} a(u+v) &= au + av \\ &= x + y \end{aligned}$$

implies $D + L$ is divisible. It also properly contains D since $L \subseteq N$ is nontrivial. Thus $D + L$ is a divisible submodule of M which properly contains D. This is a contradiction as D was chosen to be a maximal divisible submodule of M. □

Problem 1.c

Proposition 77.3. *Assume that R is a PID. Then any R-module can be embedded into an R-module which is divisible.*

Proof. Any R-module can be embedded into an injective R-module and every injective R-module is divisible by Proposition (77.9) (this is proved in the Appendix). □

77.2 Hom left exactness

Proposition 77.4. *The sequence of R-modules*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0 \tag{320}$$

is exact if and only if for all R-modules N the induced sequence

$$0 \longrightarrow \mathrm{Hom}_R(M_3, N) \xrightarrow{\varphi_2^*} \mathrm{Hom}_R(M_2, N) \xrightarrow{\varphi_1^*} \mathrm{Hom}_R(M_1, N) \tag{321}$$

is exact.

[14] For completeness, we included proof of this in the Appendix.

Proof. Suppose that (320) is exact and let N be any R-module. We first show exactness at $\mathrm{Hom}_R(M_3, N)$. Let $\psi_3 \in \ker \varphi_2^*$. Then

$$\begin{aligned} 0 &= \varphi_2^*(\psi_3) \\ &= \psi_3\varphi_2 \\ &= \psi_3, \end{aligned}$$

where we used the fact that φ_2 is surjective to obtain the third line from the second line. Therefore φ_2^* is injective, which implies exactness at $\mathrm{Hom}_R(M_3, N)$.

Next we show exactness at $\mathrm{Hom}_R(M_2, N)$. Let $\psi_2 \in \ker \varphi_1^*$. Then

$$\begin{aligned} 0 &= \varphi_1^*(\psi_2) \\ &= \psi_2\varphi_1 \end{aligned}$$

implies ψ_2 kills the image of φ_1. We define $\psi_3 \colon M_3 \to N$ as follows: let $u_3 \in M_3$. Choose $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ (such a choice is possible since φ_2 is surjective). We define

$$\psi_3(u_3) = \psi_2(u_2).$$

The map ψ_3 is well-defined since ψ_2 kills the image of φ_1. Indeed, if $v_2 \in M_2$ was another lift of u_3 under φ_2, then

$$\begin{aligned} v_2 - u_2 &\in \ker \varphi_2 \\ &= \mathrm{im}\, \varphi_1. \end{aligned}$$

Thus

$$\begin{aligned} \psi_2(v_2) &= \psi_2(v_2 - u_2 + u_2) \\ &= \psi_2(v_2 - u_2) + \psi_2(u_2) \\ &= \psi_2(u_2). \end{aligned}$$

Thus the map ψ_3 is well-defined. The map ψ_3 is also R-linear. Indeed, let $a, b \in R$ and let $u_3, v_3 \in M_3$. Choose lifts of u_3, v_3 under φ_2, say $u_2, v_2 \in M_2$ (so $\varphi_2(u_2) = u_3$ and $\varphi(v_2) = v_3$). Then $au_2 + bv_2$ is easily seen to be a lift of $au_3 + bv_3$ under φ and so we have

$$\begin{aligned} \psi_3(au_3 + bv_3) &= \psi_2(au_2 + bv_2) \\ &= a\psi_2(u_2) + b\psi_2(v_2) \\ &= a\psi_3(u_3) + b\psi_3(v_3). \end{aligned}$$

Thus ψ_3 is R-linear. Finally, observe that

$$\begin{aligned} \varphi_2^*(\psi_3)(u_2) &= (\psi_3\varphi_2)(u_2) \\ &= \psi_3(\varphi_2(u_2)) \\ &= \psi_3(u_3) \\ &= \psi_2(u_2) \end{aligned}$$

for all $u_2 \in M_2$. It follows that $\psi_2 = \varphi_2^*(\psi_3)$, and hence $\psi_2 \in \mathrm{im}\, \varphi_2^*$. Therefore we have exactness at $\mathrm{Hom}_R(M_2, N)$.

Conversely, suppose that (320) is exact for all R-modules N. We first show φ_2 is surjective. Set $N = M_3/\mathrm{im}\, \varphi_2$ and let $\pi \colon M_3 \to M_3/\mathrm{im}\, \varphi_2$ be the quotient map. Observe that

$$\begin{aligned} \varphi_2^*(\pi) &= \pi\varphi_2 \\ &= 0 \\ &= \varphi_2^*(0). \end{aligned}$$

It follows from injectivity of φ_2^* that $\pi = 0$. In other words, $M_3 = \mathrm{im}\, \varphi_2$, hence φ_2 is surjective.

Next we show exactness at M_2. First set $N = M_3$. Then exactness of (320) implies

$$\begin{aligned} 0 &= (\varphi_1^*\varphi_2^*)(1_{M_3}) \\ &= (\varphi_1^*(\varphi_2^*(1_{M_3})) \\ &= \varphi_1^*(1_{M_3}\varphi_2) \\ &= 1_{M_3}\varphi_2\varphi_1 \\ &= \varphi_2\varphi_1. \end{aligned}$$

Thus $\ker \varphi_2 \supseteq \operatorname{im} \varphi_1$. For the reverse inclusion, set $N = M_2/\operatorname{im} \varphi_1$ and let $\pi \colon M_2 \to M_2/\operatorname{im} \varphi_1$ be the quotient map. Then

$$\begin{aligned} \varphi_1^*(\pi) &= \pi\varphi_1 \\ &= 0 \end{aligned}$$

implies there exists $\psi_3 \colon M_3 \to M_2/\operatorname{im} \varphi_1$ such that $\pi = \varphi_2^*(\psi_3)$ by exactness of (320). Thus, if $u_2 \in \ker \varphi_2$, then

$$\begin{aligned} 0 &= \psi_3(0) \\ &= \psi_3(\varphi_2(u_2)) \\ &= (\psi_3\varphi_2)(u_2) \\ &= (\varphi_2^*(\psi_3))(u_2) \\ &= \pi(u_2) \end{aligned}$$

implies $u_2 \in \operatorname{im} \varphi_1$. Thus $\ker \varphi_2 \subseteq \operatorname{im} \varphi_1$. $\square$

77.3 Hom

Problem 3.a

Proposition 77.5. *Let M be an R-module. Then*

$$\operatorname{Hom}_R(R/I, M) \cong 0 :_M I,$$

where

$$0 :_M I = \{u \in M \mid xm = 0 \text{ for all } x \in I\}.$$

Proof. We define $\Psi \colon \operatorname{Hom}_R(R/I, M) \to 0 :_M I$ by

$$\Psi(\varphi) = \varphi(\overline{1})$$

for all $\varphi \in \operatorname{Hom}_R(R/I, M)$. Note that Ψ lands in $0 :_M I$ since if $x \in I$, then

$$\begin{aligned} x\varphi(\overline{1}) &= \varphi(\overline{x}) \\ &= \varphi(\overline{0}) \\ &= 0. \end{aligned}$$

We claim that Ψ is an R-module isomorphism.

Let us first show that it is an R-linear map. Let $a, b \in R$ and let $\varphi, \psi \in \operatorname{Hom}_R(R/I, M)$. Then

$$\begin{aligned} \Psi(a\varphi + b\psi) &= (a\varphi + b\psi)(\overline{1}) \\ &= a\varphi(\overline{1}) + b\psi(\overline{1}) \\ &= a\Psi(\varphi) + b\Psi(\varphi). \end{aligned}$$

Thus Ψ is an R-linear map.

Next, we show that Ψ is bijective by constructing an inverse map. Define $\Phi \colon 0 :_M I \to \operatorname{Hom}_R(R/I, M)$ by

$$\Phi(u) = \varphi_u$$

for all $u \in 0 :_M I$, where $\varphi_u \colon R/I \to M$ is defined by

$$\varphi_u(\overline{a}) = au$$

for all $\overline{a} \in R/I$. Note that φ_u is well-defined here since if $a + x$ is another represenative of the coset $\overline{a}$ where $x \in I$, then

$$\begin{aligned} \varphi_u(\overline{a + x}) &= (a + x)u \\ &= au \\ &= \varphi_u(\overline{a}). \end{aligned}$$

Similarly, φ_u is easily checked to be R-linear. Thus Φ lands in $\mathrm{Hom}_R(R/I, M)$. Moreover, it is an inverse to Ψ since if $\varphi \in \mathrm{Hom}_R(R/I, M)$, then

$$\begin{aligned}
(\Phi\Psi)(\varphi) &= \Phi(\Psi(\varphi)) \\
&= \Phi(\varphi(\overline{1})) \\
&= \varphi_{\varphi(\overline{1})} \\
&= \varphi,
\end{aligned}$$

where the last equality follows from

$$\begin{aligned}
\varphi_{\varphi(\overline{1})}(\overline{a}) &= \overline{a}\varphi(\overline{1}) \\
&= \varphi(\overline{a})
\end{aligned}$$

for all $\overline{a} \in R/I$. Thus $\Phi\Psi = 1$.

Similarly, if $u \in 0 :_M I$, then

$$\begin{aligned}
(\Psi\Phi)(u) &= \Psi(\Phi(u)) \\
&= \Phi(\varphi_u)) \\
&= \varphi_u(\overline{1}) \\
&= u.
\end{aligned}$$

Thus $\Psi\Phi = 1$. □

Corollary 74. *Let A be an abelian group. Then*

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \cong A[m]$$

where $A[m] = \{a \in A \mid ma = 0\}$.

Proof. This follows from Proposition (77.5) by taking $R = \mathbb{Z}$, $M = A$, and $I = m\mathbb{Z}$. □

Problem 3.b

Proposition 77.6. *Let $m, n \in \mathbb{N}$ and let $d = \gcd(m, n)$. Then*

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$$

Proof. By Corollary (74), it suffices to show that $\mathbb{Z}/d\mathbb{Z} \cong 0 :_{\mathbb{Z}/n\mathbb{Z}} m\mathbb{Z}$. Indeed, since $0 :_{\mathbb{Z}/n\mathbb{Z}} m\mathbb{Z}$ is a submodule of $\mathbb{Z}/n\mathbb{Z}$, it must be equal to a module of the form $k\mathbb{Z}/n\mathbb{Z}$ where $n \mid k$. Define $\Psi\colon \mathbb{Z}/d\mathbb{Z} \to 0 :_{\mathbb{Z}/n\mathbb{Z}} m\mathbb{Z}$ by

$$\Psi(\overline{a}) = \overline{(n/d)a}.$$

for all $\overline{a} \in \mathbb{Z}/d\mathbb{Z}$.[15]We claim that Ψ gives the desired isomorphism. Indeed, we first need to show that Ψ is well-defined. Let $a + db$ is another representative of the coset $\overline{a}$. Then

$$\begin{aligned}
\Psi(\overline{a+db}) &= \overline{(n/d)(a+db)} \\
&= \overline{(n/d)a + nb} \\
&= \overline{(n/d)a} \\
&= \Psi(\overline{a}).
\end{aligned}$$

Thus Ψ is well-defined.

Next we need to show that Ψ lands in $0 :_{\mathbb{Z}/n\mathbb{Z}} m\mathbb{Z}$. Let $\overline{a} \in \mathbb{Z}/d\mathbb{Z}$. Then

$$\begin{aligned}
m\Psi(\overline{a}) &= m\overline{(n/d)a} \\
&= \overline{m(n/d)a} \\
&= \overline{(mn/d)a} \\
&= \overline{n(m/d)a} \\
&= \overline{0}.
\end{aligned}$$

[15]Our notation is a little ambiguous here in that we use the overline notation to denote a coset both in $\mathbb{Z}/d\mathbb{Z}$ and in $\mathbb{Z}/n\mathbb{Z}$. However we often do this in Mathematics in order to clean notation. For instance, we use the same $+$ symbol to denote addition in any abelian group. Context will always make it clear what our notation is referring to.

Thus Ψ lands in $0 :_{\mathbb{Z}/n\mathbb{Z}} m\mathbb{Z}$.

Finally, we show that Ψ is an isomorphism. Note that the map Ψ is $\mathbb{Z}$-linear since it is just the "multiplication by $n/d \in \mathbb{Z}$" map. It remains to show that Ψ is bijective. We first show it is injective. Let $\overline{a} \in \ker \Psi$. Then

$$\begin{aligned}\overline{0} &= \Psi(\overline{a}) \\ &= \overline{(n/d)a}\end{aligned}$$

implies

$$(n/d)a = nb \tag{322}$$

for some $n \in \mathbb{Z}$. Multiplying both sides of (322) by d gives us

$$\begin{aligned}dnb &= d(n/d)a \\ &= na,\end{aligned}$$

which imlpies $a = db$ since $\mathbb{Z}$ is an integral domain. Thus $\overline{a} = \overline{0}$ in $\mathbb{Z}/d\mathbb{Z}$, which implies Ψ is injective.

Now we show it is surjective. Before doing so, we first choose $x, y \in \mathbb{Z}$ such that

$$mx + ny = d.$$

Such a choice is possible since $d = \gcd(m, n)$. Now let $\overline{b} \in 0 :_{\mathbb{Z}/n\mathbb{Z}} m\mathbb{Z}$. Then $m\overline{b} = \overline{0}$ implies there exists a $c \in \mathbb{Z}$ such that

$$mb = nc$$

Then

$$\begin{aligned}b &= b((m/d)x + (n/d)y) \\ &= (bm/d)x + (n/d)by \\ &= (nc/d)x + (n/d)by \\ &= (n/d)cx + (n/d)by \\ &= (n/d)(cx + by).\end{aligned}$$

Therefore, setting $a = cx + by$, we see that

$$\begin{aligned}\Psi(\overline{a}) &= \overline{(n/d)a} \\ &= \overline{(n/d)(cx + by)} \\ &= \overline{b}.\end{aligned}$$

implies Ψ is surjective. □

77.4 Contravariant hom takes direct sums to products

Proposition 77.7. *Let M be an R-module, let I be an index set, and let N_i be an R-module for each $i \in I$. Then*

$$Hom_R\left(\bigoplus_{i \in I} N_i, M\right) \cong \prod_{i \in I} Hom_R(N_i, M)$$

Proof. For each $i \in I$, let $\iota_i \colon N_i \to \bigoplus_{i \in I} N_i$ denote the ith inclusion map. Define a map $\Psi \colon \mathrm{Hom}_R(\bigoplus_{i \in I} N_i, M) \to \prod_{i \in I} \mathrm{Hom}_R(N_i, M)$ by

$$\Psi(\varphi) = (\varphi|_{N_i}) = (\varphi \circ \iota_i)$$

for all $\varphi \in \mathrm{Hom}_R(\bigoplus_{i \in I} N_i, M)$. The map Ψ is R-linear as it is a composition of R-linear maps in each component. To see that it is an isomorphism, we construct an inverse map. Define a map $\Phi \colon \prod_{i \in I} \mathrm{Hom}_R(N_i, M) \to \mathrm{Hom}_R(\bigoplus_{i \in I} N_i, M)$ by

$$\Phi((\varphi_i))(y_{i_1} + \cdots + y_{i_n}) = \varphi_{i_1}(y_{i_1}) + \cdots + \varphi_{i_n}(y_{i_n})$$

for all $(\varphi_i) \in \prod_{i \in I} \mathrm{Hom}_R(N_i, M)$ and $y_{i_1} + \cdots + y_{i_n} \in \bigoplus_{i \in I} N_i$.

Let us check that Ψ is indeed the inverse to Φ. Let $\varphi \in \mathrm{Hom}_R(\bigoplus_{i \in I} N_i, M)$ and let $y_{i_1} + \cdots + y_{i_n} \in \bigoplus_{i \in I} N_i$. Then

$$\begin{aligned}(\Phi\Psi)(\varphi)(y_{i_1} + \cdots + y_{i_n}) &= \Phi(\varphi|_{N_i})(y_{i_1} + \cdots + y_{i_n}) \\ &= \varphi|_{N_{i_1}}(y_{i_1}) + \cdots + \varphi|_{N_{i_n}}(y_{i_n}) \\ &= \varphi(y_{i_1}) + \cdots + \varphi(y_{i_n}) \\ &= \varphi(y_{i_1} + \cdots + y_{i_n}).\end{aligned}$$

It follows that $\Phi\Psi = 1$.

Conversely, let $(\varphi_i) \in \prod_{i\in I} \mathrm{Hom}_R(N_i, M)$. Observe that for each $i \in I$, we have

$$(\Phi(\varphi_i) \circ \iota_i)(y) = \varphi_i(y)$$

for all $y \in N_i$. It follows that $\Phi(\varphi_i) \circ \iota_i = \varphi_i$. Therefore

$$\begin{aligned}(\Psi\Phi)((\varphi_i)) &= \Psi(\Phi(\varphi_i)) \\ &= (\Phi(\varphi_i) \circ \iota_i) \\ &= (\varphi_i).\end{aligned}$$

This implies $\Psi\Phi = 1$. □

77.5 Hom example

Example 77.1. Let R be a Noetherian integral domain, let I be a nonzero ideal, and let K be the field of fractions of R. For each $n \geq 1$, we have

$$\mathrm{Hom}_R(R/I^n, K) \cong 0.$$

To see this, we first show we cannot have $I^n = 0$ for any $n > 1$. Indeed, assume for a contradiction that $I^n = 0$ for some $n > 1$. Choose n to be minimal so that $I^{n-1} \neq 0$ and $I^n = 0$. Choose a nonzero element $x \in I$ and a nonzero element $y \in I^{n-1}$. Then $xy \in I^n = 0$ which implies $xy = 0$, contradicting the fact that R is an integral domain. Now let $m \geq 1$. Choose a nonzero element in $x \in I^m$ and suppose $\varphi \in \mathrm{Hom}_R(R/I^n, K)$. Let $\overline{a} \in R/I^n$. Then

$$\begin{aligned}x\varphi(\overline{a}) &= \varphi(x\overline{a}) \\ &= \varphi(\overline{xa}) \\ &= \varphi(0) \\ &= 0\end{aligned}$$

implies $\varphi(\overline{a}) = 0$ since $x \neq 0$ and K is the field of fractions of R. Thus $\varphi = 0$ and hence $\mathrm{Hom}_R(R/I^m, K) \cong 0$. Thus $\mathrm{Hom}_R(R/I^n, K) \cong 0$ for all $n \geq 1$, which implies

$$\prod_{n\geq 1} \mathrm{Hom}_R(R/I^m, K) \cong 0.$$

On the other hand, we claim that

$$\mathrm{Hom}_R\left(\prod_{n\geq 1} R/I^m, K\right) \ncong 0.$$

Indeed, consider the sequence element $(\overline{1}) \in \prod_{n\geq 1} R/I^m$ and let $a \in R$. Then

$$\begin{aligned}(\overline{a}) = (\overline{0}) &\iff a \in I^n \text{ for all } n \geq 1 \\ &\iff a \in \bigcap_{n\geq 1} I^n \\ &\iff a = 0\end{aligned}$$

where the last equality follows from the fact that $\bigcap_{n\geq 1} I^n = 0$ by Krull's Intersection Theorem. Therefore the map $\varphi\colon \mathrm{span}_R((\overline{1})) \to K$ given by

$$\varphi((\overline{a})) = a$$

for all $(\overline{a}) \in \mathrm{span}_R((\overline{1}))$ is a well-defined R-linear map. Since K is an injective R-module, we can extend this nonzero R-linear map to a nonzero R-linear map $\widetilde{\varphi} \in \mathrm{Hom}_R\left(\prod_{n\geq 1} R/I^m, K\right)$. Thus

$$\mathrm{Hom}_R\left(\prod_{n\geq 1} R/I^m, K\right) \ncong 0.$$

77.6 Every R-module is free if and only if R is a field

Proposition 77.8. *Every R-module is free if and only if R is a field.*

Proof. If R is a field, then an R-module is just an R-vector space. A standard argument using Zorn's Lemma tells us that every vector space has a basis, and hence every vector space is free.

Conversely, suppose that every R-module is free. Let I be a proper ideal in R. Then R/I is a nonzero free R-module, so there exists an $\overline{a} \in R/I$ such that

$$x\overline{a} = \overline{0}$$

implies $x = 0$ for all $x \in R$. In particular, if $x \in I$, then

$$\begin{aligned} x\overline{a} &= \overline{xa} \\ &= \overline{0} \end{aligned}$$

implies $x = 0$. Thus I must be the zero ideal. Therefore the only proper ideal of R is the zero ideal. This is equivalent to R being a field. □

Appendix

77.7 Baer's Criterion

Lemma 77.1. *Let E be an R-module. Then E is injective if and only if for every inclusion of R-modules $M \subset N$ and for every homomorphism $\psi\colon M \to E$ there exists a homomorphism $\widetilde{\psi}\colon N \to E$ such that $\widetilde{\psi}|_M = \psi$.*

Proof. One direction is obvious. To prove the other direction, let $\varphi\colon M \to N$ be an injective homomorphism of R-modules and let $\psi\colon M \to E$ be a homorphism. Since φ is injective, it induces an isomorphism $\varphi\colon M \to \varphi(M)$ of R-modules. Let φ^{-1} be the inverse homomorphism to this isomorphism. Then $\varphi(M) \subset N$ and $\psi\varphi^{-1}\colon \varphi(M) \to E$ is a homomorphism, and so by hypothesis, there exists $\widetilde{\psi}\colon N \to E$ such that $\widetilde{\psi}|_{\varphi(M)} = \psi\varphi^{-1}$. This implies

$$\begin{aligned} \widetilde{\psi}\varphi &= \widetilde{\psi}|_{\varphi(M)}\varphi \\ &= \psi\varphi^{-1}\varphi \\ &= \psi. \end{aligned}$$

Therefore E is injective. □

Theorem 77.2. *(Baer's Criterion) Let E be an R-module. Then E is injective if and only if for every ideal $I \subset R$ and for every homomorphism $\psi\colon I \to E$ there exists a morphism $\widetilde{\psi}\colon R \to E$ such that $\widetilde{\psi}|_I = \psi$.*

Proof. One direction is obvious. For the other direction, let $M \subset N$ be an inclusion of R-modules and let $\psi\colon M \to E$ be a homomorphism. Define the partially ordered set $(\mathscr{F}, \leq)$ where

$$\mathscr{F} := \{\psi'\colon M' \to N \mid M \subset M' \subset N \text{ and } \psi' \text{ extends } \psi\}.$$

and the where partial order $\leq$ is defined by

$$\psi' \leq \psi'' \text{ if and only if } \psi'' \text{ extends } \psi'.$$

If $\mathscr{T}$ is a totally ordered subset of $\mathscr{F}$, then it has an upper bound (namely we take the direct limit of a all $\psi' \in \mathscr{T}$). Therefore by Zorn's lemma, there is a homomorphism $\psi'\colon N' \to E$ with $M \subset N' \subset N$ which is maximal with respect to the property that ψ' extends ψ. We claim that $N' = N$. We will prove this by contradiciton: assume that $N' \neq N$. Choose an element $u \in N \backslash N'$ and consider the ideal

$$I = \{a \in R \mid au \in N'\}.$$

It is a nonempty proper ideal of R since $0 \in I$ and $1 \notin I$. By hypothesis, the composite

$$I \xrightarrow{\cdot u} N' \xrightarrow{\psi'} E$$

extends to a homomorphism $\widetilde{\psi}\colon R \to E$. Define $\psi''\colon N' + Ru \to E$ by the formula

$$\psi''(v + au) = \psi'(v) + \widetilde{\psi}(a)$$

for all $v + au \in N' + Rn$. To see that this is well-defined, suppose $v_1 + a_1 u$ and $v_2 + a_2 u$ represent the same element in $N' + Ru$. Then $v_2 - v_1 = (a_1 - a_2)u$ implies $a_1 - a_2 \in I$. Therefore $\widetilde{\psi}(a_1 - a_2) = \psi'((a_1 - a_2)u)$, and so

$$
\begin{aligned}
\psi''(v_2 + a_2 u) &= \psi'(v_2) + \widetilde{\psi}(a_2) \\
&= \psi'(v_2 - (v_2 - v_1))) + \widetilde{\psi}(a_1 + (a_2 - a_1)) \\
&= \psi'(v_2 + (a_1 - a_2)u) + \widetilde{\psi}(a_1 + (a_2 - a_1)) \\
&= \psi'(v_1) + \psi'((a_1 - a_2)u) + \widetilde{\psi}(a_1) + \psi'((a_2 - a_1)u) \\
&= \psi'(v_1) + \widetilde{\psi}(a_1).
\end{aligned}
$$

Thus ψ'' is well-defined. We also note that ψ'' extends ψ'. Since ψ' was maximal, this leads to a contradiction. So we must have $N' = N$. □

77.8 Divisible Modules Over a PID are Injective

Proposition 77.9. *Let M be an R-module. If M is injective, then M is divisible. The converse holds if R is a PID.*

Proof. Suppose M is injective and let $a \in R$ be a nonzerodivisor. Then the map $\varphi\colon M \to aM$, given by

$$\varphi(u) = au$$

for all $u \in M$ is an injective R-linear map. Thus we obtain a splitting map of φ, say $\psi\colon aM \to M$. Thus if $u \in M$, then we have

$$
\begin{aligned}
u &= (\psi\varphi)(u) \\
&= \psi(\varphi(u)) \\
&= \psi(au) \\
&= a\psi(u).
\end{aligned}
$$

This implies $M = aM$, that is, M is divisible.

For the converse direction, assume that R is a PID and that M is a divisible R-module. Let $\varphi\colon \langle x \rangle \to M$ be a homomorphism, where $\langle x \rangle$ is an ideal in R. Let $a \in R$ be a nonzerodivisor and set $u = \varphi(x)$. Since $M = xM$, we have $u = xv$ for some $v \in M$. Then the map $\widetilde{\varphi}\colon R \to M$, given by

$$\widetilde{\varphi}(a) = av$$

for all $a \in R$, extends φ. Indeed, it is clearly R-linear. Also

$$
\begin{aligned}
\widetilde{\varphi}(bx) &= (bx)v \\
&= b(xv) \\
&= bu \\
&= b\varphi(x) \\
&= \varphi(bx)
\end{aligned}
$$

for all $bx \in \langle x \rangle$. It follows from Baer's Criterion that M is injective. □

78 Homework 5

78.1 Localization

Problem 1.a

Definition 78.1. Let R be a commutative ring. A subset $S \subset R$ is called **multiplicatively closed** if $1 \in S$ and $s, t \in S$ implies $st \in S$.

Definition 78.2. Let S be a multiplicatively closed subset of R. We define the **localization of R with respect to** S, denoted R_S or $S^{-1}R$, as follows: as a set R_S is given by

$$R_S := \left\{ \frac{a}{s} \mid a \in R, s \in S \right\}$$

where a/s denotes the equivalence class of $(a,s) \in R \times S$ with respect to the following equivalence relation:

$$(a,s) \sim (a',s') \text{ if and only if there exists } s'' \in S \text{ such that } s''s'a = s''sa'. \tag{323}$$

We give R_S a ring structure by defining addition and multiplication on R_S by

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2a_1 + s_1a_2}{s_1s_2} \quad \text{and} \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1a_2}{s_1s_2}, \tag{324}$$

for a_1/s_1 and a_2/s_2 in R_S, where $1/1$ is the multiplicative identity element in R_S and $0/0$ is the additive identity in R_S. The ring R_S comes equipped with a natural ring homomoprhism $\rho_S \colon R \to R_S$, given by

$$\rho_S(a) = \frac{a}{1}$$

for all $a \in R$.

Proposition 78.1. *With the notation as above, R_S is a ring. Furthermore, $\rho_S \colon R \to R_S$ is a ring homomorphism.*

Proof. There are several things we need to check. We will break them into steps

Step 1: We show that the relation (143) is in fact a equivalence relation. First we show reflexivity of $\sim$. Let $(a,s) \in R \times S$. Then since $1 \in S$ and $1 \cdot sa = 1 \cdot sa$, we have $(a,s) \sim (a,s)$. Next we show symmetry of $\sim$. Suppose $(a,s) \sim (a',s')$. Choose $s'' \in S$ such that $s''s'a = s''sa'$. Then by symmetry of equality, we have $s''sa' = s''s'a$. Therefore $(a',s') \sim (a,s)$. Finally, we show transitivity of $\sim$. Suppose $(a_1,s_1) \sim (a_2,s_2)$ and $(a_2,s_2) \sim (a_3,s_3)$. Choose $s_{12}, s_{23} \in S$ such that

$$s_{12}s_2a_1 = s_{12}s_1a_2 \quad \text{and} \quad s_{23}s_3a_2 = s_{23}s_2a_3$$

Then $s_{23}s_{12}s_2 \in S$ and

$$\begin{aligned}
(s_{23}s_{12}s_2)(s_3a_1) &= s_{23}(s_{12}s_2a_1)s_3 \\
&= s_{23}(s_{12}s_1a_2)s_3 \\
&= s_{12}s_1(s_{23}s_3a_2) \\
&= s_{12}s_1(s_{23}s_2a_3) \\
&= (s_{12}s_{23}s_2)(s_1a_3).
\end{aligned}$$

Thus $\sim$ is in fact an equivalence relation.

Step 2: Addition and multiplication defined in (144) are well-defined. Suppose $a_1/s_1 = a_1'/s_1'$ and $a_2/s_2 = a_2'/s_2'$. Choose $s_1'', s_2'' \in S$ such that

$$s_1''s_1'a_1 = s_1''s_1a_1' \quad \text{and} \quad s_2''s_2'a_2 = s_2''s_2a_2'.$$

Then $s_1''s_2'' \in S$ and

$$\begin{aligned}
s_1''s_2''(s_2a_1 + s_1a_2)s_1's_2' &= s_2''s_2(s_1''s_1'a_1)s_2' + s_1''s_1(s_2''s_2'a_2)s_1' \\
&= s_2''s_2(s_1''s_1a_1')s_2' + s_1''s_1(s_2''s_2a_2')s_1' \\
&= s_2''s_2(s_1''s_1a_1')s_2' + s_1''s_1(s_2''s_2a_2')s_1' \\
&= s_1''s_2''(s_2'a_1' + s_1'a_2')s_1s_2
\end{aligned}$$

implies

$$\frac{s_2a_1 + s_1a_2}{s_1s_2} = \frac{s_2'a_1' + s_1'a_2'}{s_1's_2'}.$$

Similarly, $s_1''s_2'' \in S$ and

$$\begin{aligned}
s_1''s_2''a_1a_2s_1's_2' &= (s_1''s_1'a_1)(s_2''s_2'a_2) \\
&= (s_1''s_1a_1')(s_2''s_2a_2') \\
&= s_1''s_2''a_1'a_2's_1s_2
\end{aligned}$$

implies

$$\frac{a_1a_2}{s_1s_2} = \frac{a_1'a_2'}{s_1's_2'}.$$

Thus we have shown that addition and multiplication in (144) are well-defined.

Step 3: Now we show that addition and multiplication in (144) gives us a ring structure. First let us show that addition in (144) gives us an abelian group with $0/1$ being the additive identity. We begin by checking associativity. Let $a_1/s_1, a_2/s_2, a_3/s_3 \in R_S$. Then

$$\begin{aligned}
\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}\right) + \frac{a_3}{s_3} &= \frac{s_2a_1 + s_1a_2}{s_1s_2} + \frac{a_3}{s_3} \\
&= \frac{s_3(s_2a_1 + s_1a_2) + (s_1s_2)a_3}{(s_1s_2)s_3} \\
&= \frac{s_3(s_2a_1) + s_3(s_1a_2) + (s_1s_2)a_3}{s_1(s_2s_3)} \\
&= \frac{(s_2s_3)a_1 + s_1(s_3a_2) + s_1(s_2a_3)}{s_1(s_2s_3)} \\
&= \frac{(s_2s_3)a_1 + s_1(s_3a_2 + s_2a_3)}{s_1(s_2s_3)} \\
&= \frac{a_1}{s_1} + \frac{s_3a_2 + s_2a_3}{s_2s_3} \\
&= \frac{a_1}{s_1} + \left(\frac{a_2}{s_2} + \frac{a_3}{s_3}\right).
\end{aligned}$$

Thus addition in (144) is associative. Now we check commutativity. Let $a_1/s_1, a_2/s_2 \in R_S$. Then

$$\begin{aligned}
\frac{a_1}{s_1} + \frac{a_2}{s_2} &= \frac{s_2a_1 + s_1a_2}{s_1s_2} \\
&= \frac{s_1a_2 + s_2a_1}{s_2s_1} \\
&= \frac{a_2}{s_2} + \frac{a_1}{s_1}.
\end{aligned}$$

Thus addition in (144) is commutative. Now we check that $0/1$ is the identity. Let $a/s \in R_S$. Then

$$\begin{aligned}
\frac{0}{1} + \frac{a}{s} &= \frac{s \cdot 0 + 1 \cdot a}{1 \cdot s} \\
&= \frac{0 + a}{s} \\
&= \frac{a}{s}.
\end{aligned}$$

Thus addition in (144) is commutative. Thus $0/1$ is the identity. Finally we check that every element has an inverse. Let $a/s \in R_S$. Then

$$\begin{aligned}
\frac{a}{s} + \frac{-a}{s} &= \frac{a - a}{s} \\
&= \frac{0}{s} \\
&= \frac{0}{1}.
\end{aligned}$$

implies $-a/s$ is the inverse to a/s. Therefore $(R_S, +)$ forms an abelian group with $0/1$ being identity element.

Now let us show that $(R_S, +, \cdot)$ is a ring. We first check that multiplication in (144) is associative. Let

$a_1/s_1, a_2/s_2, a_3/s_3 \in R_S$. Then

$$\begin{aligned}\left(\frac{a_1}{s_1}\frac{a_2}{s_2}\right)\frac{a_3}{s_3} &= \frac{a_1a_2}{s_1s_2}\frac{a_3}{s_3} \\ &= \frac{(a_1a_2)a_3}{(s_1s_2)s_3} \\ &= \frac{a_1(a_2a_3)}{s_1(s_2s_3)} \\ &= \frac{a_1}{s_1}\frac{a_2a_3}{s_2s_3} \\ &= \frac{a_1}{s_1}\left(\frac{a_2}{s_2}\frac{a_3}{s_3}\right).\end{aligned}$$

Therefore multiplication in (144) is associative. Next we check that multiplication in (144) distributes over addition. Let $a_1/s_1, a_2/s_2, a_3/s_3 \in R_S$. Then

$$\begin{aligned}\frac{a_1}{s_1}\left(\frac{a_2}{s_2}+\frac{a_3}{s_3}\right) &= \frac{a_1}{s_1}\left(\frac{s_3a_2+s_2a_3}{s_2s_3}\right) \\ &= \frac{a_1(s_3a_2+s_2a_3)}{s_1s_2s_3} \\ &= \frac{a_1s_3a_2+a_1s_2a_3}{s_1s_2s_3} \\ &= \frac{s_3a_1a_2+s_2a_1a_3}{s_1s_2s_3} \\ &= \frac{s_3a_1a_2}{s_1s_2s_3}+\frac{s_2a_1a_3}{s_1s_2s_3} \\ &= \frac{a_1a_2}{s_1s_2}+\frac{a_1a_3}{s_1s_3} \\ &= \frac{a_1}{s_1}\frac{a_2}{s_2}+\frac{a_1}{s_1}\frac{a_3}{s_3}\end{aligned}$$

Thus multiplication in (144) distributes over addition. Finally, let us check that $1/1$ is the identity element in R_S under multplication. Let $a/s \in R_S$. Then

$$\begin{aligned}\frac{1}{1}\cdot\frac{a}{s} &= \frac{1\cdot a}{1\cdot s} \\ &= \frac{a}{s}.\end{aligned}$$

Thus $1/1$ is the identity element in R_S under multiplication.

Step 4: For the final step, we prove that $\rho_S\colon R \to R_S$ is a ring homomorphism. First note that it sends the identity to the identity. Next, let $a, b \in R$. Then

$$\begin{aligned}\rho_S(a+b) &= \frac{a+b}{1} \\ &= \frac{1\cdot a+1\cdot b}{1\cdot 1} \\ &= \frac{a}{1}+\frac{b}{1} \\ &= \rho_S(a)+\rho_S(b)\end{aligned}$$

and

$$\begin{aligned}\rho_S(ab) &= \frac{ab}{1} \\ &= \frac{ab}{1\cdot 1} \\ &= \frac{a}{1}\cdot\frac{b}{1} \\ &= \rho_S(a)\rho_S(b).\end{aligned}$$

Thus ρ_S is a ring homomorphism. $\square$

Definition 78.3. Let S be a multiplicatively closed subset of R and let M be an R-module. We define the **localization of M with respect to S**, denoted M_S or $S^{-1}M$, as follows: as a set M_S is given by

$$M_S := \left\{ \frac{u}{s} \mid u \in M, s \in S \right\}$$

where u/s denotes the equivalence class of $(u,s) \in M \times S$ with respect to the following equivalence relation:

$$(u,s) \sim (u',s') \text{ if and only if there exists } s'' \in S \text{ such that } s''s'u = s''su'. \tag{325}$$

We give M_S an R_S-module structure by ring defining addition and scalar multiplication on M_S by

$$\frac{u_1}{s_1} + \frac{u_2}{s_2} = \frac{s_2u_1 + s_1u_2}{s_1s_2} \quad \text{and} \quad \frac{a}{s}\frac{u}{t} = \frac{au}{st}, \tag{326}$$

for $u_1/s_1, u_2/s_2, u/t \in M_S$ and $a/s \in R_S$, with $0/0$ being the additive identity in M_S.

Proposition 78.2. *With the notation above, M_S is an R_S-module. By restricting scalars via the ring the homomoprhism $\rho_S \colon R \to R_S$, it is also an R-module. More specifically, the R-module scalar multiplication is given by*

$$a \cdot \frac{u}{s} = \frac{au}{s}$$

for all $a \in R$ and $u/s \in M_S$.

Proof. The proof of this is similar to the proof of (78.1), but we include it here for completeness. Again, there are several things we need to check, so we break it up into steps.

Step 1: We show that the relation (143) is in fact a equivalence relation. First we show reflexivity of $\sim$. Let $(u,s) \in M \times S$. Then since $1 \in S$ and $1 \cdot su = 1 \cdot su$, we have $(u,s) \sim (u,s)$. Next we show symmetry of $\sim$. Suppose $(u,s) \sim (u',s')$. Choose $s'' \in S$ such that $s''s'u = s''su'$. Then by symmetry of equality, we have $s''su' = s''s'u$. Therefore $(u',s') \sim (u,s)$. Finally, we show transitivity of $\sim$. Suppose $(u_1,s_1) \sim (u_2,s_2)$ and $(u_2,s_2) \sim (u_3,s_3)$. Choose $s_{12}, s_{23} \in S$ such that

$$s_{12}s_2u_1 = s_{12}s_1u_2 \quad \text{and} \quad s_{23}s_3u_2 = s_{23}s_2u_3$$

Then $s_{23}s_{12}s_2 \in S$ and

$$\begin{aligned}
(s_{23}s_{12}s_2)(s_3u_1) &= s_{23}(s_{12}s_2u_1)s_3 \\
&= s_{23}(s_{12}s_1u_2)s_3 \\
&= s_{12}s_1(s_{23}s_3u_2) \\
&= s_{12}s_1(s_{23}s_2u_3) \\
&= (s_{12}s_{23}s_2)(s_1u_3).
\end{aligned}$$

Thus $\sim$ is in fact an equivalence relation.

Step 2: Addition and multiplication in (147) are well-defined. Suppose $u_1/s_1 = u_1'/s_1'$ and $u_2/s_2 = u_2'/s_2'$. Choose $s_1'', s_2'' \in S$ such that

$$s_1''s_1'u_1 = s_1''s_1u_1' \quad \text{and} \quad s_2''s_2'u_2 = s_2''s_2u_2'.$$

Then $s_1''s_2'' \in S$ and

$$\begin{aligned}
s_1''s_2''(s_2u_1 + s_1u_2)s_1's_2' &= s_2''s_2(s_1''s_1'u_1)s_2' + s_1''s_1(s_2''s_2'u_2)s_1' \\
&= s_2''s_2(s_1''s_1u_1')s_2' + s_1''s_1(s_2''s_2u_2')s_1' \\
&= s_2''s_2(s_1''s_1u_1')s_2' + s_1''s_1(s_2''s_2u_2')s_1' \\
&= s_1''s_2''(s_2'u_1' + s_1'u_2')s_1s_2
\end{aligned}$$

implies

$$\frac{s_2u_1 + s_1u_2}{s_1s_2} = \frac{s_2'u_1' + s_1'u_2'}{s_1's_2'}.$$

Similarly, $s_1''s_2'' \in S$ and

$$\begin{aligned}
s_1''s_2''u_1u_2s_1's_2' &= (s_1''s_1'u_1)(s_2''s_2'u_2) \\
&= (s_1''s_1u_1')(s_2''s_2u_2') \\
&= s_1''s_2''u_1'u_2's_1s_2
\end{aligned}$$

implies

$$\frac{a_1a_2}{s_1s_2} = \frac{a_1'a_2'}{s_1's_2'}.$$

Thus we have shown that addition and scalar multiplication in (147) are well-defined.

Step 3: Now we show that addition and multiplication in (147) gives us an R_S-module structure. First let us show that addition in (147) gives us an abelian group with $0/1$ being the additive identity. We begin by checking associativity. Let $u_1/s_1, u_2/s_2, u_3/s_3 \in M_S$. Then

$$\begin{aligned}
\left(\frac{u_1}{s_1} + \frac{u_2}{s_2}\right) + \frac{u_3}{s_3} &= \frac{s_2u_1 + s_1u_2}{s_1s_2} + \frac{u_3}{s_3} \\
&= \frac{s_3(s_2u_1 + s_1u_2) + (s_1s_2)u_3}{(s_1s_2)s_3} \\
&= \frac{s_3(s_2u_1) + s_3(s_1u_2) + (s_1s_2)u_3}{s_1(s_2s_3)} \\
&= \frac{(s_2s_3)u_1 + s_1(s_3u_2) + s_1(s_2u_3)}{s_1(s_2s_3)} \\
&= \frac{(s_2s_3)u_1 + s_1(s_3u_2 + s_2u_3)}{s_1(s_2s_3)} \\
&= \frac{u_1}{s_1} + \frac{s_3u_2 + s_2u_3}{s_2s_3} \\
&= \frac{u_1}{s_1} + \left(\frac{u_2}{s_2} + \frac{u_3}{s_3}\right).
\end{aligned}$$

Thus addition in (147) is associative. Now we check commutativity. Let $u_1/s_1, u_2/s_2 \in M_S$. Then

$$\begin{aligned}
\frac{u_1}{s_1} + \frac{u_2}{s_2} &= \frac{s_2u_1 + s_1u_2}{s_1s_2} \\
&= \frac{s_1u_2 + s_2u_1}{s_2s_1} \\
&= \frac{u_2}{s_2} + \frac{u_1}{s_1}.
\end{aligned}$$

Thus addition in (147) is commutative. Now we check that $0/1$ is the identity. Let $u/s \in M_S$. Then

$$\begin{aligned}
\frac{0}{1} + \frac{u}{s} &= \frac{s \cdot 0 + 1 \cdot u}{1 \cdot s} \\
&= \frac{0 + u}{s} \\
&= \frac{u}{s}.
\end{aligned}$$

Thus $0/1$ is the identity. Finally we check that every element has an inverse. Let $u/s \in M_S$. Then

$$\begin{aligned}
\frac{u}{s} + \frac{-u}{s} &= \frac{u - u}{s} \\
&= \frac{0}{s} \\
&= \frac{0}{1}.
\end{aligned}$$

implies $-u/s$ is the inverse to u/s. Therefore $(M_S, +)$ forms an abelian group with $0/1$ being the identity element.

Now let us show that $(M_S, +, \cdot)$ is an R_S-module. We first check that scalar multiplication in (147) is associative.

Let $a_1/s_1, a_2/s_2 \in R_S$ and let $u/s \in M_S$. Then

$$\begin{aligned}
\left(\frac{a_1}{s_1}\frac{a_2}{s_2}\right)\frac{u}{s} &= \frac{a_1 a_2}{s_1 s_2}\frac{u}{s} \\
&= \frac{(a_1 a_2)u}{(s_1 s_2)s} \\
&= \frac{a_1(a_2 u)}{s_1(s_2 s)} \\
&= \frac{a_1}{s_1}\frac{a_2 u}{s_2 s} \\
&= \frac{a_1}{s_1}\left(\frac{a_2}{s_2}\frac{u}{s}\right).
\end{aligned}$$

Therefore scalar multiplication in (147) is associative. Next we check that scalar multiplication in (147) distributes over addition. Let $a/s \in R_S$ and $u_1/s_1, u_2/s_2 \in M_S$. Then

$$\begin{aligned}
\frac{a}{s}\left(\frac{u_1}{s_1}+\frac{u_2}{s_2}\right) &= \frac{a}{s}\left(\frac{s_2 u_1 + s_1 u_2}{s_1 s_2}\right) \\
&= \frac{a(s_2 u_1 + s_1 u_2)}{s s_1 s_2} \\
&= \frac{a s_2 u_1 + a s_1 u_2}{s s_1 s_2} \\
&= \frac{s_2 a u_1 + s a u_2}{s s_1 s_2} \\
&= \frac{s_2 a u_1}{s s_1 s_2} + \frac{s a u_2}{s s_1 s_2} \\
&= \frac{a u_1}{s s_1} + \frac{a u_2}{s s_2} \\
&= \frac{a}{s}\frac{u_1}{s_1} + \frac{a}{s}\frac{u_2}{s_2}.
\end{aligned}$$

Similarly, let $a_1/s_1, a_2/s_2 \in R_S$ and $u/s \in M_S$. Then

$$\begin{aligned}
\left(\frac{a_1}{s_1}+\frac{a_2}{s_2}\right)\frac{u}{s} &= \left(\frac{s_2 a_1 + s_1 a_2}{s_1 s_2}\right)\frac{u}{s} \\
&= \frac{(s_2 a_1 + s_1 a_2)u}{s_1 s_2 s} \\
&= \frac{s_2 a_1 u + s_1 a_2 u}{s_1 s_2 s} \\
&= \frac{s_2 a_1 u + s_1 a_2 u}{s_2 s_1 s} \\
&= \frac{s_2 a_1 u}{s_2 s_1 s} + \frac{s_1 a_2 u}{s_1 s_2 s} \\
&= \frac{a_1 u}{s_1 s} + \frac{a_2 u}{s_2 s} \\
&= \frac{a_1}{s_1}\frac{u}{s} + \frac{a_2}{s_2}\frac{u}{s}.
\end{aligned}$$

Thus multiplication in (147) distributes over addition. Finally, let us check that $1/1$ fixes M_S. Let $u/s \in M_S$. Then

$$\begin{aligned}
\frac{1}{1}\cdot\frac{u}{s} &= \frac{1\cdot u}{1\cdot s} \\
&= \frac{u}{s}.
\end{aligned}$$

Thus $1/1$ fixes M_S. □

Problem 1.b

Lemma 78.1. *Let N be an R-module. Every element in $R_S \otimes_R N$ can be expressed as an elementary tensor of the form $(1/s) \otimes v$ with $s \in S$ and $v \in N$.*

Proof. Let $\sum_{i=1}^{n}(a_i/s_i)\otimes v_i$ be a general tensor in $R_S\otimes_R N$. Then

$$\begin{aligned}
\frac{a_1}{s_1}\otimes v_1+\cdots+\frac{a_n}{s_n}\otimes v_n &= \frac{a_1s_2\cdots s_n}{s_1s_2\cdots s_n}\otimes v_1+\cdots+\frac{s_1s_2\cdots a_n}{s_1s_2\cdots s_n}\otimes v_n\\
&= \frac{1}{s_1s_2\cdots s_n}\otimes a_1s_2\cdots s_nv_1+\cdots+\frac{1}{s_1s_2\cdots s_n}\otimes s_1s_2\cdots a_nv_n\\
&= \frac{1}{s_1s_2\cdots s_n}\otimes (a_1s_2\cdots s_nv_1+\cdots+s_1s_2\cdots a_nv_n)\\
&= \frac{1}{s}\otimes v,
\end{aligned}$$

where $s=s_1s_2\cdots s_n$ and $v=a_1s_2\cdots s_nv_1+\cdots+s_1s_2\cdots a_nv_n$. □

Problem 1.c

Proposition 78.3. *Let S be a multiplicatively closed subset of R. Then we have a natural isomorphism between functors*

$$R_S\otimes_R -\colon \mathbf{Mod}_R\to\mathbf{Mod}_{R_S}\quad \textit{and}\quad -_S\colon \mathbf{Mod}_R\to\mathbf{Mod}_{R_S}$$

Proof. For each R-module M, we define $\eta_M\colon R_S\otimes_R M\to M_S$ by

$$\eta_M\left(\frac{1}{s}\otimes u\right)=\frac{u}{s}$$

for all $(1/s)\otimes u\in R_S\otimes_R M$. Every tensor in $R_S\otimes_R M$ can be expressed as an elementary tensor of the form $(1/s)\otimes u$, and so η_M really is defined on all of $R_S\otimes M$. Also η_M is a well-defined R-linear map since the map $R_S\times M\to M_S$ given by

$$\left(\frac{1}{s},u\right)\mapsto\frac{u}{s}$$

is readily seen to be R-bilinear. The map η_M is surjective since every element in M_S can be expressed in the form u/s. Let us show that η_M is injective. Suppose $(1/s)\otimes u\in\ker\eta_M$. Then $u/s=0$. Thus there exists a $t\in S$ such that

$$\begin{aligned}
tu &= ts\cdot 0\\
&= 0.
\end{aligned}$$

Then this implies

$$\begin{aligned}
\frac{1}{s}\otimes u &= \frac{t}{st}\otimes u\\
&= \frac{1}{st}\otimes tu\\
&= \frac{1}{st}\otimes 0\\
&= 0.
\end{aligned}$$

Thus η_M is injective, and hence an isomorphism.

Now we will show that η is a natural transformation. Let $\varphi\colon M\to N$ be an R-linear map. We need to show that the diagram below commutes

$$\begin{tikzcd}
R_S\otimes_R M \arrow[r, "\eta_M"] \arrow[d, "1\otimes\varphi"'] & M_S \arrow[d, "\varphi_S"] \\
R_S\otimes_R N \arrow[r, "\eta_N"'] & N_S
\end{tikzcd} \tag{327}$$

Let $(1/s) \otimes u \in R_S \otimes_R M$. Then

$$\begin{aligned}
(\varphi_S \eta_M)\left(\frac{1}{s} \otimes u\right) &= \varphi_S\left(\eta_M\left(\frac{1}{s} \otimes u\right)\right) \\
&= \varphi_S\left(\frac{u}{s}\right) \\
&= \frac{\varphi(u)}{s} \\
&= \eta_N\left(\frac{1}{s} \otimes \varphi(u)\right) \\
&= \eta_N\left((1 \otimes \varphi)\left(\frac{1}{s} \otimes u\right)\right) \\
&= (\eta_N(1 \otimes \varphi))\left(\frac{1}{s} \otimes u\right).
\end{aligned}$$

Therefore the diagram (327) commutes. □

Problem 1.d

Corollary 75. *Let $(1/s) \otimes v$ be a tensor in $R_S \otimes_R N$. Then $(1/s) \otimes v = 0$ if and only if there exists a $t \in S$ such that $tv = 0$.*

Proof. We have

$$\begin{aligned}
\frac{1}{s} \otimes v = 0 &\iff \eta_N\left(\frac{1}{s} \otimes v\right) = 0 \\
&\iff \frac{v}{s} = 0 \\
&\iff \text{there exists a } t \in S \text{ such that } tv = 0.
\end{aligned}$$

□

Problem 1.e

Proposition 78.4. *Let S be a multiplicatively closed subset of R. Then R_S is a flat R-module.*

Proof. Let $\varphi\colon M \to N$ be an injective R-linear map. We must show that $1 \otimes \varphi\colon R_S \otimes_R M \to R_S \otimes_R N$ is injective. Suppose $(1/s) \otimes u \in \ker 1 \otimes \varphi$. Thus $(1/s) \otimes \varphi(u) = 0$. By the corollary above, this implies there exists a $t \in S$ such that $t\varphi(u) = 0$. Thus

$$\begin{aligned}
0 &= t\varphi(u) \\
&= \varphi(tu).
\end{aligned}$$

Since φ is injective, this implies $tu = 0$. Applying corollary above again, we see that $(1/s) \otimes u = 0$. Therefore $\ker 1 \otimes \varphi = 0$ and hence $1 \otimes \varphi$ is injective. Thus R_S is a flat R-module. □

Problem 1.f

Proposition 78.5. *$\mathbb{Q}$ is a flat $\mathbb{Z}$-module that is not projective.*

Proof. It follows from Proposition (78.4) that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module, so we just need to show that $\mathbb{Q}$ is not projective. Let $\varphi\colon \bigoplus_{i \in \mathbb{N}} \mathbb{Z} \to \mathbb{Q}$ be the unique $\mathbb{Z}$-linear map defined on the standard basis $\{e_n\}$ of $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}$ by

$$\varphi(e_n) = \frac{1}{n}$$

for all $n \in \mathbb{N}$, and let $\psi\colon \mathbb{Q} \to \mathbb{Q}$ be the identity map. Observe that φ is surjective since if $m/n \in \mathbb{Q}$, then $\varphi(me_n) = m/n$. However there is no $\widetilde{\psi}\colon \mathbb{Q} \to \bigoplus_{n \in \mathbb{N}} \mathbb{Z}$ such that $\psi = \varphi\widetilde{\psi}$. Indeed, observe that the injective map

$$\bigoplus_{n \in \mathbb{N}} \mathbb{Z} \to \prod_{n \in \mathbb{N}} \mathbb{Z}$$

induces the injective map

$$\operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \bigoplus_{n \in \mathbb{N}} \mathbb{Z}\right) \to \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \prod_{n \in \mathbb{N}} \mathbb{Z}\right)$$

since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, -)$ is a left-exact covariant functor. Therefore the injection

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \bigoplus_{n\in\mathbb{N}} \mathbb{Z}\right) \to \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \prod_{n\in\mathbb{N}} \mathbb{Z}\right) \\ \cong \prod_{n\in\mathbb{N}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \\ \cong 0\end{aligned}$$

implies

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \bigoplus_{n\in\mathbb{N}} \mathbb{Z}\right) \cong 0.$$

Thus the only $\mathbb{Z}$-linear map from $\mathbb{Q}$ to $\bigoplus_{n\in\mathbb{N}} \mathbb{Z}$ is the zero map. □

78.2 Torsion submodule

Proposition 78.6. *Let R be an integral domain with quotient field K, let M be an R-module, and let M_{tor} denote the set of all torsion elements of M. Then*

1. *M/M_{tor} is torsion free.*
2. *$M \otimes_R K \cong M/M_{\mathrm{tor}} \otimes_R K$.*

Proof.
1. Suppose $a \in R\backslash\{0\}$ and $\overline{u} \in M/M_{\mathrm{tor}}$ such that $a\overline{u} = \overline{0}$. Then there exists a $v \in M_{\mathrm{tor}}$ such that $au = v$. Since $v \in M_{\mathrm{tor}}$, there exists a $b \in R\backslash\{0\}$ such that $bv = 0$. Then

$$\begin{aligned}(ba)u &= b(au) \\ &= bv \\ &= 0\end{aligned}$$

implies $u \in M_{\mathrm{tor}}$. Thus $\overline{u} = \overline{0}$.

2. The quotient map $\pi \colon M \to M/M_{\mathrm{tor}}$ induces an R-linear map $\pi \otimes 1 \colon M \otimes_R K \to M/M_{\mathrm{tor}} \otimes_R K$. We claim that $\pi \otimes 1$ is an isomorphism. We will show this by constructing an inverse. Define $\varphi \colon M/M_{\mathrm{tor}} \otimes_R K \to M \otimes_R K$ by

$$\varphi\left(\overline{u} \otimes \frac{a}{s}\right) = u \otimes \frac{a}{s} \tag{328}$$

for all $\overline{u} \otimes (a/s) \in M/M_{\mathrm{tor}} \otimes_R K$. We claim that (328) is well-defined. Indeed, choose another representative of the coset class $\overline{u}$, say $v \in M$. So $u - v \in M_{\mathrm{tor}}$, which means that there exists a nonzero $b \in R$ such that $b(u-v) = 0$. Then

$$\begin{aligned}\varphi\left(\overline{v} \otimes \frac{a}{s}\right) &= v \otimes \frac{a}{s} \\ &= v \otimes \frac{ba}{bs} \\ &= bv \otimes \frac{a}{bs} \\ &= bu \otimes \frac{a}{bs} \\ &= u \otimes \frac{ba}{bs} \\ &= u \otimes \frac{a}{s} \\ &= \varphi\left(\overline{u} \otimes \frac{a}{s}\right).\end{aligned}$$

Also, (328) is R-bilinear in $\overline{u}$ and a/s. Thus φ is well-defined. It is also clearly the inverse to $\pi \otimes 1$. Hence $\pi \otimes 1$ is an isomorphism. □

78.3 Tensor-hom adjointness

Lemma 78.2. *Let M_1, M_2, M_3 be R-modules. Then*

$$\mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3)) \cong \mathrm{Hom}_R(M_1 \otimes_R M_2, M_3). \tag{329}$$

Moreover (329) is natural in M_3.

Remark 133. It is also natural in M_1 and M_2, but we omit the proof of this.

Proof. We define

$$\Psi_{M_3} \colon \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3)) \to \mathrm{Hom}_R(M_1 \otimes_R M_2, M_3)$$

to be the map which sends a $\psi \in \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3))$ to the map $\Psi_{M_3}(\psi) \in \mathrm{Hom}_R(M_1 \otimes_R M_2, M_3)$ defined by

$$\Psi_{M_3}(\psi)(u_1 \otimes u_2) = (\psi(u_1))(u_2) \tag{330}$$

for all elementary tensors $u_1 \otimes u_2 \in M_1 \otimes_R M_2$. Note that $\Psi_{M_3}(\psi)$ is a well-defined R-linear map since the map $M_1 \times M_2 \to M_3$ given by

$$(u_1, u_2) \mapsto (\psi(u_1))(u_2)$$

is R-bilinear. Indeed, let $a \in R$. Then we have

$$\begin{aligned}
(\psi(au_1))(u_2) &= (a\psi(u_1))(u_2) \\
&= (\psi(u_1))(au_2) \\
&= a((\psi(u_1))(u_2))
\end{aligned}$$

since both ψ and $\psi(u_1)$ are R-linear. Similarly, if $v_1 \in M_1$, then

$$\begin{aligned}
(\psi(u_1 + v_1))(u_2) &= (\psi(u_1) + \psi(v_1))(u_2) \\
&= (\psi(u_1))(u_2) + (\psi(v_1))(u_2),
\end{aligned}$$

and if $v_2 \in M_2$, then

$$(\psi(u_1))(u_2 + v_2) = (\psi(u_1))(u_2) + (\psi(u_1))(v_2).$$

Thus $\Psi_{M_3}(\psi)$ is a well-defined R-linear map.

Let us check that Ψ_{M_3} is R-linear. Let $a, b \in R$ and $\psi, \varphi \in \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3))$. Then for all $u_1 \otimes u_2 \in M_1 \otimes_S M_2$, we have

$$\begin{aligned}
\Psi_{M_3}(a\varphi + b\psi)(u_1 \otimes u_2) &= ((a\varphi + b\psi)(u_1))(u_2) \\
&= (a\varphi(u_1) + b\psi(u_1))(u_2) \\
&= (a\varphi(u_1))(u_2) + (b\psi(u_1))(u_2) \\
&= a(\varphi(u_1))(u_2) + b(\psi(u_1))(u_2) \\
&= a\Psi_{M_3}(\varphi)(u_1 \otimes u_2) + b\Psi_{M_3}(\psi)(u_1 \otimes u_2)
\end{aligned}$$

Thus Ψ_{M_3} is R-linear.

To see that Ψ_{M_3} is an isomorphism, we construct an inverse function. Define

$$\Phi_{M_3} \colon \mathrm{Hom}_R(M_1 \otimes_R M_2, M_3) \to \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3))$$

to be the map which sends $\varphi \in \mathrm{Hom}_R(M_1 \otimes_R M_2, M_3)$ to the map $\Phi_{M_3}(\varphi) \in \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3))$ defined by

$$(\Phi(\varphi)(u_1))(u_2) = \varphi(u_1 \otimes u_2)$$

for all $u_1 \in M_1$ and $u_2 \in M_2$. We claim that Ψ_{M_3} and Φ_{M_3} are inverse to each other. Indeed, we have

$$\begin{aligned}
(\Psi_{M_3}(\Phi_{M_3}(\varphi)))(u_1 \otimes u_2) &= (\Phi_{M_3}(\varphi)(u_1))(u_2) \\
&= \varphi(u_1 \otimes u_2).
\end{aligned}$$

for all $u_1 \otimes u_2$ and $\varphi \in \mathrm{Hom}_R(M_1 \otimes_R M_2, M_3)$. It follows that

$$\Psi_{M_3}\Phi_{M_3} = 1_{\mathrm{Hom}_R(M_1 \otimes_R M_2, M_3)}.$$

Similarly, we have

$$\begin{aligned}
(\Phi_{M_3}(\Psi_{M_3}(\psi))(u_1))(u_2) &= \Psi_{M_3}(\psi)(u_1 \otimes u_2) \\
&= (\psi(u_1))(u_2)
\end{aligned}$$

for all $u_1 \in M_1$, $u_2 \in M_2$, and $\psi \in \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3))$. It follows that

$$\Phi_{M_3}\Psi_{M_3} = 1_{\mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3))}.$$

Thus Ψ_{M_3} is an isomorphism.

Naturality in M_3 means that if $\lambda \colon M_3 \to M_3'$ is an R-module homomorphism, then we have a commutative diagram

$$\begin{tikzcd} \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3)) \arrow[r, "\Psi_{M_3}"] \arrow[d, "(\lambda_*)_*"'] & \mathrm{Hom}_R(M_1 \otimes_R M_2, M_3) \arrow[d, "\lambda_*"] \\ \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3')) \arrow[r, "\Psi_{M_3'}"'] & \mathrm{Hom}_R(M_1 \otimes_S M_2, M_3') \end{tikzcd}$$

Thus we want to show for all $\psi \in \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, M_3))$, we have

$$\lambda_* \left(\Psi_{M_3}(\psi)\right) = \Psi_{M_3'}((\lambda_*)_*(\psi)) \tag{331}$$

To see that (331) is equal, we apply all elementary tensors to both sides. Let $u_1 \otimes u_2 \in M_1 \otimes_R M_2$. We have

$$\begin{aligned} \left(\lambda_* \left(\Psi_{M_3}(\psi)\right)\right)(u_1 \otimes u_2) &= \lambda\left(\left(\Psi_{M_3}(\psi)\right)(u_1 \otimes u_2)\right) \\ &= \lambda\left((\psi(u_1))(u_2)\right) \\ &= (\lambda_*(\psi(u_1)))(u_2) \\ &= ((\lambda_*)_*(\psi))(u_1))(u_2) \\ &= \left(\Psi_{M_3'}((\lambda_*)_*(\psi))\right)(u_1 \otimes u_2). \end{aligned}$$

□

78.4 Tensor product of projective modules is projective

Proposition 78.7. *Let P and Q be projective R-modules. Then $P \otimes_R Q$ is a projective R-module.*

Proof. It suffices to show that $\mathrm{Hom}_R(P \otimes_R Q, -)$ is exact. Let

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0 \tag{332}$$

be a short exact sequence. Then since Q is projective, the induced sequence

$$0 \longrightarrow \mathrm{Hom}_R(Q, M_1) \longrightarrow \mathrm{Hom}_R(Q, M_2) \longrightarrow \mathrm{Hom}_R(Q, M_3) \longrightarrow 0$$

is exact. Then since P is projective, the induced sequence

$$0 \longrightarrow \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_1)) \longrightarrow \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_2)) \longrightarrow \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_3)) \longrightarrow 0$$

is exact. By tensor-hom adjointness, we have a commutative diagram[16]

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_1)) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_2)) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_3)) \arrow[r] \arrow[d, "\cong"] & 0 \\ 0 \arrow[r] & \mathrm{Hom}_R(P \otimes_R Q, M_1) \arrow[r] & \mathrm{Hom}_R(P \otimes_R Q, M_2) \arrow[r] & \mathrm{Hom}_R(P \otimes_R Q, M_3) \arrow[r] & 0 \end{tikzcd}$$

where the columns are isomorphisms and where the top row is exact. It follows from the 3×3 lemma that the bottom row is exact too.

□

[16]Note how we need naturality in the third argument to get a commutative diagram.

79 Homework 6

Canonical form of matrix over $\mathbb{Q}$

Exercise 8. Find the canonical forms of the following matrix over $\mathbb{Q}$:

$$A = \begin{pmatrix} -12 & -140 & -469 & -1154 & 6622 & -16231 \\ -107 & 9 & -194 & -905 & 3543 & -11613 \\ -216 & 281 & 449 & 122 & -4473 & 4274 \\ -74 & -342 & -925 & -1840 & 12248 & -27049 \\ -39 & 68 & 135 & 149 & -1560 & 2575 \\ -14 & 44 & 110 & 197 & -1415 & 2966 \end{pmatrix}.$$

Solution 1. Using sagemath, we find that the invariant factors are $(x-2)^2 \mid (x-2)^4$. Thus the rational canonical form of A is given by

$$A_{\text{rat}} = \begin{pmatrix} 0 & 0 & 0 & -16 & 0 & 0 \\ 1 & 0 & 0 & 32 & 0 & 0 \\ 0 & 1 & 0 & -24 & 0 & 0 \\ 0 & 0 & 1 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 & 1 & 4 \end{pmatrix}.$$

The elementary divisors are $\{(x-2)^2, (x-2)^4\}$. Thus the primary rational canonical form of A is given by

$$A_{\text{prat}} = \begin{pmatrix} 0 & 0 & 0 & -16 & 0 & 0 \\ 1 & 0 & 0 & 32 & 0 & 0 \\ 0 & 1 & 0 & -24 & 0 & 0 \\ 0 & 0 & 1 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 & 1 & 4 \end{pmatrix}.$$

Also using sagemath, we find that the characteristic polynomial of A is given by

$$\chi_A(x) = (x-2)^6.$$

Therefore the Jordan canonical form of A is given by

$$A_{\text{jor}} = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

79.1 Canonical forms of matrix over $\mathbb{R}$ with characteristic polynomial $(x^3-1)^2$

Exercise 9. Find all possible canonical forms for a matrix over $\mathbb{R}$ with characteristic polynomial $(x^3-1)^2$.

Solution 2. Let A be a matrix over the real numbers with characteristic polynomial

$$\chi_A(x) = (x^3-1)^2 = (x-1)^2(x^2+x+1)^2.$$

Let A_{rat} be the rational canonical form of A and let A_{prat} be the primary rational canonical form of A. The minimal polynomial of A has the same irreducible factors as the characteristic polynomial of A. Thus we have the following cases: if the minimal polynomial of A is equal to the characteristic polynomial of A, then the invariant factors of A are $(x-1)^2(x^2+x+1)^2$ and the elementary divisors of A are $\{(x-1)^2, (x^2+x+1)^2\}$. Therefore

$$A_{\text{rat}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -2 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad A_{\text{prat}} = \begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & -3 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

If the minimal polynomial of A is $(x-1)(x^2+x+1)^2$, then the invariant factors of A are $(x-1) \mid (x-1)\left(x^2+x+1\right)^2$ and the elementary divisors of A are $\{x-1, x-1, (x^2+x+1)^2\}$. Therefore

$$A_{\mathrm{rat}} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A_{\mathrm{prat}} = \begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & -3 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

If the minimal polynomial of A is $(x-1)^2(x^2+x+1)$, then the invariant factors of A are $\left(x^2+x+1\right) \mid (x-1)^2\left(x^2+x+1\right)$ and the elementary divisors of A are $\{x^2+x+1, x^2+x+1, (x-1)^2\}$. Therefore

$$A_{\mathrm{rat}} = \begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix} \quad \text{and} \quad A_{\mathrm{prat}} = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

If the minimal polynomial of A is $(x-1)(x^2+x+1)$, then the invariant factors of A are $(x-1)\left(x^2+x+1\right) \mid (x-1)\left(x^2+x+1\right)$ and the elementary divisors of A are $\{x^2+x+1, x^2+x+1, x-1, x-1\}$. Therefore

$$A_{\mathrm{rat}} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad A_{\mathrm{prat}} = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

79.2 Counting conjugacy classes in $\mathrm{GL}_3(\mathbb{F}_2)$

Exercise 10. Find the number of conjugacy classes in $\mathrm{GL}_3(\mathbb{F}_2)$ and a representative of each class.

Solution 3. Two matrices in $\mathrm{GL}_3(\mathbb{F}_2)$ are conjugative if and only if they have the same invariant factors. Thus we just need to find all possible sets of invariant factors $a(x) \mid b(x) \mid c(x)$ in $\mathbb{F}_2[x]$ such that the companion matrices are all nonsingular, which is equivalent to the constant term of each polynomial being nonzero. There are six such cases. We list them below in the table below:

Invariant Factors	Coset Representative
$(x+1) \mid (x+1) \mid (x+1)$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
$(x+1) \mid (x+1)^2$	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
x^3+1	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
x^3+x^2+x+1	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$
x^3+x^2+1	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$
x^3+x+1	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

80 Homework 7

80.1 $K(\alpha^2) = K(\alpha)$ if α is algebraic of odd degree

Proposition 80.1. *Let $K \subseteq L$ be an extension of fields and let $\alpha \in L$ be algebraic over K of odd degree. Then $K(\alpha^2) = K(\alpha)$.*

Proof. It suffices to show that $K(\alpha) \subseteq K(\alpha^2)$ since the other direction is clear. The extension of fields

$$K \subseteq K(\alpha^2) \subseteq K(\alpha)$$

gives us the relation

$$[K(\alpha) : K] = [K(\alpha) : K(\alpha^2)][K(\alpha^2) : K] \tag{333}$$

We claim that $[K(\alpha) : K(\alpha^2)] \leq 2$. Indeed, let denote $n = [K(\alpha) : K]$. Then a K-basis of $K(\alpha)$ is given by

$$\{\alpha^i \mid 0 \leq i \leq n-1\}.$$

It follows that

$$\{\alpha^{2i} \mid 0 \leq 2i \leq n-1\}$$

is a linearly independent set in $K(\alpha^2)$. Therefore $[K(\alpha^2) : K] \geq n/2$, which implies

$$\begin{aligned}
[K(\alpha) : K(\alpha^2)] &= \frac{[K(\alpha) : K]}{[K(\alpha^2) : K]} \\
&= \frac{n}{[K(\alpha^2) : K]} \\
&\leq \frac{n}{n/2} \\
&= 2.
\end{aligned}$$

and hence $[K(\alpha) : K(\alpha^2)] \leq 2$ by (333).

Now combining (333) with the fact that $2 \nmid [K(\alpha) : K]$, we see that $2 \nmid [K(\alpha) : K(\alpha^2)]$. Therefore $[K(\alpha) : K(\alpha^2)] = 1$, which implies $K(\alpha) = K(\alpha^2)$. □

Remark 134. Note that if α was transcendental, then all we say can is $K(\alpha^2)$ is *strictly* contained in $K(\alpha)$. Indeed, assume for a contradiction that $K(\alpha^2) = K(\alpha)$. Then $\alpha \in K(\alpha^2)$ implies

$$\alpha = a_0 + a_2\alpha^2 + a_4\alpha^4 \cdots + a_{2N}\alpha^{2N}$$

for some $N \in \mathbb{N}$ and $a_0, a_2, a_4, \dots, a_{2N} \in K$. However this would imply α is algebraic over K, which is a contradiction.

80.2 Finite subgroup of $K^\times$ is cyclic and applications

Problem 2.a

Lemma 80.1. *Let A be a finite abelian group. Then the order of every element must divide the maximal order.*

Proof. From the fundamental theorem of finite abelian groups, we have an isomorphism

$$A \cong \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_n}$$

where $k_1 \mid \cdots \mid k_n$. Let $e_1, \dots, e_n$ denote the standard $\mathbb{Z}$-basis for $\mathbb{Z}^n$, and let $\overline{e}_i$ denote the corresponding coset in $\mathbb{Z}_{k_i}$ for each $1 \leq i \leq n$. Since $k_i \mid k_n$ we see that k_n kills each $\mathbb{Z}_{k_i}$ for all $1 \leq i \leq n$. Therefore k_n kills all of A. In particular, the order of every element must divide k_n, which is in fact the maximal order as $k_n = \mathrm{ord}(\overline{e}_{i_n})$. □

Lemma 80.2. *The number of roots of a polynomial over a field is at most the degree of the polynomial.*

Proof. Let K be a field and let $f(T)$ be a polynomial coefficients in K. By replacing K with a splitting field of $f(T)$ if necessary, we may assume that $f(T)$ splits into linear factors over K, say

$$f(T) = (T - \alpha_1) \cdots (T - \alpha_n).$$

where $\alpha_1, \dots \alpha_n \in K$ and $n = \deg f(T)$. Let $\alpha \in K$. Then we have

$$\begin{aligned}
f(\alpha) = 0 &\iff (\alpha - \alpha_1) \cdots (\alpha - \alpha_n) = 0 \\
&\iff \alpha - \alpha_i = 0 \text{ for some } i \\
&\iff \alpha = \alpha_i \text{ for some } i,
\end{aligned}$$

where we obtained the second line from the first line from the fact that K is an integral domain. Therefore $f(T)$ has *at most* n roots. □

Proposition 80.2. *Let K be a field and let G be a finite subgroup of $K^\times$. Then G is cyclic.*

Proof. Let $n = |G|$ and let m be the maximal order among all elements in G. We will show $m = n$. By Lagrange's Theorem, we have $m \mid n$, and hence $m \leq n$. It follows from Lemma (80.1) that every order of every element must divide the maximal order. In particular, we have $x^m = 1$ for all $x \in G$. Therefore all numbers in G are roots of the polynomial $T^m - 1$. By Lemma (80.2), the number of roots of a polynomial over a field is at most the degree of the polynomial, so $n \leq m$. Combining both inequalities gives us $m = n$. □

Problem 2.b

Proposition 80.3. *Let K be a finite field. Then the product of two nonsquares in K is a square in K.*

Proof. By problem 2.a, $K^\times$is cyclic. Choose $\gamma \in K^\times$ such that $K^\times = \langle \gamma \rangle$.

Step 1: Assume that $\operatorname{char} K = 2$. Thus $|K| = 2^k$ for some $n \geq 1$. We claim that every number is a square. Indeed, clearly 0 is a square of itself. Also, for any $\gamma^i \in K^\times$, we have

$$\begin{aligned} \gamma^i &= (\gamma^i)^{2^k} \\ &= (\gamma^i)^{2 \cdot 2^{k-1}} \\ &= (\gamma^{i(2^{k-1})})^2. \end{aligned}$$

Thus every number is a square.

Step 2: Now assume that $\operatorname{char} K \neq 2$ and denote $n = |K^\times|$. We claim that the set of all nonsquares in K is given by

$$\{\gamma^{2i+1} \in K^\times \mid 1 \leq 2i + 1 \leq n - 2\}. \tag{334}$$

Indeed, assume for a contradiction that $\gamma^{2i+1} = (\gamma^j)^2 = \gamma^{2j}$ for some $\gamma^j \in K^\times$. If $2i + 1 \geq 2j$, then this implies

$$\gamma^{2(i-j)+1} = 1. \tag{335}$$

Then (335) implies $2(i - j) + 1 \mid n - 1$, which is a contradiction since $2(i - j) + 1$ is odd and $n - 1$ is even. Similarly, if $2j \geq 2i + 1$, then

$$\gamma^{2(j-i)-1} = 1,$$

which implies $2(j - i) - 1 \mid n - 1$. Again this is a contradiction since $2(j - i) - 1$ is odd and $n - 1$ is even. Therefore every number in (334) is a nonsquare. In fact it contains *all* nonsquares, since as a set, we can partition K as

$$K = \{0\} \cup \{\gamma^{2i} \in K^\times \mid 0 \leq 2i \leq n - 3\} \cup \{\gamma^{2i+1} \in K^\times \mid 1 \leq 2i + 1 \leq n - 2\}.$$

Clearly $\{\gamma^{2i} \in K^\times \mid 0 \leq 2i \leq n - 3\}$ and $\{0\}$ consists of square elements.

Step 3: Let γ^{2i+1} and γ^{2j+1} be nonsquares in K for some $1 \leq 2i + 1, 2j + 1 \leq n - 2$. Then their product is a square:

$$\begin{aligned} \gamma^{2i+1}\gamma^{2j+1} &= \gamma^{2i+2j+2} \\ &= (\gamma^{i+j+1})^2. \end{aligned}$$

Thus the product of two nonsquares is a square. □

Problem 2.c

Proposition 80.4. *Let K be a finite field. Then each number in K is the sum of two squares.*

Proof. If $\operatorname{char} K = 2$, then every element is a square (by step 1 in problem 2.b), and hence is a sum of two squares. Therefore we may assume that $\operatorname{char} K \neq 2$. Let $a \in K$ and denote $n = |K|$. Consider the following sets

$$S = \{x \in K \mid x \text{ is a square}\} \quad \text{and} \quad a - S = \{a - x \in K \mid x \text{ is a square}\}.$$

We claim that $|a - S| = |S|$. Indeed, let $\varphi \colon K \to K$ be the negation map given by

$$\varphi(x) = -x$$

for all $x \in K$ and let $\psi \colon K \to K$ be the addition by a map given by

$$\psi(x) = a + x$$

for all $x \in A$. Then φ is a bijection since -1 is a unit and ψ is a bijection since K is a group under addition, and thus their composite $\psi\varphi$ is a bijection. In particular, it restricts to a bijection $S \to a - S$ since

$$\psi\varphi(S) = a - S.$$

Finally, by step 2 in problem 2.b, we know that more than half of the numbers in K are squares. Therefore since $|S| > n/2$, $|a - S| > n/2$, and

$$\begin{aligned} |S \cup (a - S)| &\leq |K| \\ &= n, \end{aligned}$$

it follows from the pigeonhole principle that $S \cap (a - S) \neq \emptyset$. Thus we may choose $a - x \in S \cap (a - S)$ where both x and $a - x$ are squares. Therefore

$$a = x + (a - x)$$

is a sum of two squares. □

80.3 B is a field if and only if A is a field

Lemma 80.3. *Let $A \subset B$ be an integral extension and suppose B is an integral domain. Then B is a field if and only if A is a field.*

Proof. Suppose that B is a field and let a be a nonzero element in A. We will show that a is a unit in A. Since a belongs to B, we know that it is a unit in B, say $ab = 1$ for some b in B. Since B is integral over A, there exists $n \in \mathbb{N}$ and $a_0, \dots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0. \tag{336}$$

Multiplying a^{n-1} on both sides of (49) gives us

$$b + a_{n-1} + \cdots + a^{n-1}a_0 = 0.$$

In particular, $b \in A$. Thus a is a unit in A.

Conversely, suppose A is a field and let b be a nonzero element in B. Since b is integral over A, there exists $n \in \mathbb{N}$ and $a_0, \dots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0,$$

where we may assume that n is minimal. Then since n is minimal and B is an integral domain, we must have $a_0 \neq 0$. Thus

$$\begin{aligned} 1 &= (-a_0)^{-1}(b^n + a_{n-1}b^{n-1} + \cdots + a_1 b) \\ &= (-a_0)^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)b \end{aligned}$$

implies

$$(-a_0)^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)$$

is the inverse of b. □

Proposition 80.5. *Let L/K be an algebraic extension of fields and let R be an integral domain such that*

$$K \subseteq R \subseteq L.$$

Then R is a field.

Proof. First note that $K \subseteq R$ is an integral extension since L/K is an algebraic extension. Indeed, let $x \in R$. Then $x \in L$, and since L/K is algebraic, there exists $n \in \mathbb{N}$ and $a_0, a_1, \dots, a_n \in K$ such that

$$a_n x^n + \cdots + a_1 x + a_0 = 0. \tag{337}$$

where $a_n \neq 0$. Since K is a field, we can multiply both sides of (50) by a_n^{-1} and obtain

$$x^n + \cdots + a_n^{-1}a_1 x + a_n^{-1}a_0 = 0. \tag{338}$$

Then (51) implies x is integral over K. Since x was arbitrary, we see that $K \subseteq R$ is an integral extension. Now it follows from Lemma (80.3) that since K is a field, R must be a field too. □

80.4 $[K(\alpha,\beta):K] \leq mn$ with equality if $\gcd(m,n)=1$

Proposition 80.6. *Let K be a field and let α and β be algebraic numbers in some field extension of K. Denote $[K(\alpha):K]=m$ and $[K(\beta):K]=n$. Then*

$$[K(\alpha,\beta):K] \leq mn$$

with equality holding if $\gcd(m,n)=1$.

Proof. Since β is algebraic over K, it is also algebraic over $K(\alpha)$. Let

$$f(T) = T^k + \alpha_{k-1}T^{k-1} + \cdots + \alpha_0$$

be the minimal polynomial of β in $K(\alpha)[T]$, where $\alpha_0,\ldots,\alpha_{n-1} \in K(\alpha)$, and let

$$g(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

be the minimal polynomial of β in $K[T]$. Since $g(T)$ is a monic polynomial with coefficients in $K(\alpha)$ which kills β, we must have $k \leq n$, by minimality of k. Therefore

$$\begin{aligned}
[K(\alpha,\beta):K] &= [K(\alpha,\beta):K(\alpha)][K(\alpha):K] \\
&= [K(\alpha)(\beta):K(\alpha)][K(\alpha):K] \\
&= km \\
&\leq nm.
\end{aligned}$$

This gives us the bound we are looking for.

Now assume that $\gcd(m,n)=1$. Denote $k'=[K(\alpha,\beta):K(\beta)]$. By the same argument as above, we have

$$km = [K(\alpha,\beta):K] = k'n.$$

Therefore $[K(\alpha,\beta):K]$ is a common multiple of m and n. Then since $\gcd(m,n)=1$, we have

$$\begin{aligned}
mn &= \operatorname{lcm}(m,n) \\
&\leq [K(\alpha,\beta):K] \\
&\leq mn.
\end{aligned}$$

It follows that $[K(\alpha,\beta):K]=mn$. □

80.5 $\operatorname{Aut}(\mathbb{R}/\mathbb{Q})=1$

Proposition 80.7. *The only automorphism of $\mathbb{R}$ which fixes $\mathbb{Q}$ is the identity map.*

Proof. Let $\sigma\colon \mathbb{R}\to\mathbb{R}$ be an automorphism of $\mathbb{R}$ which fixes $\mathbb{Q}$. We will show that σ is the identity map as follows:

Step 1: We first show that σ sends positive numbers to positive numbers. Let x be a positive real number. Then $x=a^2$ for some $a \in \mathbb{R}\backslash\{0\}$. Then

$$\begin{aligned}
\sigma(x) &= \sigma(a^2) \\
&= \sigma(a)^2 \\
&> 0.
\end{aligned}$$

It follows that σ sends positive numbers to positive numbers.

Step 2: Next we show σ is strictly increasing. Let x and y be real numbers such that $x>y$. Then $x-y>0$. This implies

$$\begin{aligned}
\sigma(x)-\sigma(y) &= \sigma(x-y) \\
&> 0.
\end{aligned}$$

It follows that σ is strictly increasing.

Step 3: We show that σ is continuous with respect to the usual topology on $\mathbb{R}$. Let (x_n) be a sequence of real numbers which converges to some real number x. Let $\varepsilon>0$ and choose $M\in\mathbb{N}$ such that $1/M<\varepsilon$. Also, choose $N\in\mathbb{N}$ such that $n\geq N$ implies

$$-\frac{1}{M} < x_n - x < \frac{1}{M}.$$

Then $n \geq N$ implies

$$\begin{aligned} -\varepsilon &< -\frac{1}{M} \\ &= \sigma\left(-\frac{1}{M}\right) \\ &< \sigma(x_n) - \sigma(x) \\ &< \sigma\left(\frac{1}{M}\right) \\ &= \frac{1}{M} \\ &< \varepsilon. \end{aligned}$$

It follows that the sequence $(\sigma(x_n))$ converges to $\sigma(x)$. This implies σ is continuous.

Step 4: Finally we show that σ is the identity map. Let x be a real number. As $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists a sequence of rational numbers (x_n) which converges to x. Choose such a sequence (x_n). It follows from continuity of σ and the fact that $\sigma(x_n) = x_n$ for all $n \in \mathbb{N}$ that we must have $\sigma(x) = x$. Thus σ is the identity map. □

81 Homework 8

81.1 $\mathbb{Q}(x^2)$ is closed intermediate extension of $\mathbb{Q}(x)/\mathbb{Q}$ but $\mathbb{Q}(x^3)$ is not

Exercise 11. Consider the field extension $\mathbb{Q} \subseteq \mathbb{Q}(x)$. Show that $\mathbb{Q}(x^2)$ is a closed intermediate extension but $\mathbb{Q}(x^3)$ is not.

Solution 4. First we show $\mathbb{Q}(x^2)$ is a closed intermediate extension. Let $\sigma \in \mathrm{Aut}(\mathbb{Q}(x)/\mathbb{Q}(x^2))$. Then σ is completely determined by where it sends x since

$$\sigma \cdot (a_n x^n + \cdots + a_1 x + a_0) = a_n \sigma(x)^n + \cdots + a_1 \sigma(x) + a_0$$

for any $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ (so $\sigma \cdot (f(x)/g(x)) = f(\sigma \cdot x)/g(\sigma \cdot x)$ for any $f/g \in \mathbb{Q}(x)$). Since σ fixes x^2, we see that $\sigma(x)$ must be a root of the monic

$$T^2 - x^2 = (T - x)(T + x).$$

In particular, either $\sigma(x) = x$ or $\sigma(x) = -x$. In particular, does not fix $\mathbb{Q}(x)$. Since there are no intermediate fields between $\mathbb{Q}(x^2)$ and $\mathbb{Q}(x)$ (as $[\mathbb{Q}(x) : \mathbb{Q}(x^2)] = 2$ is prime), we see that the fixed field of $\mathrm{Aut}(\mathbb{Q}(x)/\mathbb{Q}(x^2))$ is $\mathbb{Q}(x^2)$. Thus $\mathbb{Q}(x^2)$ is a closed intermediate extension.

Now we show $\mathbb{Q}(x^3)$ is not a closed intermediate extension. Let $\sigma \in \mathrm{Aut}(\mathbb{Q}(x)/\mathbb{Q}(x^3))$. As seen above, σ is completely determined by where it sends x. Since σ fixes x^3, we see that $\sigma(x)$ must be a root of the monic

$$T^3 - x^3 = (T - x)(T - \zeta_3 x)(T - \zeta_3^2 x).$$

Since $\zeta_3 \notin \mathbb{Q}$, we see that the only possible choice is $\sigma(x) = x$. Thus the fixed field of $\mathrm{Aut}(\mathbb{Q}(x)/\mathbb{Q}(x^3))$ is $\mathbb{Q}(x)$ (and not $\mathbb{Q}(x^3)$). Thus $\mathbb{Q}(x^3)$ is not a closed intermediate extension.

81.2 Degree 2 extensions

Problem 2.a

Proposition 81.1. *Let F/K be a field extension such that $[F : K] = 2$. Suppose that* $\mathrm{char}\, K \neq 2$. *Then L is Galois over K.*

Proof. It suffices to show that F is a splitting field of a separable polynomial over K. Let $\alpha \in L \backslash K$ and let $\pi_\alpha(T)$ be the minimal polynomial of α over K. Then $\pi_\alpha(T)$ must have degree 2 (it can't have degree 1 this would imply $\alpha \in K$ and it can't have degree > 2 since this would imply $[F : K] > 2$). Since α is a root of $\pi_\alpha(T)$, we see that $\pi_\alpha(T)$ factors as

$$\pi_\alpha(T) = (T - \alpha)p(T)$$

where $p(T)$ has degree 1 since $\pi_\alpha(T)$ has degree 2. Since $\mathrm{char}\, K \neq 2$, we have $\pi'_\alpha(T) \neq 0$ (since the lead term of $\pi'_\alpha(T)$ is $2T \neq 0$). Thus $\pi_\alpha(T)$ is a separable polynomial over K. Since $p(T)$ has degree 1, it obviously has a root in F. Thus $\pi_\alpha(T)$ splits completely in F. In particular F is the splitting field of $\pi_\alpha(T)$ since $[F : K] = 2 = \deg \pi_\alpha$. □

Problem 2.b

Exercise 12. Give an example of a field extension F/K such that $[F:K] = 2$ and $\operatorname{char} K = 2$ but F/K is not Galois.

Solution 5. Let $K = \mathbb{F}_2(t)$ and let $F = K(\sqrt{t})$. Then L/K is an inseparable extension. Indeed, the minimal polynomial of $\sqrt{t}$ over K is $X^2 + t$, which factors over F as

$$X^2 + t = (X + \sqrt{t})^2.$$

This has a multiple root, which implies $\sqrt{t}$ in inseparable over K. Thus L/K is an inseparable extension, and hence is not Galois.

Problem 3.c

Exercise 13. Give an example of a field extension F/K such that $[F:K] = 2$ and $\operatorname{char} K = 2$ with F/K being Galois.

Solution 6. Let $K = \mathbb{F}_2$ and $F = \mathbb{F}_2[T]/\langle f(T)\rangle$ where $f(T) = T^2 + T + 1$. The minimal polynomial of $\overline{T} \in F$ is given by

$$f(X) = X^2 + X + 1,$$

indeed, observe $f(X)$ is irreducible over $\mathbb{F}_2$ by a brute force calculation:

$$\begin{aligned} XX &= X^2 \\ X(X+1) &= X^2 + X \\ (X+1)(X+1) &= X^2 + 1. \end{aligned}$$

Furthermore, $f(X)$ is separable over $\mathbb{F}_2$ since $f(X)$ is irreducible and $f'(X) = 1 \neq 0$. Finally, note that

$$\begin{aligned} (X + \overline{T})(X + \overline{T+1}) &= X^2 + (\overline{T+1} + \overline{T})X + \overline{T}(\overline{T+1}) \\ &= X^2 + X + \overline{T}^2 + \overline{T} \\ &= X^2 + X + 1. \end{aligned}$$

Thus $f(X)$ splits in F. In particular, F is a splitting field of the separable polynomial $f(X)$ (again for degree reasons).

81.3 If L/K and M/L are Galois extensions, then M/K need not be a Galois extension

Exercise 14. Let E/K and F/E be Galois extensions. Then is F/K a Galois extension?

Solution 7. No. Consider the following tower of field extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}).$$

Observe that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are Galois extensions since they are field extensions of degree 2 and since we are working over characteristic 0 fields. However $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois since $\sqrt[4]{2}$ is the root of the polynomial $T^4 - 2$, but this polynomial factors over $\mathbb{Q}(\sqrt[4]{2}, i)$ as

$$T^4 - 2 = (T - \sqrt[4]{2})(T - i\sqrt[4]{2})(T + \sqrt[4]{2})(T + i\sqrt[4]{2}).$$

In particular, $T^4 - 2$ only has two roots in $\mathbb{Q}(\sqrt[4]{2})$ (the other roots are imaginary numbers whereas $\mathbb{Q}(\sqrt[4]{2})$ consists of real numbers).

81.4 Extensions over $\mathbb{Q}$ given by $f = x^5 - 3$ and $g = x^4 + x^3 + x^2 + x + 1$

Let $f(X) = X^5 - 3$ and let $g(X) = X^4 + X^3 + X^2 + X + 1$. Also let α be a complex root of f and let β be a complex root of g. Observe that f is irreducible over $\mathbb{Q}$ since it is Eisenstein at 3 and g is irreducible over $\mathbb{Q}$ since

$$\begin{aligned} g(X+5) &= (X+1)^4 + (X+1)^3 + (X+1)^2 + (X+1) + 1 \\ &= X^4 + 5X^3 + 10X^2 + 10X + 5 \end{aligned}$$

is Eisenstein at 5 (also g is the 5th cyclotomic polynomial).

Let $\zeta_5 = e^{2\pi i/5}$. We can factor f over $\mathbb{C}$ as

$$f(X) = (X - \sqrt[5]{3})(X - \zeta_5\sqrt[5]{3})(X - \zeta_5^2\sqrt[5]{3})(X - \zeta_5^3\sqrt[5]{3})(X - \zeta_5^4\sqrt[5]{3}). \tag{339}$$

Indeed, $\zeta_5^b\sqrt[5]{3}$ is a root of f for all $b \in \mathbb{Z}/5\mathbb{Z}$ (you'll see in a second why I'm writing $b \in \mathbb{Z}/5\mathbb{Z}$ and not simply just $0 \le b \le 4$). Since these five roots are distinct from each other and since $\deg f = 5$, they must exhaust all the roots of f. In particular, $\alpha = \zeta_5^b\sqrt[5]{3}$ for some $b \in \mathbb{Z}/5\mathbb{Z}$. Similarly, we can factor g over $\mathbb{C}$ as

$$g(X) = (X - \zeta_5)(X - \zeta_5^2)(X - \zeta_5^3)(X - \zeta_5^4). \tag{340}$$

Indeed, ζ_5^a is a root of g for all $a \in (\mathbb{Z}/5\mathbb{Z})^\times$ (again, you'll see in a second why I'm writing $a \in (\mathbb{Z}/5\mathbb{Z})^\times$ and not simply just $1 \le a \le 4$). Since these four roots are distinct from each other and since $\deg g = 4$, they must exhaust all the roots of g (alternatively, one can see this from the fact that g is the 5th cyclotomic polynomial). In particular, $\beta = \zeta_5^a$ for some $a \in (\mathbb{Z}/5\mathbb{Z})^\times$.

Problem 1.a

Exercise 15. Find $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and show that this extension is not Galois.

Solution 8. As shown above, f is irreducible over $\mathbb{Q}$ with $\deg f = 5$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. To see why $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois, it suffices to show that $\mathbb{Q}(\sqrt[5]{3})/\mathbb{Q}$ is not Galois (since there is a $\mathbb{Q}$-isomorphism taking $\mathbb{Q}(\alpha)$ to $\mathbb{Q}(\sqrt[5]{3})$). A $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[5]{3})$ must send $\sqrt[5]{3}$ to $\zeta_5^b\sqrt[5]{3}$ for some $b \in \mathbb{Z}/5\mathbb{Z}$, but $\zeta_5^b\sqrt[5]{3}$ is not a real number if $b \neq 0$, so it can't belong to $\mathbb{Q}(\sqrt[5]{3})$, so the only possibility is $\sqrt[5]{3} \mapsto \sqrt[5]{3}$. Thus $\mathrm{Aut}(\mathbb{Q}(\sqrt[5]{3})/\mathbb{Q})$ is trivial. Thus $\mathbb{Q}(\sqrt[5]{3})/\mathbb{Q}$ is not Galois, which implies $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois.

Problem 1.b

Exercise 16. Show that g is irreducible over $\mathbb{Q}(\alpha)$.

Solution 9. We showed above that g is irreducible over $\mathbb{Q}$, but now we want to show it is irreducible over $\mathbb{Q}(\alpha)$. Since f and g are monic irreducible polynomials over $\mathbb{Q}$ which kill α and β respectively, we see that f is the minimal polynomial for α and g is the minimal polynomial for β. Since $\deg f = 5$ and $\deg g = 4$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. Since $\gcd(4, 5) = 1$, it follows that $[\mathbb{Q}(\alpha, \beta) \colon \mathbb{Q}] = 4 \cdot 5 = 20$ (by a previous HW problem). This also implies g is the minimal polynomial for β over $\mathbb{Q}(\alpha)$. Indeed, if $h(X)$ is an irreducible monic polynomial with coefficients in $\mathbb{Q}(\alpha)$ which kills β, then $20 = 4 \cdot \deg h$, which implies $\deg h = 5$, but g is also a monic polynomial with coefficients in $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ which kills β, thus $h \mid g$. Since $\deg h = \deg g$ and both g and h are monic, we must have $g = h$. Thus g is the minimal polynomial for β over $\mathbb{Q}(\alpha)$. In particular, it is irreducible over $\mathbb{Q}(\alpha)$.

Problem 1.c

Exercise 17. Let $\overline{F}$ be the field obtained by adjoining all of the roots of f to $\mathbb{Q}$. Find the Galois group $\mathrm{Gal}(\overline{F}/\mathbb{Q})$.

Solution 10. From the polynomial factorization (339), we see that $\overline{F} = \mathbb{Q}(\zeta_5, \sqrt[5]{3})$. Indeed, since $\zeta_5 = \zeta_5\sqrt[5]{3}/\sqrt[5]{3}$, we have $\zeta_5 \in \overline{F}$, and hence $\mathbb{Q}(\zeta_5, \sqrt[5]{3}) \subseteq \overline{F}$. Conversely, $\zeta_5^b\sqrt[5]{3}$ is clearly in $\mathbb{Q}(\zeta_5, \sqrt[5]{3})$ for all $b \in \mathbb{Z}/5\mathbb{Z}$. Thus $\mathbb{Q}(\zeta_5, \sqrt[5]{3}) \supseteq \overline{F}$.

Any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_5, \sqrt[5]{3})$ is completely determined by where it sends ζ_5 and where it sends $\sqrt[5]{3}$. There are 4 places to send ζ_5, namely ζ_5, ζ_5^2, ζ_5^3, and ζ_5^4. Similarly, there are 5 places to send $\sqrt[5]{3}$, namely $\sqrt[5]{3}$, $\zeta_5\sqrt[5]{3}$, $\zeta_5^2\sqrt[5]{3}$, $\zeta_5^3\sqrt[5]{3}$, and $\zeta_5^4\sqrt[5]{3}$. In total, there are $4 \cdot 5 = 20$ possible automorphisms. In fact all such possibilities are realized since $[\mathbb{Q}(\zeta_5, \alpha) : \mathbb{Q}] = 20$. Let us describe them now:

For $a \in (\mathbb{Z}/5\mathbb{Z})^\times$ and $b \in \mathbb{Z}/5\mathbb{Z}$, let $\sigma_{a,b} \colon \mathbb{Q}(\zeta_5, \sqrt[5]{3}) \to \mathbb{Q}(\zeta_5, \sqrt[5]{3})$ be the $\mathbb{Q}$-automorphism which sends ζ_5 to ζ_5^a and $\sqrt[5]{3}$ to $\zeta_5^b\sqrt[5]{3}$ (any $\mathbb{Q}$-automorphism has a unique expression of this form). By a direct calculation, we have

$$\sigma_{a,b}\sigma_{a',b'} = \sigma_{aa',ab'+b} \tag{341}$$

for all $a, a' \in (\mathbb{Z}/5\mathbb{Z})^\times$ and $b, b' \in \mathbb{Z}/5\mathbb{Z}$, where multiplication and addition in the subscripts are taken modulo 5. The multiplcation rule (341) behaves just like matrix multiplication:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix}.$$

So we have an isomorphism from

$$\mathrm{Aff}(\mathbb{Z}/5\mathbb{Z}) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/5\mathbb{Z})^\times,\ b \in \mathbb{Z}/5\mathbb{Z} \right\}$$

to $\mathrm{Gal}(\mathbb{Q}(\zeta_5, \sqrt[5]{3})/\mathbb{Q})$ given by $\sigma_{a,b} \mapsto \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$.

Problem 1.d

Exercise 18. Find an explicit formula for the roots of $f(X)$.

Solution 11. This was done above.

81.5 Extension over $\mathbb{Q}$ given by $f = x^6 - 3x^3 + 1$

Let F be the field obtained by adjoining all roots of the polynomial $f(X) = X^6 - 3X^3 + 1$. From the quadratic formula, we can factor f as

$$f(X) = \left(X^3 - \left(\frac{3-\sqrt{5}}{2}\right)\right)\left(X^3 - \left(\frac{3+\sqrt{5}}{2}\right)\right). \tag{342}$$

Let $\zeta_3 = e^{2\pi i/3}$, $\alpha = \sqrt[3]{\frac{3-\sqrt{5}}{2}}$, and $\beta = \sqrt[3]{\frac{3+\sqrt{5}}{2}}$ (by cubed root here we mean the real cube root). Then we can factor (342) even further as

$$f(X) = (X-\alpha)(X-\zeta_3\alpha)(X-\zeta_3^2\alpha)(X-\beta)(X-\zeta_3\beta)(X-\zeta_3^2\beta). \tag{343}$$

In particular, $F = \mathbb{Q}(\zeta_3, \alpha)$. To see this, note that $\zeta_3 \in F$ since $\zeta_3 = \zeta_3\alpha/\alpha$, so $F \supseteq \mathbb{Q}(\zeta_3, \alpha)$. Conversely, observe that

$$\begin{aligned}(\alpha\beta)^3 &= \left(\frac{3-\sqrt{5}}{2}\right)\left(\frac{3+\sqrt{5}}{2}\right)\\ &= \frac{9-5}{4}\\ &= 1\end{aligned}$$

implies $(\alpha\beta)^3 = 1$. Since both α and β are *real* numbers, we must have $\alpha\beta = 1$. Thus $\beta = \alpha^{-1}$, which implies $\beta \in \mathbb{Q}(\zeta_3, \alpha)$. Clearly now, all the other roots of f are in $\mathbb{Q}(\zeta_3, \alpha)$ as well. Thus we may rewrite (343) as

$$f(X) = (X-\alpha)(X-\zeta_3\alpha)(X-\zeta_3^2\alpha)(X-\alpha^{-1})(X-\zeta_3\alpha^{-1})(X-\zeta_3^2\alpha^{-1}). \tag{344}$$

Problem 2.a

Exercise 19. Show that complex conjugation is a nontrivial automorphism of F.

Solution 12. Note that complex conjugation is an automorphism of F which fixes $\mathbb{Q}$ since it is an automorphism of $\mathbb{C}$ which fixes $\mathbb{Q}$ and $F/\mathbb{Q}$ is Galois. That complex conjugation is nontrivial follows from the fact that F contains a nonreal complex number, namely ζ_3. So complex conjugation will send ζ_3 to $\overline{\zeta_3}$, and $\zeta_3 \neq \overline{\zeta_3}$.

Problem 2.b

Exercise 20. If γ is a real root of this polynomial, show that the map induced by $\gamma \mapsto \gamma^{-1}$ gives rise to an automorphism of $\mathbb{Q}(\gamma)$.

Solution 13. From the polynomial factorization (344), we see that the real roots of f are given by α and α^{-1}. Without loss of generality, assume $\gamma = \alpha$. Then $\alpha \mapsto \alpha^{-1}$ induces the automorphism $\varphi \colon \mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha^{-1}] = \mathbb{Q}[\alpha]$ given by

$$\varphi(\pi(\alpha)) = \pi(\alpha^{-1})$$

for all $\pi(\alpha) \in \mathbb{Q}[\alpha]$.

Problem 2.c

Exercise 21. Show that $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] = 12$.

Solution 14. Since $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$, we know from a previous HW that $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] \leq 12$. Therefore

$$\begin{aligned}12 &\geq [\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}]\\ &= [\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]\\ &= [\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}(\alpha)] \cdot 6\\ &\geq 12,\end{aligned}$$

where the last inequality follows from the fact that ζ_3 is a nonreal complex number and $\mathbb{Q}(\alpha)$ consists of real numbers (so $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}(\alpha)] \geq 2$). It follows that $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] = 12$.

Problem 2.d

Exercise 22. Find $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \alpha)/\mathbb{Q})$.

Solution 15. Any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_3, \alpha)$ is completely determined by where it sends ζ_3 and where it sends α. There are 2 places to send ζ_3, namely ζ_3 and ζ_3^2. Similarly, there are 6 places to send α, namely α, $\zeta_3\alpha$, $\zeta_3^2\alpha$, α^{-1}, $\zeta_3\alpha^{-1}$ and $\zeta_3^2\alpha^{-1}$. In total, there are $2 \cdot 6 = 12$ possible automorphisms. In fact all such possibilities are realized since $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}] = 12$. Let us describe them now:

For $a \in (\mathbb{Z}/3\mathbb{Z})^\times$ and $b \in \mathbb{Z}/3\mathbb{Z}$, let $\sigma_{a,b}^{\pm} \colon \mathbb{Q}(\zeta_3, \alpha) \to \mathbb{Q}(\zeta_3, \alpha)$ be the $\mathbb{Q}$-automorphism which sends ζ_3 to ζ_3^a and α to $\zeta_3^b\alpha^{\pm}$ (any such $\mathbb{Q}$-automorphism has a unique expression of this form). By a direct calculation, we have

$$\begin{aligned}
\sigma_{a,b}^{+}\sigma_{a',b'}^{+} &= \sigma_{aa',b+ab'}^{+} \\
\sigma_{a,b}^{-}\sigma_{a',b'}^{+} &= \sigma_{aa',b+ab'}^{-} \\
\sigma_{a,b}^{+}\sigma_{a',b'}^{-} &= \sigma_{aa',b+ab'}^{-} \\
\sigma_{a,b}^{-}\sigma_{a',b'}^{-} &= \sigma_{aa',b+ab'}^{+}
\end{aligned}$$

The multiplcation rules above behaves just like matrix multiplication (with a sign involved):

$$\begin{aligned}
\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix} \\
-\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} &= -\begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix} \\
\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\left(-\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}\right) &= -\begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix} \\
\left(-\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\right)\left(-\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}\right) &= \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

So we have an isomorphism from

$$\mathbb{Z}_2 \times \mathrm{Aff}(\mathbb{Z}_3) \cong \left\{ \pm \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/3\mathbb{Z})^\times,\ b \in \mathbb{Z}/3\mathbb{Z} \right\}$$

to $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \alpha)/\mathbb{Q})$ given by $\sigma_{a,b}^{\pm} \mapsto \pm\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$.

Problem 2.e

Exercise 23. Find an explicit formula for the roots of $f(X)$.

Solution 16. This was done above.

81.6 Extension over $\mathbb{Q}$ given by $f = x^6 - x^3 + 1$

Let $f(X) = X^6 - X^3 + 1$ and let F be the splitting field of F over $\mathbb{Q}$. Observe that $f(-X) = X^6 + X^3 + 1$. This is just the 9th cyclotomic polynomial. Thus if we let $\zeta_9 = e^{2\pi i/9}$, then we have

$$\begin{aligned}
f(-X) &= X^6 + X^3 + 1 \\
&= (X - \zeta_9)(X - \zeta_9^2)(X - \zeta_9^4)(X - \zeta_9^5)(X - \zeta_9^7)(X - \zeta_9^8).
\end{aligned}$$

In other words,

$$\begin{aligned}
f(X) &= (-X - \zeta_9)(X - \zeta_9^2)(-X - \zeta_9^4)(-X - \zeta_9^5)(-X - \zeta_9^7)(-X - \zeta_9^8) \\
&= (X + \zeta_9)(X + \zeta_9^2)(X + \zeta_9^4)(X + \zeta_9^5)(X + \zeta_9^7)(X + \zeta_9^8)
\end{aligned}$$

In particular, $F = \mathbb{Q}(\zeta_9)$.

Problem 3.a

Exercise 24. Show that there is an intermediate field E such that $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\zeta_9)$ with $[E : \mathbb{Q}] = 2$.

Solution 17. Observe that $\zeta_3 \in \mathbb{Q}(\zeta_9)$ since $\zeta_9^2 = \zeta_3$. Thus $\mathbb{Q}(\zeta_9)$ contains $\mathbb{Q}(\zeta_3)$, which is a degree 2 extension over $\mathbb{Q}$.

Problem 3.b

Exercise 25. Find the Galois group of $(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ and list all of the intermediate fields.

Solution 18. Any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_9)$ is completely determined by where it sends ζ_9. There are are 6 places to send ζ_9 (namely ζ_9^a where $a \in (\mathbb{Z}/9\mathbb{Z})^\times$). So in total, there are 6 possible automorphisms. In fact all such possibilities are realized since $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6$. Let us describe them now:

For $a \in (\mathbb{Z}/9\mathbb{Z})^\times$, let $\sigma_a \colon \mathbb{Q}(\zeta_9) \to \mathbb{Q}(\zeta_9)$ be the $\mathbb{Q}$-automorphism which sends ζ_9 to ζ_9^a. By a direct calculation, we have

$$\sigma_a \sigma_{a'} = \sigma_{aa}$$

for all $a, a' \in (\mathbb{Z}/9\mathbb{Z})^\times$, where the multiplication in the subscript is taken modulo 9. Thus we have an isomorphism from $(\mathbb{Z}/9\mathbb{Z})^\times$ to $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ given by $\sigma_a \mapsto a$. Below is the lattice of subgroups of $(\mathbb{Z}/9\mathbb{Z})^\times$

$$\begin{tikzcd}[arrows=dash] & \{1\} \arrow[dl] \arrow[dr] & \\ \{1,4,7\} \arrow[dr] & & \{1,8\} \arrow[dl] \\ & \{1,2,4,5,7,8\} & \end{tikzcd}$$

These correspond to the squares in $(\mathbb{Z}/9\mathbb{Z})^\times$ and the cubes in $(\mathbb{Z}/9\mathbb{Z})^\times$ respectively. The corresponding lattice of fields is given by

$$\begin{tikzcd}[arrows=dash] & \mathbb{Q}(\zeta_9) \arrow[dl] \arrow[dr] & \\ \mathbb{Q}(\zeta_3) \arrow[dr] & & \mathbb{Q}(\zeta_9^{-1} + \zeta_9) \arrow[dl] \\ & \mathbb{Q} & \end{tikzcd}$$

Problem 3.c

Exercise 26. Find an explicit formula for the roots of $f(X)$.

Solution 19. This was done above.

82 Homework 10

82.1 Criterion for separable extension

Proposition 82.1. *Let F/K be a finite field extension of degree n. Suppose K has characteristic $p > 0$ and p does not divide n. Then F is separable over K.*

Proof. Assume for a contradiction that F/K is inseparable. Choose $\alpha \in F$ such that α is inseparable over K. Then the minimal polynomial of α over K must have the form

$$\pi_{\alpha,K}(X) = X^{pm} + a_{m-1}X^{p(m-1)} + \cdots + a_1 X^p + a_0,$$

where $a_0, a_1, \ldots, a_{m-1} \in K$ and $d > 0$. Here we are using the fact that an irreducible polynomial over a field is separable if and only if its derivative is not equal zero (if you need to see a proof of this, then please see the Appendix problem 1.a). In particular, $[K(\alpha) : K] = pm$. But this implies $p \mid n$ since

$$\begin{aligned} n &= [F : K] \\ &= [F : K(\alpha)][K(\alpha) : K] \\ &= [F : K(\alpha)]pm. \end{aligned}$$

This is a contradiction. □

Proposition 82.2. *Let F/K be a field extension and suppose K has characteristic $p > 0$. Let $\alpha \in F$ be algebraic over K. The α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all $n \geq 1$.*

Proof. Suppose α is separable. Then since $K(\alpha)/K$ is a separable extension. This implies $K(\alpha)/K(\alpha^p)$ is a separable extension (if you need to see a proof of this, then please see the Appendix problem 1.b). Let $\pi(X)$ be the minimal polynomial of α over $K(\alpha^p)$. Observe that α is a root of the polynomial $X^p - \alpha^p = (X-\alpha)^p$ over $K(\alpha^p)$. This implies $\pi(X) \mid (X-\alpha)^p$ which implies $\pi(X) \mid (X-\alpha)$ since π is irreducible. Thus $\pi(X) = X - \alpha$ which implies $[K(\alpha) : K(\alpha^p)] = 1$ and hence $K(\alpha) = K(\alpha^p)$. Since α^p is also separable over K, we can proceed by induction and obtain

$$\begin{aligned} K(\alpha) &= K(\alpha^p) \\ &= K(\alpha^{p^2}) \\ &\vdots \\ &= K(\alpha^{p^n}) \end{aligned}$$

for all $n \geq 1$.

Conversely, suppose $K(\alpha) = K(\alpha^{p^n})$ for all $n \geq 1$ and assume for a contradiction that α is not separable. Then the minimal polynomial of α over K must have the form

$$\pi_{\alpha,K}(X) = X^{pm} + a_{m-1}X^{p(m-1)} + \cdots + a_1 X^p + a_0.$$

Observe that α^p is a root of the monic polynomial

$$\pi_{\alpha,K}(X^{1/p}) = X^m + a_{m-1}X^{(m-1)} + \cdots + a_1 X + a_0.$$

In fact, $\pi_{\alpha,K}(X^{1/p})$ is irreducible since $\pi_{\alpha,K}(X)$ is irreducible (if $\pi_{\alpha,K}(X^{1/p}) = fg$ with $\deg f, \deg g < \deg \pi_{\alpha,K}(X^{1/p})$ then $\pi_{\alpha,K} = f(X^p)g(X^p)$). Thus $\pi_{\alpha,K}(X^{1/p})$ is the minimal polynomial of α^p. In particular, this implies

$$\begin{aligned} [K(\alpha) : K] &= pm \\ &> m \\ &\geq [K(\alpha^p) : K] \\ &= [K(\alpha) : K], \end{aligned}$$

which is a contradiction. □

82.2 Absolute galois group of finite field is abelian

Problem 2.a

Proposition 82.3. *Let K be a finite field and let F be an algebraic closure of K. Then* $\mathrm{Gal}(F/K)$ *is abelian.*

Proof. Let $\sigma, \tau \in \mathrm{Gal}(F/K)$ and suppose $\sigma\tau \neq \tau\sigma$. Choose $\alpha \in F$ such that $\sigma\tau(\alpha) \neq \tau\sigma(\alpha)$. Let E/K be a finite Galois extension such that $\alpha \in E$. Then $\sigma|_E \tau|_E \neq \tau|_E \sigma|_E$ since $\sigma\tau(\alpha) \neq \tau\sigma(\alpha)$. This is a contradiction since every finite Galois extension over K is cyclic (and in particular abelian). □

Problem 2.b

Proposition 82.4. *Let K be a finite field, let F be an algebraic closure of K, and let $\sigma \in$* $\mathrm{Gal}(F/K)\backslash\{1\}$. *Then σ has infinite order.*

Proof. Assume for a contradiction that σ has finite order, say $\mathrm{ord}(\sigma) = m$. Choose an element $\alpha \in F$ such that $\sigma(\alpha) \neq \alpha$ (this is possible since $\sigma \neq 1$). Also, choose a positive integer n which relatively prime to m and choose a finite field extension L/F of degree $[L : F] = n$ such that $\alpha \in L$. Note that L/F is necessarily a Galois extension (by classification theorem of finite fields) with Galois group $\mathrm{Gal}(L/F) \cong \mathbb{Z}/n\mathbb{Z}$. Define $\rho_L \colon \mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$ to be the restriction map, given by

$$\rho_L(\tau) = \tau|_L$$

for all $\tau \in \mathrm{Gal}(F/K)$. Then ρ_L is clearly a homomorphism of groups, and so in particular, $\mathrm{ord}(\rho_L(\sigma)) \mid m$. Since $\mathrm{Gal}(L/K)$ is cyclic of order n (which is relatively prime to m), we see that $\mathrm{ord}(\rho_L(\sigma)) = 1$. But $\alpha \in L$ and

$$\begin{aligned} \alpha &\neq \sigma(\alpha) \\ &= \sigma|_L(\alpha) \\ &= \rho_L(\sigma)(\alpha). \end{aligned}$$

Thus $\rho_L(\sigma)$ cannot have order 1, which is a contradiction. □

82.3 If α separable and β totally separable then $K(\alpha+\beta) = K(\alpha,\beta)$ and if also $\alpha \neq 0 \neq \beta$ then $K(\alpha\beta) = K(\alpha,\beta)$

Proposition 82.5. *Let F be an extension of K and $\alpha, \beta \in F$ such that α is separable over K and β is totally inseparable over K. Then $K(\alpha+\beta) = K(\alpha,\beta)$. Moreover, if both α and β are nonzero, then $K(\alpha,\beta) = K(\alpha\beta)$.*

Proof. First we show $K(\alpha+\beta) = K(\alpha,\beta)$. The direction $K(\alpha+\beta) \subseteq K(\alpha,\beta)$ is clear, so it suffices to show $K(\alpha+\beta) \supseteq K(\alpha,\beta)$. To do this, we just need to show that $\alpha, \beta \in K(\alpha+\beta)$. We may assume $\operatorname{char} K = p$. Since β is totally inseparable over K, we have $\beta^{p^m} = b$ for some $m \geq 0$ and $b \in K$. Observe that

$$\begin{aligned}
\alpha^{p^m} &= ((\alpha+\beta)-\beta)^{p^m} \\
&= (\alpha+\beta)^{p^m} - b \\
&\in K(\alpha+\beta).
\end{aligned}$$

Therefore the element α is purely inseparable over $K(\alpha+\beta)$; but since α is separable over K, then α is also separable over $K(\alpha+\beta)$. Thus $\alpha \in K(\alpha+\beta)$, which implies $\beta = (\alpha+\beta) - \alpha \in K(\alpha+\beta)$.

Now suppose $\alpha \neq 0 \neq \beta$. We will show $K(\alpha\beta) = K(\alpha,\beta)$. The direction $K(\alpha\beta) \subseteq K(\alpha,\beta)$ is clear, so it suffices to show $K(\alpha\beta) \supseteq K(\alpha,\beta)$. To do this, we just need to show that $\alpha, \beta \in K(\alpha\beta)$. Observe that

$$\begin{aligned}
\alpha^{p^m} &= (\alpha\beta\beta^{-1})^{p^m} \\
&= (\alpha\beta)^{p^m} b^{-1} \\
&\in K(\alpha\beta).
\end{aligned}$$

Therefore the element α is purely inseparable over $K(\alpha\beta)$; but since α is separable over K, then α is also separable over $K(\alpha\beta)$. Thus $\alpha \in K(\alpha\beta)$, which implies $\beta = \alpha\beta\alpha^{-1} \in K(\alpha\beta)$. □

Appendix

82.4 Criterion for separability

Proposition 82.6. *Let K be a field and let $\pi(X)$ be an irreducible polynomial in $K[X]$. Then $\pi(X)$ is separable over K if and only if $\pi'(X) \neq 0$. In particular, when K has characteristic p, then $\pi(X)$ is separable if and only if it is not a polynomial in X^p.*

Proof. Separability is equivalent to $\gcd(\pi(X), \pi'(X)) = 1$. If $\pi(X)$ and $\pi'(X)$ are not relatively prime, then $\pi(X) \mid \pi'(X)$ since $\pi(X)$ is irreducible. Taking the derivative drops degrees, so having $\pi'(X)$ being divisible by $\pi(X)$ forces $\pi'(X) = 0$. Conversely, if $\pi'(X) = 0$, then $\gcd(\pi(X), \pi'(X)) = \pi(X)$ is nonconstant, so $\pi(X)$ is inseparable. Thus separability of $\pi(X)$ is equivalent to $\pi'(X) \neq 0$.

When K has characteristic 0, every irreducible over K has nonzero derivative since any nonconstant polynomial has nonzero derivative. So all irreducibles over K are separable.

Now suppose K has characteristic p. Writing

$$\pi(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 T + a_0,$$

the condition $\pi'(X) = 0$ means $ia_i = 0$ in K for $0 \leq i \leq n$. This implies $p \mid i$ whenever $a_i \neq 0$, so the only nonzero terms in $\pi(X)$ occur in degrees divisible by p. In particular, $n = \deg \pi$ is a multiple of p, say $n = pm$. Write each exponent of a nonzero term in $\pi(X)$ as a multiple of p:

$$\pi(X) = X^{pm} + a_{p(m-1)}X^{p(m-1)} + \cdots + a_p X^p + a_0 = g(X^p)$$

where $g(X) \in K[X]$. So $\pi(X) \in K[X^p]$. Conversely, if $\pi(X) = g(X^p)$ is a polynomial in X^p, then $\pi'(X) = g'(X^p)pX^{p-1} = 0$, so $\pi(X)$ is inseparable in $K[X]$. □

Problem 1.b

Proposition 82.7. *Let $F \subseteq K \subseteq L$ be an extension of fields. Suppose L/F is a separable extension. Then L/K is a separable extension.*

Proof. Let $\alpha \in L$, let $\pi_{\alpha,K}(X)$ be the minimal polynomial of α over K, and let $\pi_{\alpha,F}(X)$ be the minimal polynomial of α over F. Then $\pi_{\alpha,K} \mid \pi_{\alpha,F}$ in $K[X]$, so

$$\pi_{\alpha,K}(X)g(X) = \pi_{\alpha,F}(X) \tag{345}$$

for some $g(X) \in K[X]$. Now differentiate both sides of (79) and set $X = \alpha$ to get

$$\pi'_{\alpha,K}(\alpha)g(\alpha) = \pi'_{\alpha,F}(\alpha).$$

Observe that $\pi'_{\alpha,F}(\alpha) \neq 0$ since this would imply $\pi_{\alpha,F} \mid \pi'_{\alpha,F}$ would contradict separability of α over F. Similarly $g(\alpha) \neq 0$ since this would imply $\pi_{\alpha,K} \mid g$ which would imply $\pi^2_{\alpha,K} \mid \pi_{\alpha,F}$ which would again contradict separability of α over F. Thus we have $\pi'_{\alpha,K}(\alpha) \neq 0$. In particular $\pi'_{\alpha,K}(X) \neq 0$, which implies α is separable over K. □

82.5 Galois group as inverse limit

Proposition 82.8. *Let K be a field and let K^{sep} be a separable closure of K. We define a preordered set $(\mathcal{G}_{K^{\mathrm{sep}}/K}, \subseteq_K)$ as follows: the underlying set is defined to be*

$$\mathcal{G}_{K^{\mathrm{sep}}/K} = \{L/K \mid L/K \text{ is finite Galois extension such that } K \subseteq L \subseteq K^{\mathrm{sep}}\}.$$

If K^{sep} and K are understood, then we simply write $\mathcal{G}$ instead of $\mathcal{G}_{K^{\mathrm{sep}}/K}$. The preorder $\subseteq_K$ is set inclusion: we shall write write $L \subseteq_K L'$ as shorthand for saying $K \subseteq L \subseteq L' \subseteq K^{\mathrm{sep}}$ with L/K and L'/K Galois. Finally, for each $L \subseteq_K L'$, we define $\rho_{L,L'} \colon \mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K)$ to be the restriction map:

$$\rho_{L,L'}(\sigma) = \sigma|_L$$

for all $\sigma \in \mathrm{Gal}(L'/K)$. With this terminology fixed, let $(\mathrm{Gal}(L/K), \rho_{L,L'})$ be an inverse system indexed over $(\mathcal{G}, \subseteq_K)$. Then

$$\mathrm{Gal}(K^{\mathrm{sep}}/K) \cong \varprojlim \mathrm{Gal}(L/K).$$

Proof. We define $\Psi \colon \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \varprojlim \mathrm{Gal}(L/K)$ by

$$\Psi(\sigma) = (\sigma|_L)_{\mathcal{G}}$$

for all $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$. It's easy to see that the collection $(\sigma|_L)_{\mathcal{G}}$ really is an element of $\varprojlim \mathrm{Gal}(L/K)$. Indeed, if $L \subseteq_K L'$, then $\rho_{L,L'}(\sigma|_{L'}) = \sigma|_L$. It's also easy to see that Ψ is a group homomorphism: if $\sigma, \tau \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$, then

$$\begin{aligned} \Psi(\sigma\tau) &= ((\sigma\tau)|_L)_{\mathcal{G}} \\ &= (\sigma|_L \tau|_L)_{\mathcal{G}} \\ &= (\sigma|_L)_{\mathcal{G}}(\tau|_L)_{\mathcal{G}} \\ &= \Psi(\sigma)\Psi(\tau). \end{aligned}$$

Let us check that Ψ is injective. Suppose $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and $\sigma|_L = 1|_L$ for all $L \in \mathcal{G}$. To see that σ is the identity, we assume for a contradiction that $\sigma \neq 1$. Choose $\alpha \in \overline{K}$ such that $\sigma(\alpha) \neq \alpha$ (such an α must exist since $\sigma \neq 1$). Then α must be contained in some finite Galois extension, say L/K, but $\sigma|_L = 1|_L$, which contradicts the fact that $\sigma(\alpha) \neq \alpha$. Thus Ψ is injective.

Now let us check that Ψ is surjective. Let $(\sigma_L)_{\mathcal{G}}$ be an element in $\varprojlim \mathrm{Gal}(L/K)$. We *define* $\sigma \colon K^{\mathrm{sep}} \to K^{\mathrm{sep}}$ as follows: for any $\alpha \in K^{\mathrm{sep}}$, we choose a finite Galois extension L/K such that $\alpha \in L$. Then we set

$$\sigma(\alpha) = \sigma_L(\alpha). \tag{346}$$

We must check that (346) is well-defined. Suppose L'/K is another finite Galois extension such that $\alpha \in L'$. Then $L \cap L'/K$ is a finite Galois extension with $\alpha \in L \cap L'$, and moreover we have

$$\begin{aligned} \sigma_{L'}(\alpha) &= \sigma_{L'}(\alpha)|_{L\cap L'} \\ &= \sigma_{L\cap L'}(\alpha) \\ &= \sigma_L(\alpha)|_{L\cap L'} \\ &= \sigma_L(\alpha). \end{aligned}$$

Thus (346) is well-defined. □

Corollary 76. *Let F be a finite and let $\overline{F}$ be a choice of an algebraic closure of F. Then*

$$\mathrm{Gal}(\overline{F}/F) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z}) \cong \prod_p \mathbb{Z}_p.$$

Proof. First note that since F is a finite field (and hence perfect), our choice of an algebraic closure of F is also a separable closure of F. By the classification result for finite fields, there exists a prime p and a positive integer k such that $F \cong \mathbb{F}_q$ where $q = p^k$. Let $\sigma\colon F \to \mathbb{F}_q$ denote this isomorphism. We can extend σ to an isomorphism $\widetilde{\sigma}\colon \overline{F} \to \mathbb{F}_{q^\infty}$ which restrict to $\sigma\colon F \to \mathbb{F}_q$. Then observe that

$$\mathrm{Gal}(\mathbb{F}_{q^\infty}/\mathbb{F}_q) = \widetilde{\sigma}\mathrm{Gal}(\overline{F}/F)\widetilde{\sigma}^{-1}.$$

So it suffices to show that

$$\mathrm{Gal}(\mathbb{F}_{q^\infty}/\mathbb{F}_q) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z}) \cong \prod_p \mathbb{Z}_p.$$

Now the isomorphism on left holds since every every $L \in \mathcal{G}_{\mathbb{F}_{q^\infty}/\mathbb{F}_q}$ has the form $L = \mathbb{F}_{q^n}$ where $n \geq 1$ and moreover, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. The isomorphism on the right holds because the Chinese Remainder Theorem and the fact inverse limits commute with finite products:

$$\begin{aligned}
\varprojlim_n (\mathbb{Z}/n\mathbb{Z}) &\cong \varprojlim_{n=p_1^{e_1}\cdots p_k^{e_k}} (\mathbb{Z}/p_1^{e_1}\cdots p_k^{e_K}\mathbb{Z}) \\
&\cong \varprojlim_{n=p_1^{e_1}\cdots p_k^{e_k}} (\mathbb{Z}/(p_1^{e_1}\mathbb{Z}) \times \cdots\cdots \mathbb{Z}/(p_k^{e_K}\mathbb{Z})) \\
&\cong \varprojlim_{p_1^{e_k}} (\mathbb{Z}/(p_1^{e_1}\mathbb{Z})) \times \cdots\cdots \varprojlim_{p_1^{e_k}} (\mathbb{Z}/(p_k^{e_K}\mathbb{Z})) \\
&\cong \prod_p \mathbb{Z}_p
\end{aligned}$$

□

83 Homework 11

83.1 Equivalent criteria for valuation domain

Proposition 83.1. *Let A be a domain and let K be its quotient field. The following conditions are equivalent*

1. *For all nonzero $a, b \in A$, either $a \mid b$ or $b \mid a$;*
2. *For all nonzero $x \in K$, either x or x^{-1} is in A;*
3. *There is a valuation v on K such that $A = \{x \in K \mid v(x) \geq 0\} \cup \{0\}$.*

Proof. ($1 \implies 2$): Let $x \in K^\times$. Write $x = a/b$ where $a, b \in A \backslash \{0\}$. Then either $a \mid b$ or $b \mid a$. If $b \mid a$, then we can write $a = bc$ for some nonzero $c \in A$. In this case, we have

$$\begin{aligned}
x &= a/b \\
&= bc/b \\
&= c,
\end{aligned}$$

and hence $x \in A$. On the other hand, if $a \mid b$, then we can write $b = ad$ for some nonzero $d \in A$. In this case, we have

$$\begin{aligned}
x^{-1} &= b/a \\
&= ad/a \\
&= d,
\end{aligned}$$

and hence $x^{-1} \in A$.

($2 \implies 3$): Let $\Gamma = K^\times/A^\times$. We define a total ordering on Γ as follows: Let $\overline{x}, \overline{y} \in \Gamma$. We say

$$\overline{x} \geq \overline{y} \text{ if and only if } xy^{-1} \in A. \tag{347}$$

Let us check that (81) is well-defined. Suppose xa and yb are two different representatives of the cosets $\overline{x}$ and $\overline{y}$ respectively, where $a, b \in A^\times$. Then

$$\begin{aligned}
(xa)(yb)^{-1} &= (xa)(b^{-1}y^{-1}) \\
&= (xy^{-1})(ab^{-1}) \\
&\in A
\end{aligned}$$

implies $\overline{xa} \geq \overline{yb}$. Thus (81) is well-defined. Next, observe that the relation given in (81) is antisymmetric: if $\overline{x} \geq \overline{y}$ and $\overline{y} \geq \overline{x}$, then $xy^{-1} \in A$ and $yx^{-1} \in A$, which implies $xy^{-1} \in A^{\times}$, and hence

$$\begin{aligned}\overline{x} &= \overline{x(yy^{-1})} \\ &= \overline{(xy^{-1})y} \\ &= \overline{y}.\end{aligned}$$

It is also transitive: if $\overline{x} \geq \overline{y}$ and $\overline{y} \geq \overline{z}$, then

$$\begin{aligned}xz^{-1} &= x(y^{-1}y)z^{-1} \\ &= (xy^{-1})(yz^{-1}) \\ &\in A,\end{aligned}$$

which implies $\overline{x} \geq \overline{z}$. It is also a total relation since either $\overline{x} \geq \overline{y}$ or $\overline{y} \geq \overline{x}$ (since either $xy^{-1} \in A$ or $yx^{-1} \in A$ by our assumption). Thus (81) gives us a total ordering on Γ.

Now we define $v \colon K^{\times} \to \Gamma$ to be the natural quotient map. Clearly v is a surjective homomorphism. We also have

$$v(x+y) \geq \min\{v(x), v(y)\} \text{ with equality if } v(x) \neq v(y).$$

Indeed, assume without loss of generality that $v(y) \geq v(x)$, so $v(x) = \min\{v(x), v(y)\}$. Then $(x+y)x^{-1} = 1 + yx^{-1} \in A$ implies $v(x+y) \geq v(x)$. Now assume $v(x) \neq v(y)$, so $yx^{-1} \notin A$. Then $x^{-1}(x+y) = 1 + yx^{-1} \notin A$. This implies $x(x+y)^{-1} \in A$ (by our assumption). Thus $v(x) \geq v(x+y)$, which implies $v(x) = v(x+y)$ by antisymmetry of $\geq$. Finally, we observe that

$$A^{\times} = \{x \in K \mid v(x) = 0\}$$

by construction. Moreover, we have

$$A = \{x \in K \mid v(x) \geq 0\} \cup \{0\},$$

since $v(x) \geq 0$ if and only if $v(x) \geq v(1)$ if and only if $x \in A$.

(3 $\implies$ 1): Let $(\Gamma, \geq)$ be a totally ordered abelian group and let $v \colon K^{\times} \to \Gamma$ be such a valuation. Suppose $a, b \in A \backslash \{0\}$, and without loss of generality, assume that $v(b) \geq v(a)$. Then

$$\begin{aligned}v(ba^{-1}) &= v(b) - v(a) \\ &\geq 0\end{aligned}$$

implies $ba^{-1} \in A$. In particular, this implies $a \mid b$. □

83.2 Integral closure equals intersection of all valuation overrings

Proposition 83.2. *Let A be an integral domain, let K be its quotient field, and let $\overline{A}$ be the integral closure of A in K. Then*

1. *$\overline{A}$ is integrally closed in K.*
2. *$\overline{A} \subseteq \bigcap_{A \subseteq B \subseteq K} B$ where the intersection runs over all valuation overrings B of A.*
3. *$\overline{A} = \bigcap_{A \subseteq B \subseteq K} B$ where the intersection runs over all valuation overrings B of A.*

Proof. 1. This follows from transitivity of integral extensions (see Appendix for proof of this). Indeed, let $x \in K$ be integral over $\overline{A}$. Then since $\overline{A}[x]$ is integral over $\overline{A}$ and since $\overline{A}$ is integral over A, we see that $\overline{A}[x]$ is integral over A. In particular, x is integral over A. This implies $x \in \overline{A}$ (by definition of integral closure). Thus $\overline{A}$ is integrally closed in K.

2. This follows from the fact the every valuation ring is integrally closed (see Appendix for proof of this). Indeed, let B be a valuation overring of A. Then since B is integrally closed and $A \subseteq B$, it follows that $\overline{A} \subseteq B$. Since B was arbitrary, we see that $\overline{A} = \bigcap_{A \subseteq B \subseteq K} B$ where the intersection runs over all valuation overrings B of A.

3. Let $x \in \bigcap_{A \subseteq B \subseteq K} B$ and assume for a contradiction that x is not integral over A. Observe that $x^{-1}A[x^{-1}]$ is a proper ideal in $A[x]$. Indeed, if $x^{-1}A[x^{-1}] = A[x^{-1}]$, then there exists $n \geq 0$ and $a_1, \dots, a_{n-1}, a_n \in A$ such that

$$a_n x^{-n} + a_{n-1} x^{-n+1} + \cdots + a_1 x^{-1} = 1. \tag{348}$$

Multiplying both sides of (55) by x^n and rearranging terms gives us

$$x^n - a_1 x^{n-1} - \cdots - a_{n-1}x - a_n = 0,$$

which contradicts the fact that x is not integral over A. Thus $x^{-1}A[x^{-1}]$ is a proper ideal in $A[x^{-1}]$. In particular, it is contained some maximal ideal, say $\mathfrak{m}$. Then there is a valuation ring $(B, \mathfrak{n})$ that dominates $(A[x^{-1}]_{\mathfrak{m}}, \mathfrak{m}A[x^{-1}]_{\mathfrak{m}})$ (see Appendix for proof of this). Since $x^{-1} \in \mathfrak{m} \subseteq \mathfrak{n}$, we see that $x \notin B$ (we can't have $x \in B$ *and* $x^{-1} \in \mathfrak{n}$ since $\mathfrak{n}$ does not contain any units). This contradicts our assumption that $x \in \bigcap_{A \subseteq B \subseteq K} B$. □

83.3 Almost integral

Exercise 27. Let A be a domain and let K be its fraction field. An element $x \in K$ is said to be **almost integral** if there is a nonzero $a \in A$ such that $ax^n \in A$ for all $n \in \mathbb{N}$. We say that a domain is **completely integrally closed** if it contains all of its almost integral elements.

1. Give an example of an element that is almost integral, but not integral.
2. Show that if $x \in K$ is integral over A, then x is almost integral over A;
3. Show that if A is Noetherian, then any almost integral element over A is integral over A;
4. Let A be a valuation domain that is not a field. Show that A is completely integrally closed if and only if A is one-dimensional (that is, every nonzero prime ideal is maximal).

Solution 20. 1. Consider ring $A = K[y, \{x/y^n \mid n \in \mathbb{N}\}]$. We have a strict inclusion of rings

$$K[x,y] \subset A \subset K[x,y,1/y].$$

In particular, A is a domain with fraction field $K(x,y)$. Note that $1/y \in K(x,y)$ is almost integral over A since $1/y \notin A$ and $x/y^n \in A$ for all $n \in \mathbb{N}$. On the other hand, $1/y$ is not integral over A. Indeed, if it were, then there would exists $m \in \mathbb{N}$ and $f_0, \dots, f_{m-1} \in A$ such that

$$\frac{1}{y^m} = \frac{f_{m-1}}{y^{m-1}} + \cdots + \frac{f_1}{y} + f_0. \tag{349}$$

Multilpying y^m on both sides of (349) gives us

$$1 = (f_{m-1} + \cdots + f_1 y^{m-2} + f_0 y^{m-1})y. \tag{350}$$

Evaluating $x = 0$ to both sides of (350) gives us

$$1 = (\widetilde{f}_{m-1} + \cdots + \widetilde{f}_1 y^{m-2} + \widetilde{f}_0 y^{m-1})y. \tag{351}$$

where $\widetilde{f}_0, \widetilde{f}_1, \dots, \widetilde{f}_{m-1}$ are polynomials over K in the variable y. Evaluating $y = 0$ to both sides of (351) gives us $1 = 0$, which is a contradiction.

2. Let $x \in K$ be integral over A. Write $x = a/b$ and choose $n \geq 1$ minimal and $a_0, a_1, \dots, a_{n-1} \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0. \tag{352}$$

We claim that for any for any $k \geq 0$, we have $b^n x^k \in A$. Indeed, first note that if $k > n$, then we can use the fact that x is integral (so $A[x] = \sum_{i=0}^{n-1} Ax^i$) to write

$$x^k = a_{n-1,k}x^{n-1} + \cdots + a_{1,k}x + a_{0,k}$$

for some $a_{0,k}, a_{1,k}, \dots, a_{n-1,k} \in A$. So it suffices to show that $b^n x^k \in A$ when $k \leq n$. This is clear though since

$$\begin{aligned} b^n x^k &= b^n \frac{a^k}{b^k} \\ &= b^{n-k}a^k \\ &\in A. \end{aligned}$$

It follows that x is almost integral over A.

3. Suppose A is a Noetherian domain and let $x \in K$ be almost integral over A. Choose $a \in A$ such that $ax^n \in A$ for all $n \in \mathbb{N}$. Consider the ascending chain of ideals, given by

$$\begin{aligned} I_0 &= \langle a \rangle \\ I_1 &= \langle a, ax \rangle \\ &\vdots \\ I_n &= \langle a, ax, \dots, ax^n \rangle \end{aligned}$$

for all $n \in \mathbb{N}$. The ascending chain of ideals (I_n) must terminate since A is Noetherian, say at $m \in \mathbb{N}$. It follows that $ax^{m+1} \in I_m$, which implies

$$ax^{m+1} = a_m ax^m + \cdots + a_1 ax + a_0 a \tag{353}$$

for some $a_0, a_1, \dots, a_m \in A$. Canceling a from both sides of (353) (we can do this since A is a domain) and rearranging terms gives us

$$x^{m+1} - a_m x^m - \cdots - a_1 x - a_0 = 0.$$

This implies x is integral over A.

4. First suppose $(A, \mathfrak{m})$ is one-dimensional valuation domain. Let $x \in K$ be almost integral over A and assume for a contradiction that $x \notin A$. Then $x^{-1} \in A$ since A is a valuation domain. Choose a nonzero $a \in A$ such that $ax^n \in A$ for all $n \in \mathbb{N}$. For each $n \in \mathbb{N}$, choose $a_n \in A$ such that $ax^n = a_n$. If a is a unit in A, then clearly $x \in A$, which is a contradiction, thus a is not a unit in A. Similarly, if x^{-1} is a unit in A, then again $x \in A$, which is a contradiction. Thus x^{-1} is also not a unit in A. We claim that $a \mid x^{-n}$ for some $n \in \mathbb{N}$. To see this, suppose that $a \nmid x^{-n}$ for all $n \in \mathbb{N}$. Then

$$\begin{aligned} x^{-1} &\notin \operatorname{rad}\langle a \rangle \\ &= \bigcap_{\substack{a \in \mathfrak{p} \\ \mathfrak{p} \text{ prime}}} \mathfrak{p} \\ &= \mathfrak{m}, \end{aligned}$$

where the last equality follows from the fact that $(A, \mathfrak{m})$ is one-dimensional local ring. Thus $x^{-1} \notin \mathfrak{m}$ which implies x^{-1} is a unit in A, a contradiction. Thus $a \mid x^{-n}$ for some $n \in \mathbb{N}$. Choose such an $n \in \mathbb{N}$ and choose $b \in A$ such that $ab = x^{-n}$. Then

$$\begin{aligned} a &= a_n x^{-n} \\ &= a_n ba, \end{aligned}$$

which implies $a_n b = 1$. That is, a_n is a unit in A, but this implies $ax^n a_n^{-1} = 1$, which impilies a is unit in A, a contradiciton.

Conversely, suppose $(A, \mathfrak{m})$ is completely integrally closed valuation domain and let $\mathfrak{p}$ be a prime ideal in A. We will show that $\mathfrak{p}$ must be the maximal ideal in A. Choose $a \in A \backslash \mathfrak{p}$. Then observe that since $\mathfrak{p}$ is a prime ideal, we must have $a^n \notin \mathfrak{p}$ for all $n \in \mathbb{N}$. Furthemore, since A is a valuation domain and since $a^n \notin \mathfrak{p}$ for all $n \in \mathbb{N}$, we see that $a^n \mid b$ for all $b \in \mathfrak{p}$ for all $n \in \mathbb{N}$. In particular, we have $\langle a^n \rangle \supset \mathfrak{p}$ for all $n \in \mathbb{N}$. In other words, we have $A \supset a^{-n}\mathfrak{p}$ for all $n \in \mathbb{N}$. So for any $b \in \mathfrak{p}$, we have $a^{-n} b \in A$ for all $n \in \mathbb{N}$. Thus a^{-1} is almost integral over A. Since A is integrally closed, we see that $a^{-1} \in A$. Thus a is a unit in A, which implies $A \backslash \mathfrak{p}$ consists of units of A. Thus $\mathfrak{p}$ must be the maximal ideal $\mathfrak{m}$.

Appendix

83.4 Transitivity of integral extensions

Transitivity of Integral Extensions

Proposition 83.3. *Let $A \subseteq B$ be a finite extension of rings. Then $A \subseteq B$ is an integral extension of rings.*

Proof. Let $b \in B$, let $\mathrm{m}_b \colon B \to B$ be the "multiplication by b" map, given by $\mathrm{m}_b(x) = bx$ for all $x \in B$, and suppose $b_1, \dots, b_n$ are generators for B as an A-module. Then for each $1 \leq i \leq n$, there exists (not necessarily unique) $a_{ji} \in A$ for all $1 \leq j \leq n$, such that

$$bb_i = \sum_{j=1}^{n} a_{ji} b_j.$$

Let $[\mathrm{m}_b] = (a_{ij})$ be there corresponding matrix representation. By the Cayley-Hamiltonian Theorem (over any commutative ring), the matrix $[\mathrm{m}_b]$ satisfies it's own characteristic polynomial, which is a monic polynomial $\chi_{[\mathrm{m}_b]}(T) \in A[T]$. In particular, this implies $\chi_{[\mathrm{m}_b]}(\mathrm{m}_b) = 0$. Note that the map $\mathrm{m}_{(-)} : B \to \mathrm{End}_A(B)$, given by $\mathrm{m}_{(-)}(b) = \mathrm{m}_b$ for all $b \in B$, is an injective A-algebra homomoprhism. Thus $\chi_{[\mathrm{m}_b]}(\mathrm{m}_b) = 0$ implies $\chi_{[\mathrm{m}_b]}(b) = 0$. Hence b integral, and since b was arbitary, this implies $A \subseteq B$ is an integral extension. □

Corollary 77. *Let $A \subset B$ be a ring extension. Then an element $b \in B$ is integral over A if and only if $A[b]$ is a finitely generated A-module.*

Proof. If b is integral over A, then there is a monic polynomial $f(T) \in A[T]$ satisfying $f(b) = 0$. Then $A[b] \cong A[T]/\langle f(T) \rangle$ as A-modules, and $A[T]/\langle f(T) \rangle$ is generated by $\overline{1}, \overline{T}, \dots, \overline{T}^{n-1}$ as an A-module, where $n = \deg f$. The converse direction follows from Proposition (83.3) □

Corollary 78. *(Transitivity of Integral Extensions) Let $A \subseteq B$ and $B \subseteq C$ be integral extensions. Then $A \subseteq C$ is an integral extension.*

Proof. Let $c \in C$. Since c is integral over B, there exists $b_0, \dots, b_{n-1} \in B$ such that

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0.$$

Then

$$A \subset A[b_0, \dots, b_{n-1}] \subset A[b_0, \dots, b_{n-1}][c]$$

is a composition of finite extensions. Thus, $A \subset A[b_0, \dots, b_{n-1}, c]$ is a finite extension, and hence an integral extension by Proposition (**??**). Therefore c is integral over A, which implies $A \subseteq C$ is an integral extension since c was arbitrary. □

83.5 Every Valuation Ring is Integrally Closed

Proposition 83.4. *Every Valuation Ring is Integrally Closed.*

Proof. Let A be a valuation ring with fraction field K and let $x \in K$ be integral over A. Then there exists $n \geq 1$ and $a_{n-1}, \dots, a_0 \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

If $x \in A$ we are done, so assume $x \notin A$. Then $x^{-1} \in A$, since A is a valuation ring. Multiplying the equation above by $x^{-(n-1)} \in A$ and moving all but the first term on the lefthand side to the righthand side yields

$$x = -a_{n-1} - \cdots - a_0 x^{-(n-1)} \in A,$$

contradicting our assumption that $x \notin A$. It follows that $x \in A$, and hence A is integrally closed. □

83.6 Domination

Definition 83.1. Let K be a field. We define a preordered set $(\mathcal{D}_K, \geq_{\mathrm{d}})$ as follows: the underlying set is defined to be

$$\mathcal{D}_K := \{A \mid A \text{ is a local domain such that } A \subseteq K\}.$$

The preorder $\leq_{\mathrm{d}}$ is defined as follows: let $A, B \in \mathcal{D}_K$. We write $B \geq_{\mathrm{d}} A$ if $B \supseteq A$ and $\mathfrak{m}_A = A \cap \mathfrak{m}_B$. In this case, we also say B **dominates** A. More generally, if R is a subring of K (so necessarily a domain), then we define a preordered set $(\mathcal{D}_{K/R}, \geq_{\mathrm{d}})$ as follows: the underlying set is defined to be

$$\mathcal{D}_{K/R} := \{A \mid A \text{ is a local domain such that } R \subseteq A \subseteq K\}.$$

The preorder $\leq_{\mathrm{d}}$ is defined as above. If $A \in \mathcal{D}_{K/R}$, then we say A is **centered** on R.

Proposition 83.5. *Let K be a field and let $A \in \mathcal{D}_K$. A maximal element in $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$ exists. Furthermore, any such maximal element is a valuation ring with K as its fraction field.*

Proof. We appeal to Zorn's Lemma. First note that $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$ is nonempty since $A \in (\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$. Let $(A_\lambda)_{\lambda \in \Lambda}$ be a totally ordered collection of local subrings of K (so $A_\mu \geq_{\mathrm{d}} A_\lambda$ for each $\mu \geq \lambda$, which means $A_\mu \supseteq A_\lambda$ and $\mathfrak{m}_\lambda = A_\lambda \cap \mathfrak{m}_\mu$ for each $\mu \geq \lambda$). Then $\bigcup_{\lambda \in \Lambda} A_\lambda$ is a local subring of K which dominates all of the A_λ. Indeed, it is straightforward to check that $\bigcup_{\lambda \in \Lambda} A_\lambda$ is a subring of K and $\bigcup_{\lambda \in \Lambda} \mathfrak{m}_\lambda$ is an ideal in $\bigcup_{\lambda \in \Lambda} A_\lambda$. To see that $\bigcup_{\lambda \in \Lambda} \mathfrak{m}_\lambda$ is the unique maximal ideal in $\bigcup_{\lambda \in \Lambda} A_\lambda$, we will show that its complement consists of units. Let $x \in \bigcup_{\lambda \in \Lambda} A_\lambda$ and suppose $x \notin \bigcup_{\lambda \in \Lambda} \mathfrak{m}_\lambda$. Since $x \in \bigcup_{\lambda \in \Lambda} A_\lambda$, there exists some λ such that $x \in A_\lambda$. Since $x \notin \bigcup_{\lambda \in \Lambda} \mathfrak{m}_\lambda$, we see that $x \notin \mathfrak{m}_\lambda$. Thus x is a unit in A_λ since $(A_\lambda, \mathfrak{m}_\lambda)$ is a local ring. It follows that x is a unit in $\bigcup_{\lambda \in \Lambda} A_\lambda$ since

$A_\lambda \subseteq \bigcup_{\lambda\in\Lambda} A_\lambda$. Thus $\bigcup_{\lambda\in\Lambda} \mathfrak{m}_\lambda$ is the unique maximal ideal in $\bigcup_{\lambda\in\Lambda} A_\lambda$. Thus every totally ordered subset of $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$ has an upper bound. It follows from Zorn's Lemma that $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$ has a maximal element.

Now we prove the latter part of the proposition. Let $(B, \mathfrak{m})$ be a maximal element in $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$. First we show B has K as its fraction field. Assume for a contradiction that K is not the fraction field of B. Choose $x \in K$ which is not in the fraction field of B. If x is transcendental over B, then $B[x]_{(x,\mathfrak{m})} \in (\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$, which contradicts maximality of B. If x is algebraic over B, then for some $b \in B$, the element bx is integral over B. In this case, the subring $B' \subseteq K$ generated by B and bx is finite over B. In particular, there exists a prime ideal $\mathfrak{m}' \subseteq B'$ lying over $\mathfrak{m}$. Then $B'_{\mathfrak{m}'}$ dominates B. In particular, this implies $B = B'_{\mathfrak{m}'}$ by maximality of B, and then x is in the fraction field of B which is a contradiction.

Finally, we show that B is a valuation ring. Let $x \in K$ and assume that $x \notin B$. Let B' denote the subring of K generated by B and x. Since B is maximal in $(\mathcal{D}_{K/A}, \geq_{\mathrm{d}})$, there is no prime of B' lying over $\mathfrak{m}$. Since $\mathfrak{m}$ is maximal we see that $\mathrm{V}(\mathfrak{m}B') = \emptyset$. Then $\mathfrak{m}B' = B'$, hence we can write

$$1 = \sum_{i=0}^{d} t_i x^i$$

with $t_i \in \mathfrak{m}$. This implies

$$(1 - t_0)(x^{-1})^d - \sum t_i (x^{-1})^{d-i} = 0.$$

In particular we see that x^{-1} is integral over B. Thus the subring B'' of K generated by B and x^{-1} is finite over B and we see that there exists a prime ideal $\mathfrak{m}'' \subseteq B''$ lying over $\mathfrak{m}$. By maximality of B, we conclude that $B = (B'')_{\mathfrak{m}''}$, and hence $x^{-1} \in B$. $\square$

Part VIII

Commutative Algebra Homework

84 Homework 1

84.1 Commutative Rng With No Maximal Ideal

Exercise 28. Given an example of a commutative ring (necessarily without identity) that does not have a maximal proper ideal.

Solution 21. Let A be any divisible group (for instance $A = \mathbb{Q}$). So $A = nA$ for every $n \in \mathbb{Z}\backslash\{0\}$. Then observe that A has no maximal proper subgroups. Indeed, assume for a contradiction that B is a maximal proper subgroup of A. Then B must have finite index in A (otherwise we can find a nonzero proper subgroup B'/B of A/B and pull this back to a proper subgroup B' of A which contains B), say $[A : B] = m$. Then we have

$$\begin{aligned} A &= mA \\ &\subseteq B \\ &\subseteq A, \end{aligned}$$

which forces $A = B$ which gives us a contradiction.

Now we turn A into a ring in a rather trivial way, namely we define multiplication on A by

$$a \cdot a' = 0$$

for all $a, a' \in A$. Clearly multiplication defined in this way gives A the structure of a commutative ring (but without an identity element). Moreover since A has no maximal proper subgroups, we see that A has no maximal ideals as a ring.

84.2 Nilradical

Exercise 29. Let R be a commutative ring with identity and let $I \subset R$ be a proper ideal of R. We denote by $\mathrm{rad}\, I$ to be the radical of I and we denote by $\mathrm{N}(R)$ to be the set of nilpotents of R.

1. Show that $\mathrm{rad}\, I$ is contained in the intersection of all prime ideals that contain I.

2. Show the other containment.

3. Show that $\mathrm{N}(R)$ is the intersection of all prime ideals of R.

Solution 22. 1. Let $x \in \operatorname{rad} I$ and let $\mathfrak{p}$ be a prime ideal in R which contains I. Choose $n \in \mathbb{N}$ such that $x^n \in I$. Then since $I \subseteq \mathfrak{p}$, we have $x^n \in \mathfrak{p}$. It follows that $x \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Since and x and $\mathfrak{p}$ were arbitrary, it follows that $\operatorname{rad} I$ is contained in all prime ideals which contains I. Thus $\operatorname{rad} I$ is contained in the intersection of all prime ideals which contains I.

2. Assume for a contradiction that

$$\operatorname{rad} I \not\supseteq \bigcap_{\substack{\mathfrak{p}\text{ prime}\\ \mathfrak{p}\supseteq I}} \mathfrak{p}.$$

Choose $x \in \bigcap_{\mathfrak{p}\supseteq I} \mathfrak{p}$ such that $x \notin \operatorname{rad} I$. Thus $x \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}$ which contain I and $x^n \notin I$ for all $n \in \mathbb{N}$. We will find a prime ideal in R which contains I but does not contain x, which will give us a contradiction.

Consider the ring obtained by localizing R at the multiplicative set $\{x^n \mid n \in \mathbb{N}\}$:

$$R_x = \{a/x^n \mid a \in \mathbb{R} \text{ and } n \in \mathbb{N}\},$$

and let $\rho\colon R \to R_x$ be the corresponding localization map, given by

$$\rho(a) = a/1$$

for all $a \in R$. Since $x^n \neq 0$ for all $n \in \mathbb{N}$, we see that $I_x = \rho(I)R_x$ is a proper ideal of R_x. In particular, there exists a prime ideal $\mathfrak{q}$ in R_x which contains I_x. Then $\rho^{-1}(\mathfrak{q})$ is a prime ideal in R which contains I but does not contain x. Indeed, if $\rho^{-1}(\mathfrak{q})$ contained x, then $\mathfrak{q}$ would contain a unit, namely $x/1$, and hence would not be prime.

3. By parts 1 and 2, we have

$$\operatorname{rad} I \neq \bigcap_{\substack{\mathfrak{p}\text{ prime}\\ \mathfrak{p}\supseteq I}} \mathfrak{p}$$

for *all* ideals I of R. In particular, since $\mathrm{N}(R) = \operatorname{rad}\langle 0\rangle$, we have

$$\mathrm{N}(R) = \bigcap_{\mathfrak{p}\text{ prime}} \mathfrak{p}.$$

84.3 Jacobson Radical

Exercise 30. Let R be a commutative ring with identity. Denote the Jacobson radical of R by $\mathrm{J}(R)$. Then $x \in \mathrm{J}(R)$ if and only if $1 + ax$ is a unit for all $a \in R$.

Solution 23. Suppose $x \in \mathrm{J}(R)$ and assume for a contradiction that $1 + ax$ is not a unit for some $a \in R$. Choose a maximal ideal in R which contains $1 + ax$, say $\mathfrak{m}$. Since $x \in \mathrm{J}(R)$, we see that in particular $x \in \mathrm{m}$. Since $1 + ax$ and ax belong to $\mathfrak{m}$, their difference also belongs to $\mathfrak{m}$. In other words, $1 \in \mathfrak{m}$. This contradicts the fact that $\mathfrak{m}$ is a proper ideal of R. Thus our original assumption was wrong, which means that $1 + ax$ is a unit for all $a \in R$.

Conversely, suppose $1 + ax$ is a unit for all $a \in R$ and assume for a contradiction that $x \notin \mathrm{J}(R)$. Choose a maximal ideal in R which does not contain x, say $\mathfrak{m}$. Then $Rx + \mathfrak{m} = R$ since $\mathfrak{m}$ is maximal. Thus there exists $a \in R$ and $y \in \mathfrak{m}$ such that $ax + y = 1$, or in other words,

$$1 - ax = y.$$

By assumption, this implies y is a unit. This contradicts the fact that $y \in \mathfrak{m}$ and $\mathfrak{m}$ is a proper ideal.

84.4 Integral Domain is Intersection of all its Localizations at Maximal Ideals

Exercise 31. Let R be an integral domain. Then

$$R = \bigcap_{\mathfrak{m}\text{ maximal}} R_{\mathfrak{m}}.$$

Solution 24. Since R is an integral domain, it has no zerodivisors. Thus all of the localization maps $\rho_{\mathfrak{m}}\colon R \to R_{\mathfrak{m}}$ are injective. In fact, they are just inclusion maps since we are identifying R and its localizations $R_{\mathfrak{m}}$ with subrings of the fraction field K of R. Thus we have

$$R \subseteq \bigcap_{\mathfrak{m}\text{ maximal}} R_{\mathfrak{m}}.$$

For the reverse inclusion, let $\gamma \in R_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ in R. Consider the set

$$R : \gamma = \{a \in R \mid a\gamma \in R\}.$$

Note that since $\gamma \in K$, we can express it as $\gamma = x/y$ where $x \in R$ and $y \neq 0$. Then it's easy to see that $y \in R : \gamma$. So $R : \gamma$ can be though of as "the set of all denominators of γ". It is easy to see that $R : \gamma$ is an ideal in R. We claim that $R : \gamma = R$. Indeed, assume for a contradiction that $R : \gamma$ is proper ideal of R. Then $R : \gamma$ is contained in a maximal ideal, say $\mathfrak{m}$. However this means that $\gamma \notin R_{\mathfrak{m}}$: if $\gamma \in R_{\mathfrak{m}}$, then we could express it as $\gamma = x/y$ where $x \in R$ and $y \notin \mathfrak{m}$. Then $y \in R : \gamma \subseteq \mathfrak{m}$ which is a contradiction. So we've found a maximal ideal $\mathfrak{m}$ such that $\gamma \notin R_{\mathfrak{m}}$ which gives us a contradiction. Thus $R : \gamma = R$. In that case, we see that $1 \in R : \gamma$, so $\gamma = 1 \cdot \gamma \in R$. Thus we have

$$R \supseteq \bigcap_{\mathfrak{m} \text{ maximal}} R_{\mathfrak{m}}.$$

85 Homework 2

85.1 An Integral Domain is a PID if and only if every Prime Ideal is Principal

Exercise 32. Let R be an integral domain. Then R is a PID if and only if every prime ideal is principal.

Solution 25. If R is a PID, then every ideal in R is principal, so every prime ideal is principal. Conversely, suppose every prime ideal is principal. Let I be an ideal in R and assume for a contradiction that I is not principal. Consider the partially order set $(\Gamma, \subseteq)$ where

$$\Gamma = \{\text{ideals } \mathfrak{a} \mid I \subseteq \mathfrak{a} \subseteq R \text{ and } \mathfrak{a} \text{ not principal}\}$$

and where $\subseteq$ is set inclusion. Note that Γ is nonempty since $I \in \Gamma$. Also note that every totally ordered subset in Γ has an upper bound. Indeed, if $(\mathfrak{a}_\lambda)_{\lambda \in \Lambda}$ is a totally ordered subset, then $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ is an upper bound of $(\mathfrak{a}_\lambda)$: the set $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ is an ideal which contains I since $(\mathfrak{a}_\lambda)$ is totally ordered and each $\mathfrak{a}_\lambda$ contains I. Also, if $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ is principal, then there must exist some $\mathfrak{a}_\lambda$ which is principal (again since $(\mathfrak{a}_\lambda)$ is totally ordered), thus $\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ is *not* principal. Hence

$$\bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda \in \Gamma.$$

Thus using Zorn's Lemma, we see that Γ has a maximal element, say $\mathfrak{p} \in \Gamma$. We claim that $\mathfrak{p}$ is a prime ideal. To see this, assume for a contradiction that $\mathfrak{p}$ is not a prime ideal. Choose $a, b \in R$ such that $ab \in \mathfrak{p}$ and $a, b \notin \mathfrak{p}$. Then observe that $\langle \mathfrak{p}, a \rangle$ and $\langle \mathfrak{p}, b \rangle$ both properly contain $\mathfrak{p}$. By maximality of $\mathfrak{p}$, they must both be principal ideals, say $\langle \mathfrak{p}, a \rangle = \langle x \rangle$ and $\langle \mathfrak{p}, b \rangle = \langle y \rangle$. Then observe that

$$\begin{aligned} \mathfrak{p} &\subseteq \langle \mathfrak{p}, a \rangle \langle \mathfrak{p}, b \rangle \\ &= (\mathfrak{p} + \langle a \rangle)(\mathfrak{p} + \langle b \rangle) \\ &= \mathfrak{p} + \langle a \rangle \mathfrak{p} + \mathfrak{p} \langle b \rangle + \langle ab \rangle \\ &\subseteq \mathfrak{p}. \end{aligned}$$

It follows that

$$\begin{aligned} \mathfrak{p} &= \langle \mathfrak{p}, a \rangle \langle \mathfrak{p}, b \rangle \\ &= \langle x \rangle \langle y \rangle \\ &= \langle xy \rangle. \end{aligned}$$

This is a contradiction since $\mathfrak{p} \in \Gamma$. Thus $\mathfrak{p}$ is a prime ideal. However by assumption *all* prime ideals are principal, so $\mathfrak{p}$ being prime implies $\mathfrak{p}$ is principal. But this again contradicts the fact that $\mathfrak{p} \in \Gamma$. Thus every ideal in R must be principal.

85.2 Noetherian Rings

Exercise 33. Let R be a commutative ring with identity. Show that the following conditions are equivalent:

1. Every ascending chain of ideals in R stabilizes: if (I_n) is ascending chain of ideals in R, meaning $I_n \subseteq I_{n+1}$ for all $n \in \mathbb{N}$, then there exists $N \in \mathbb{N}$ such that $I_N = I_n$ for all $n \geq N$.

2. Every ideal of R is finitely generated.

Solution 26. Suppose every chain of ideal in R stabilizes and let I be an ideal in R. Assume for a contradiction that I is not finitely generated. Choose any $x_1 \in I$. Since I is not finitely generated, we have

$$\langle x_1 \rangle \subset I$$

where the inclusion is proper. Next we choose $x_2 \in I \backslash \langle x_1 \rangle$. Again, since I is not finitely generated, we have

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset I$$

where each inclusion is proper. Proceeding inductively on $n \geq 3$, we choose $x_n \in I \backslash \langle x_1, \ldots, x_{n-1} \rangle$. Then since I is not finitely generated, we have

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots \subset \langle x_1, x_2, \ldots, x_n \rangle \subset I$$

where each inclusion is proper. Continuing in this manner, we construct an ascending chain of ideals

$$(\langle x_1, x_2 \ldots, x_n \rangle)_{n \in \mathbb{N}}$$

which never stabilizes since $\langle x_1, x_2, \ldots, x_n \rangle$ is properly contained in $\langle x_1, x_2, \ldots, x_n, x_{n+1} \rangle$ for all $n \in \mathbb{N}$. This contradicts the hypothesis that every chain of ideal in R stabilizes. Thus every ideal in R is finitely generated.

Now let us show the converse. Suppose every ideal in R is finitely generated. Let (I_n) be an ascending chain of ideals. Then $\bigcup_{n=1}^{\infty} I_n$ is an ideal in R since (I_n) is totally ordered, thus it must be finitely generated, say

$$\bigcup_{n=1}^{\infty} I_n = \langle x_1, \ldots, x_m \rangle.$$

Observe that $x_i \in I_{n_i}$ for some $n_i \in \mathbb{N}$ for each $1 \leq i \leq m$. Set $N = \max_{1 \leq i \leq m}\{n_i\}$. Then $x_i \in I_N$ for each $1 \leq i \leq m$ since (I_n) is totally ordered. It follows that for any $n \geq N$, we have

$$\begin{aligned} I_N &\subseteq I_n \\ &\subseteq \bigcup_{n=1}^{\infty} I_n \\ &= \langle x_1, \ldots, x_m \rangle \\ &\subseteq I_N. \end{aligned}$$

In particular we have $I_N = I_n$ for all $n \geq N$. Thus every chain of ideals in R stabilizes.

85.3 PIDs and UFDs

Exercise 34. Let R be an integral domain and let A be an overring of R: that is, $R \subseteq A \subseteq K$ where K is the field of fractions of R.

1. Show that R is a PID if and only if R is a UFD and $\dim R \leq 1$.
2. Show that if R is a UFD then any localization of R is a UFD.
3. Show that if R is a PID, then A is a localization of R.
4. Is 3 true for UFDs? Prove or give a counterexample.

Solution 27. 1. Suppose R is a UFD and $\dim R \leq 1$. If $\dim R = 0$, then R must a field: the zero ideal is prime since R is a domain and if $\dim R = 0$, then no prime ideal can contain the zero ideal, so the zero ideal must be maximal, hence $R/\langle 0 \rangle \cong R$ shows that R is a field. So we may assume $\dim R = 1$. To show that R is a PID, it suffices to show that every nonzero prime ideal in R is principal, by problem 1. But this is easy! Indeed, let $\mathfrak{p}$ be a nonzero prime ideal in R. Since R is a UFD, $\mathfrak{p}$ contains a nonzero prime element, say $p \in \mathfrak{p}$. Then we have

$$0 \subset \langle p \rangle \subseteq \mathfrak{p},$$

where the first inclusion is proper since p is nonzero. Thus R having dimension 1 forces $\langle p \rangle = \mathfrak{p}$. Thus every prime ideal in R is principal, and we are done.

Conversely, suppose R is a PID. To show that R is a UFD, we just need to show that all prime ideals in R contains a nonzero prime element. However this is clear as every prime ideal is principal and hence generated by a prime element. See the Appendix for an alternative proof of the fact that all PIDs are UFDs. It remains to show that $\dim R \leq 1$. Assume for a contradiction that $\langle p \rangle$ and $\langle q \rangle$ are prime ideals in R with p and q being nonzero prime elements in R such that $\langle q \rangle$ properly contains $\langle p \rangle$, so $p = aq$ for some $a \in R$. Since $q \notin \langle p \rangle$ we see that $a \in \langle p \rangle$ which implies $a = bp$ for some $b \in R$. Thus

$$\begin{aligned} p &= aq \\ &= bpq \\ &= pbq \end{aligned}$$

implies $1 = bq$ since R is an integral domain. However this means q is a unit, which is a contradiction since q is prime. Thus we cannot have a proper inclusion of nonzero prime ideals in R. This implies $\dim R \leq 1$.

2. Let R be a UFD and let S be a multipicatively closed subset of R. We want to show that R_S is a UFD also. To do this, we will show that every prime ideal in R_S contains a nonzero prime element. Let $\mathfrak{p}_S$ be a prime ideal in R_S where $\mathfrak{p}$ is a prime ideal in R such that $\mathfrak{p} \cap S = \emptyset$ (every prime ideal in R_S has this form by Theorem (85.2)). Since R is a UFD, the prime $\mathfrak{p}$ contains a nonzero prime element, say $p \in \mathfrak{p}$. Then the ideal generated by p is a prime ideal, and furthermore, it intersects S trivially since it is contained in $\mathfrak{p}$; that is

$$\langle p \rangle \cap S = \emptyset.$$

It follows that $\langle p \rangle_S$ is a prime ideal in R_S (again by Theorem (85.2)). Note $\langle p \rangle_S = \langle p/1 \rangle$ where $\langle p/1 \rangle$ denotes the ideal in R_S generated by $p/1$. Therefore $p/1$ is a prime element in R_S which is clearly contained in $\mathfrak{p}_S$. Thus R_S is a UFD.

3. Let $S = \{y \in R \mid 1/y \in A\}$. Observe that S is a multiplicatively closed subset of R since if $y_1, y_2 \in S$, then $y_1 y_2 \in S$ since

$$1/(y_1 y_2) = (1/y_1)(1/y_2) \in A.$$

Every element in R_S has the form x/y where $x \in R$, $1/y \in A$ and $\gcd(x, y) = 1$. Since $R \subseteq A$, we see that any $x/y \in R_S$ is an element of A, thus $R_S \subseteq A$. To show the reverse inclusion, let $x/y \in A$, where $x, y \in R$ and $\gcd(x, y) = 1$. We need to show that $1/y \in A$. Since R is a PID and $\gcd(x, y) = 1$, we have $\langle x, y \rangle = 1$. Thus there exists $a, b \in R$ such that $ax + by = 1$. Then observe that

$$\begin{aligned} \frac{1}{y} &= \frac{ax + by}{y} \\ &= a\left(\frac{x}{y}\right) + b \\ &\in A. \end{aligned}$$

It follows that $x/y \in R_S$. Thus $A \subseteq R_S$.

4. No. Let k be a field, let $R = k[X, Y]$, let $A = k[X, Y, X/Y]$, and let $K = k(X, Y)$ be the field of fractions of R. Then A is an overring of R which is contained in K. However A is not the localization of R at any multiplicative set S. Indeed, assume for a contradiction that S is a multiplicative subset of R such that $R_S = A$. Then since $X/Y \in A$, we have

$$X/Y = f/g$$

for some $f \in R$ and $g \in S$, where we may assume (by canceling common factors if necessary) that $\gcd(f, g) = 1$. Then we have

$$gX = Yf.$$

Since $K[X, Y]$ is a UFD and $\gcd(X, Y) = \gcd(f, g) = 1$, we see that $g = \alpha Y$ where $\alpha \in K^\times$. However $1/\alpha Y \notin A$, so this is a contradiction.

85.4 Appendix

85.4.1 PIDs are UFDs

Theorem 85.1. *Let R be a principal ideal domain. Then R is a unique factorization domain.*

Proof. Let a be nonzero nonunit in R. Since R is a Noetherian, an irreducible factorization of a exists, so it suffices to check that such an irreducible factorization is unique. Let

$$p_1 \cdots p_m = a = q_1 \cdots q_n \tag{354}$$

be two irreducible factorizations of a. By relabeling if necessary, we may assume that $m \leq n$. We will prove by induction on $m \geq 1$ that $m = n$ and (perhaps after relabeling) we have $p_i \sim q_i$ for all $1 \leq i \leq m$. For base case $m = 1$, we have

$$p_1 = a = q_1 \cdots q_n.$$

The first step will be to show that $n = 1$. To prove this, we assume for a contradiction that $n > 1$. Since R is a principal ideal domain, every irreducible is a prime. In particular, p_1 is prime. Thus $p_1 \mid q_i$ for some $1 \leq i \leq n$. By relabeling necessary, we may assume that $p_1 \mid q_1$. In terms of ideals, this means $\langle q_1 \rangle \subseteq \langle p_1 \rangle$. Since both $\langle q_1 \rangle$ and $\langle p_1 \rangle$ are maximal ideals, this implies $\langle q_1 \rangle = \langle p_1 \rangle$. Thus $q_1 = xp_1$ for some $x \in R^\times$. This implies

$$\begin{aligned} 0 &= p_1 - q_1 q_2 \cdots q_n \\ &= p_1 - xp_1 q_2 \cdots q_n \\ &= p_1(1 - xq_2 \cdots q_n). \end{aligned}$$

Again $p_1 \neq 0$ and R an integral domain implies $xq_2 \cdots q_n = 1$, thus $q_2 \cdots q_n \in R^\times$. This is a contradiction as each $q_2, \dots, q_n$ are irreducible! Thus $n = 1$, and clearly in this case, we have $p_1 \sim q_1$ (as $p_1 = q_1$).

Now suppose $m > 1$ and we have shown that if a has an irreducible factorization of length k where $1 \leq k < m$, then it has a unique irreducible factorization. Again, let (38) be two irreducible factorizations of a where we may assume that $m \leq n$. Arguing as above, p_1 is prime, and since $q_1 \cdots q_n \in \langle p_1 \rangle$, we must have $q_i \in \langle p \rangle$ for some $1 \leq i \leq n$. By rebaling if necessary, we may assume that $q_1 \in \langle p_1 \rangle$. Thus $\langle q_1 \rangle \subseteq \langle p_1 \rangle$, and since both $\langle q_1 \rangle$ and $\langle p_1 \rangle$ are maximal ideals, we must in fact have $\langle q_1 \rangle = \langle p_1 \rangle$. In particular, $q_1 = p_1 x$ for some $x \in R^\times$. This implies

$$\begin{aligned} 0 &= p_1 p_2 \cdots p_m - q_1 q_2 \cdots q_n \\ &= p_1 p_2 \cdots p_m - p_1 x q_2 \cdots q_n \\ &= p_1(p_2 \cdots p_m - xq_2 \cdots q_n). \end{aligned}$$

Since $p_1 \neq 0$ and R is an integral domain, this implies

$$p_2 \cdots p_m = xq_2 \cdots q_n.$$

Note that xq_2 is an irreducible element, and thus we may apply induction step to get $m = n$ and (perhaps after relabeling) $p_i \sim q_i$ for all $2 \leq i \leq m$. Since already we have $p_1 \sim q_1$, we are done. □

85.4.2 Prime Ideals in R_S

Theorem 85.2. *Let S be a multiplicatively closed subset of R. Then we have a bijection*

$$\Psi \colon \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \emptyset\} \to \operatorname{Spec} R_S$$

given by $\Psi(\mathfrak{p}) = \mathfrak{p}_S$ for all prime ideals $\mathfrak{p}$ in R such that $\mathfrak{p} \cap S = \emptyset$. Then inverse to Ψ, which we denote by

$$\Phi \colon \operatorname{Spec} R_S \to \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \emptyset\}$$

is given by $\Phi(\mathfrak{q}) = \rho^{-1}(\mathfrak{q})$ for all prime ideals $\mathfrak{q}$ in R_S where $\rho \colon R \to R_S$ is the canonical localization map.

Proof. First note that both Ψ and Φ land in their designated target spaces. Indeed, for any prime ideal $\mathfrak{q}$ in $\operatorname{Spec} R_S$, the ideal $\rho^{-1}(\mathfrak{q})$ is easily seen to be prime in R. Also if $\mathfrak{p}$ is a prime ideal in R such that $\mathfrak{p} \cap S = \emptyset$, then $\mathfrak{p}_S$ is a prime ideal in R_S. Indeed, let $x/s, y/t \in \mathfrak{p}_S$, where $x, y \in \mathfrak{p}$ and $s, t \in S$, and suppose $(x/s)(y/t) \in \mathfrak{p}_S$. Then $xy/st \in \mathfrak{p}_S$, which implies $xy \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we have either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Without loss of generality, say $x \in \mathfrak{p}$. Then clearly $x/s \in \mathfrak{p}_S$. This implies $\mathfrak{p}_S$ is prime.

We now want to show that these two maps are inverse to each other. First let us show that Ψ is injective. Let $\mathfrak{p}$ and $\mathfrak{p}'$ be two distinct primes in R such that $\mathfrak{p} \cap S = \mathfrak{p}' \cap S = \emptyset$. Without loss of generality, say $\mathfrak{p} \not\subseteq \mathfrak{p}'$. Choose $x \in \mathfrak{p} \backslash \mathfrak{p}'$. Then observe that $x/1 \in \mathfrak{p}_S$. Furthermore, we also have $x/1 \notin \mathfrak{p}'_S$. Indeed, assume for a contradiction $x/1 \in \mathfrak{p}'_S$. Then $x/1 = y/s$ with $y \in \mathfrak{p}'_S$ and $s \in S$. Then there exists $t \in S$ such that $tsx = ty \in \mathfrak{p}'$. As $\mathfrak{p}'$ is prime and $s, t \notin \mathfrak{p}'$, we must have $x \in \mathfrak{p}'$, which is a contradiction. This shows that $\mathfrak{p}_S$ and $\mathfrak{p}'_S$ are distinct, and hence Ψ is injective.

Now we will show Ψ is surjective. Let $\mathfrak{q} \in \operatorname{Spec} R_S$. We claim that $\mathfrak{q} = \rho^{-1}(\mathfrak{q})_S$. Indeed, we have

$$\begin{aligned} \rho^{-1}(\mathfrak{q})_S &= \{x/s \mid x \in \rho^{-1}(\mathfrak{q}) \text{ and } s \in S\} \\ &= \{x/s \mid x/1 \in \mathfrak{q} \text{ and } s \in S\} \\ &= \mathfrak{q}, \end{aligned}$$

where equality in the last line follows from the fact that $\mathfrak{q}$ is prime: if $x/s \in \mathfrak{q}$, then $x/1 \in \mathfrak{q}$ since $1/s \notin \mathfrak{q}$ and $x/s = (x/1)(1/s)$. Thus Ψ is surjective and hence a bijection. In proving that Ψ is surjective, we also see that the inverse of Ψ is Φ. □

86 Homework 3

86.1 Von Neumann Regular Rings

Definition 86.1. Let R be a commutative ring (maybe without identity). We say R is **von Neumann regular** if for every $x \in R$ there exists $y \in R$ such that $x = xyx$.

Exercise 35. Show that any direct product or direct sum of fields is von Neumann regular.

Solution 28. Let $\{K_\lambda\}_{\lambda \in \Lambda}$ be a collection of fields indexed over a set Λ. First let us show that $\prod_\lambda K_\lambda$ is von Neumann regular. Let (x_λ) be an arbitrary element in $\prod K_\lambda$. For each $\lambda \in \Lambda$, note that K_λ is von Neumann regular. Indeed, K_λ is a field, so if $x_\lambda \neq 0$, we can choose $y_\lambda = x_\lambda^{-1}$, and if $x_\lambda = 0$, we can choose $y_\lambda = 0$. In any case, we see that $(y_\lambda) \in \prod K_\lambda$ satisfies

$$\begin{aligned}(x_\lambda)(y_\lambda)(x_\lambda) &= (x_\lambda y_\lambda x_\lambda) \\ &= (x_\lambda).\end{aligned}$$

Thus $\prod_\lambda K_\lambda$ is von Neumann regular.

The same proof also shows $\bigoplus_\lambda K_\lambda$ is von Neumann regular. Indeed, we view $\bigoplus_\lambda K_\lambda$ as a subring of $\prod_\lambda K_\lambda$ given by the set of all sequences $(x_\lambda) \in \prod_\lambda K_\lambda$ such that there exists a finite subset Λ_0 of Λ where $x_\lambda = 0$ for all $\lambda \in \Lambda \backslash \Lambda_0$. In this case, for each $\lambda_0 \in \Lambda_0$, we choose $y_{\lambda_0} \in K_{\lambda_0}$ such that $x_{\lambda_0} y_{\lambda_0} x_{\lambda_0} = x_{\lambda_0}$ as before, and for each $\lambda \in \Lambda \backslash \Lambda_0$, we simply set $y_\lambda = 0$. Then clearly $(y_\lambda) \in \bigoplus_\lambda K_\lambda$ satisfies

$$\begin{aligned}(x_\lambda)(y_\lambda)(x_\lambda) &= (x_\lambda y_\lambda x_\lambda) \\ &= (x_\lambda).\end{aligned}$$

Thus $\bigoplus_\lambda K_\lambda$ is von Neumann regular.

Exercise 36. Let R be a commutative ring with identity. Suppose R is von Neumann regular. Then R is 0-dimensional.

Solution 29. Assume for a contradiction that R is not 0-dimensional. Choose primes $\mathfrak{p}, \mathfrak{q} \in R$ such that $\mathfrak{p} \subset \mathfrak{q}$ where the inclusion is strict. Clearly $R/\mathfrak{p}$ is von Neumann, so by passing the to quotient $R/\mathfrak{p}$ if necessary, we may as well assume that R is an integral domain, that $\mathfrak{p} = 0$, and that $\mathfrak{q}$ is a nonzero ideal in R. Choose a nonzero element $x \in \mathfrak{q}$. Since R is von Neumann, there exists $y \in R$ such that $xyx = x$. This implies

$$x(yx - 1) = 0.$$

Since $x \neq 0$ and R is a domain, we see that $yx = 1$. So x is a unit. This contradicts the fact that $x \in \mathfrak{q}$ (prime ideals do not contain units!). Thus our assumption that R is not 0-dimensional leads to a contradiction, so R must be 0-dimensional.

Exercise 37. Let R be a commutative ring with identity. Suppose R is von Neumann regular and let $\mathfrak{p}$ be a prime ideal in R. Then $R_\mathfrak{p} \cong R/\mathfrak{p}$.

Solution 30. Note that since R is 0-dimensional (by problem 2) we see that $\mathfrak{p}$ is a maximal ideal, and thus $R/\mathfrak{p}$ is a field. In particular, it follows that $R/\mathfrak{p} \cong (R/\mathfrak{p})_{\mathfrak{p}/\mathfrak{p}} = (R/\mathfrak{p})_\mathfrak{p}$. We claim that $R_\mathfrak{p}$ is also a field. Indeed, to this, it suffices to show that the maximal ideal $\mathfrak{p}R_\mathfrak{p} = 0$. Let $x/s \in \mathfrak{p}R_\mathfrak{p}$ where $x \in \mathfrak{p}$ and $s \notin \mathfrak{p}$. Choose $y \in R$ such that $xyx = x$. In other words, we have have $(xy - 1)x = 0$. Note that $xy - 1 \notin \mathfrak{p}$ since $xy \in \mathfrak{p}$ and $1 \notin \mathfrak{p}$. It follows that $x/s = 0$ in $R_\mathfrak{p}$. Therefore $\mathfrak{p}R_\mathfrak{p} = 0$. In particular, it follows that $R_\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. Finally, since localization is exact, we already have $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong (R/\mathfrak{p})_\mathfrak{p}$. Thus

$$R_\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong (R/\mathfrak{p})_\mathfrak{p} \cong R/\mathfrak{p}.$$

86.2 R is a UFD if and only if $R[X]$ is a UFD

Exercise 38. Let R be an integral domain. Then R is a unique factorization domain if and only if $R[X]$ is a unique factorization domain.

We give two solutions.

Solution 31. First suppose $R[X]$ is a unique factorization domain. Let a be a nonzero nonunit in R. Then viewing a as a constant polynomial in $R[X]$ we see that a has an irreducible factorization, say

$$a = p_1(X) \cdots p_m(X) \tag{355}$$

where $p_1, \dots, p_m$ are irreducible polynomials in $R[X]$. By taking degrees on both sides of (355), we obtain

$$0 = \deg(p_1 \cdots p_m) = \deg p_1 + \cdots + \deg p_m, \tag{356}$$

where we used the fact that R is a domain to get the equality on the right in (356). In particular, $\deg p_i = 0$ for all $1 \leq i \leq m$. Thus each p_i is a constant polynomial. Irreducible constant polynomials in $R[X]$ are precisely the irreducible elements in R, so (355) is an irreducible factorization in R. Furthermore, the factorization (355) is unique since $R[X]$ is a unique factorization domain.

Now suppose R is a unique factorization domain. Let $f(X)$ be a nonzero nonunit in $R[X]$ and let K be the fraction field of R. First note that $R[X]$ is Noetherian, and thus f has an irreducible factorization (see Appendix for proof of this). Suppose

$$p_1(X) \cdots p_m(X) = f(T) = q_1(X) \cdots q_n(X)$$

are two irreducible factorizations of f in $R[X]$. By Gauss' Lemma, each p_i and q_j is irreducible in $K[X]$. Since $K[X]$ is a unique factorization domain, we see that $m = n$ and (perhaps after relabeling) $p_i \sim q_i$ in $K[X]$. In particular, $p_i = x_i q_i$ for some $x_i \in K[X]^\times = K^\times$. Note that since $p_i, q_i \in R[X]$, we must have $x_i \in R \backslash \{0\}$. Therefore

$$\begin{aligned} 0 &= p_1(X) \cdots p_m(X) - q_1(X) \cdots q_m(X) \\ &= p_1(X) \cdots p_m(X) - x_1 \cdots x_m p_1(X) \cdots p_m(X) \\ &= p_1(X) \cdots p_m(X)(1 - x_1 \cdots x_m) \\ &= f(X)(1 - x_1 \cdots x_m), \end{aligned}$$

and since $f \neq 0$ and $R[X]$ is a domain, this implies $1 = x_1 \cdots x_n$, which implies each x_i is a unit in R. Thus $p_i \sim q_i$ in $R[X]$. It follows that $R[X]$ is a unique factorization domain.

Solution 32. By the same proof as in the solution above, we see that if $R[X]$ is a unique factorization domain, then R is a unique factorization domain. We want to give an alternative proof for the converse direction. Suppose R is a unique factorization domain. Let $\mathfrak{q}$ be a prime ideal in $R[X]$. Then $\mathfrak{q} \cap R$ is a prime ideal in R. Since R is a unique factorization domain, there exists a prime element of R which is contained in $\mathfrak{q} \cap R$, say $a \in \mathfrak{q} \cap R$. Then observe that a is a prime element of $R[X]$ which is contained in $\mathfrak{q}$. Indeed, suppose $a = fg$ where $f, g \in R[X]$. By taking degrees on both sides, we see that $\deg f = 0 = \deg g$. Thus $f, g \in R$, which means either $f \in \langle a \rangle$ or $g \in \langle a \rangle$. Hence a is a prime element of $R[X]$. It follows that every prime ideal in $R[X]$ contains a prime element, thus $R[X]$ is a unique factorization domain.

86.3 Units of $R[X]$

Exercise 39. Let R be a commutative ring with identity. Characterize $(R[X])^\times$.

Solution 33. Let $f(X) \in R[X]$ and it express it as

$$f(X) = a_m X^m + \cdots + a_1 X + a_0$$

where $a_0, a_1, \dots, a_m \in R$. We claim that f is a unit in $R[X]$ if and only if a_0 is a unit in R and a_i is nilpotent for all $1 \leq i \leq m$.

To see this, first suppose a_0 is a unit in R and a_i is nilpotent for all $1 \leq i \leq m$. Then each $a_i X^i$ is also nilpotent, and since the sum of two nilpotent elements is nilpotent, we see that $\sum_{i=1}^m a_i X^i$ is nilpotent. Also since a_0 is a unit in R, it is also a unit in $R[X]$. So f is the sum of a unit plus a nilpotent element. This implies f is a unit since the sum of a unit plus a nilpotent element is always a unit (if u is a unit with $uv = 1$, and ε is a nilpotent element with $\varepsilon^m = 0$, then $(u + \varepsilon) \sum_{i=1}^m v^i \varepsilon^{i-1} = 1$). This establishes one direction.

For the reverse direction, suppose f is a unit in $R[X]$. We consider two steps:

Step 1: Assume that R is a domain. In this case, we want to show that a_0 is a unit in R and $a_i = 0$ for all $1 \leq i \leq m$. To see this, first we assume for a contradiction that $a_i \neq 0$ for some $1 \leq i \leq m$. By relabeling if necessary, we may in fact that assume $a_m \neq 0$ where a_m is the lead coefficient of f. Now let $g(X) \in R[X]$ such that $fg = 1$ and it express it as

$$g(X) = b_n X^n + \cdots + b_1 X + b_0$$

where $b_0, b_1, \dots, b_n \in R$ and $b_n \neq 0$. Then the lead term of fg is just $a_m b_n X^{m+n}$ since $a_m \neq 0$ and $b_n \neq 0$ and R is a domain. This is a contradiction since $fg = 1$ and $m + n \geq 1$. Thus we must have $a_i = 0$ for all $1 \leq i \leq m$. By the same proof, we must also have $b_j = 0$ for all $1 \leq j \leq n$. Thus $f(X) = a_0$ and $g(X) = b_0$, and $fg = 1$ implies $a_0 b_0 = 1$ which implies a_0 is a unit.

Step 2: Now we consider the more general case where R may not be a domain. First, to see why a_0 is a unit, note that a_0 is in the image of the unit f under the evaluation map $\mathrm{ev}_0 \colon R[X] \to R$, where ev_0 is given by $\mathrm{ev}_0(h) = h(0)$ for all $h(X) \in R[X]$. Thus $a_0 = \mathrm{ev}_0(f)$ is a unit since f is a unit and ev_0 is a ring homomorphism (which preserves the identity element). Next, to see why a_i is nilpotent for all $1 \leq i \leq m$, first note that for any prime ideal $\mathfrak{p}$ in R, the quotient $R/\mathfrak{p}$ is a domain. Since f is a unit in $R[X]$, its image $\overline{f}$ is a unit in $(R/\mathfrak{p})[X]$. Since $\overline{f}$ is obtained from f by reducing coefficients modulo $\mathfrak{p}$, we see from step 1 above that $a_i \in \mathfrak{p}$ for all $1 \leq i \leq m$. Since $\mathfrak{p}$ was arbitrary, we see that

$$a_i \in \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p} = \mathrm{N}(R)$$

where $\mathrm{N}(R)$ is the set of all nilpotents in R (see homework 1 for why $\bigcap \mathfrak{p} = \mathrm{N}(R)$).

86.4 Maximal Chains of Ideals

Definition 86.2. Let R be a commutative ring with identity and let $(I_\lambda)_{\lambda \in \Lambda}$ be a chain of ideals between the ideals $I \subseteq J$. We say (I_λ) is **maximal** if any ideal $\mathfrak{a} \subseteq R$ that is comparable to every ideal in (I_λ), must in fact belong to (I_λ).

Exercise 40. Show that for any ideals $I \subseteq J$, there is a maximal chain of ideals between I and J (inclusive of I and J).

Solution 34. If $I = J$, then clearly (I, J) is a maximal chain, so assume $I \subset J$ is a proper inclusion. Let $\mathcal{F}$ be the family of all chains of ideals between I and J which include I and J. Thus $(I_\lambda)_{\lambda \in \Lambda} \in \mathcal{F}$ means the following:

- Λ is a totally ordered set with a minimal and maximal element. To each $\lambda \in \Lambda$ we have an ideal I_λ such that if $\lambda < \mu$[17], then $I_\lambda \subset I_\mu$, where the inclusion is proper. If λ_0 is the minimal element of Λ and λ_1 is the maximal element of Λ, then $I = I_{\lambda_0}$ and $J = I_{\lambda_1}$,

We give $\mathcal{F}$ the structure of a partially ordered set via set inclusion. In particular, if this means that if $(I_\lambda)_{\lambda \in \Lambda}$ and $(I_{\lambda'})_{\lambda' \in \Lambda'}$ are two members of $\mathcal{F}$, then we say $(I_\lambda)_{\lambda \in \Lambda} \subseteq (I_{\lambda'})_{\lambda' \in \Lambda'}$ if $\Gamma \subseteq \Lambda$, or in other words, if every member of $(I_\lambda)_{\lambda \in \Lambda}$ is also a member of $(I_{\lambda'})_{\lambda' \in \Lambda'}$. We say the chain $(I_{\lambda'})_{\lambda' \in \Lambda'}$ is **larger** than the chain $(I_\lambda)_{\lambda \in \Lambda}$ if $(I_\lambda)_{\lambda \in \Lambda} \subseteq (I_{\lambda'})_{\lambda' \in \Lambda'}$ and $(I_{\lambda'})_{\lambda' \in \Lambda'} \not\subseteq (I_\lambda)_{\lambda \in \Lambda}$.

Note that $\mathcal{F}$ is nonempty since $(I, J) \in \mathcal{F}$. We claim that every totally ordered subset of $\mathcal{F}$ has an upper bound. Indeed, let

$$((I_\lambda)_{\lambda \in \Lambda(\alpha)})_{\alpha \in A} \tag{357}$$

be a totally ordered subset of $\mathcal{F}$. In detail, this means:

- A is a totally ordered set. To each $\alpha \in A$, we have a chain of ideals $(I_\lambda)_{\lambda \in \Lambda(\alpha)}$ such that if $\alpha < \beta$, then $\Lambda(\alpha) \subset \Lambda(\beta)$ where this inclusion is strict.

Clearly an upper bound of (357) is given by

$$(I_\lambda)_{\lambda \in \bigcup_{\alpha \in A} \Lambda(\alpha)}.$$

Thus $\mathcal{F}$ is nonempty and every totally ordered subset of $\mathcal{F}$ has an upper bound. It follows from Zorn's Lemma that $\mathcal{F}$ has a maximal element, say $(I_\lambda)_{\lambda \in \Lambda}$. In fact, $(I_\lambda)_{\lambda \in \Lambda}$ is maximal in the sense of Definition (86.2). To see this, assume for a contradiction that $(I_\lambda)_{\lambda \in \Lambda}$ is note maximal in the sense of Definition (86.2). Then there exists an ideal $\mathfrak{a}$ in R such that $\mathfrak{a}$ is suppose $\mathfrak{a}$ is comparable to every ideal in $(I_\lambda)_{\lambda \in \Lambda}$ and $\mathfrak{a} \neq I_\lambda$ for any $\lambda \in \Lambda$. Define $\widetilde{\Lambda} = \Lambda \cup \{\widetilde{\lambda}\}$ and set $I_{\widetilde{\lambda}} = \mathfrak{a}$. Then observe that chain $(I_\lambda)_{\lambda \in \widetilde{\Lambda}}$ is larger than $(I_\lambda)_{\lambda \in \Lambda}$, contradicting maximality of $(I_\lambda)_{\lambda \in \Lambda}$. Thus $(I_\lambda)_{\lambda \in \Lambda}$ is maximal in the sense of Definition (86.2). Furthermore, the chain $(I_\lambda)_{\lambda \in \Lambda}$ contains I and J by definition of $\mathcal{F}$, so we are done.

86.5 Appendix

86.5.1 Nonzero Nonunits in Noetherian Domains have Irreducible Factorizations

Proposition 86.1. *Let R be a Noetherian domain and let a be a nonzero nonunit in R. Then a has an irreducible factorization.*

Proof. If a is irreducible, then we are done, so assume that a is reducible. We assume for a contradiction that a cannot be factored into irreducible. Since a is reducible, there is a factorization of a into nonzero nonunits, say

$$a = a_1 b_1.$$

[17]Note by $\lambda < \mu$ we mean $\lambda \leq \mu$ and $\lambda \neq \mu$

If both a_1 and b_1 can be factored into irreducibles, then so can a, so at least one of them cannot be factored into irreducible elements, say a_1. In particular, a_1 is reducible, and thus there is factorization of a_1 into nonzero nonunits, say

$$a_1 = a_2 b_2.$$

By the same reasoning above, we may assume that a_2 cannot be factored into irreducibles. Proceeding inductively, we construct sequences (a_n) and (b_n) in R where each a_n is reducible and each b_n is a nonzero nonunit, furthermore we have the factorization

$$a_n = a_{n+1} b_{n+1}$$

for all $n \in \mathbb{N}$. In particular, we have an ascending chain of ideals $(\langle a_n \rangle)$. Indeed, $\langle a_n \rangle \subseteq \langle a_{n+1} \rangle$ because $a_n = a_{n+1} b_{n+1}$. Since R is Noetherian, this ascending chain must terminate, say at $N \in \mathbb{N}$. In particular, we have $\langle a_N \rangle = \langle a_{N+1} \rangle$. This implies there exists $c_N \in R$ such that

$$a_N c_N = a_{N+1}.$$

Thus we have

$$\begin{aligned} 0 &= a_N - a_{N+1} b_{N+1} \\ &= a_N - a_N c_N b_{N+1} \\ &= a_N (1 - c_N b_{N+1}). \end{aligned}$$

Since R is an integral domain, this implies $b_{N+1} c_N = 1$ (as $a_N \neq 0$), which implies b_{N+1} is a unit. This is a contradiction. □

87 Homework 4

87.1 Characterization of Projective Modules over a Field

Exercise 41. Let R be an integral domain. Show that the following conditions are equivalent.

1. Every R-module is free.
2. Every R-module is projective.
3. Every R-module is injective.
4. R is a field.

Solution 35. (1 implies 2) Suppose every R-module is free and let P be any R-module. We want to show that P is projective. Let $\varphi \colon M \to N$ be a surjective R-module homomorphism and let $\psi \colon P \to N$ be any R-module homomorphism. Let $\{e_\lambda\}_{\lambda \in \Lambda}$ be a basis for P as a free R-module. For each $\lambda \in \Lambda$, choose $u_\lambda \in M$ such that $\varphi(u_\lambda) = \psi(e_\lambda)$ (such a choice is possible as φ is surjective). Define $\widetilde{\psi} \colon P \to M$ to be the unique R-module homomorphism such that $\widetilde{\psi}(e_\lambda) = u_\lambda$ for all $\lambda \in \Lambda$. Then for all $\lambda \in \Lambda$ we have

$$\begin{aligned} (\varphi \circ \widetilde{\psi})(e_\lambda) &= \varphi(\widetilde{\psi}(e_\lambda)) \\ &= \varphi(u_\lambda) \\ &= \psi(e_\lambda). \end{aligned}$$

It follows that $\varphi \circ \widetilde{\psi} = \psi$. Therefore P is projective. Since P was arbitrary, it follows that every R-module is projective.

(2 implies 3) Suppose every R-module is projective. Let E be an R-module and let

$$0 \longrightarrow E \longrightarrow M \longrightarrow N \longrightarrow 0 \tag{358}$$

be a short exact sequence of R-modules. Then since N is a projective R-module, the short exact sequence (363) splits. It follows that E is an injective R-module (see Appendix for equivalent criteria for an R-module to be injective). Since E was arbitrary, it follows that every R-module is injective.

(3 implies 4) Suppose every R-module is injective. We want to show R is a field. Assume for a contradiction that R is not a field. Choose a nonzero nonunit element in R, say $x \in R$. Then the multiplication map $\mathrm{m}_x \colon R \to R$, given by

$$\mathrm{m}_x(a) = ax$$

for all $a \in R$, splits since it is an injective map (as R is a domain) and since R is injective as an R-module over itself. Thus there exists an R-linear map $\varphi \colon R \to R$ such that $\varphi \mathrm{m}_x = 1_R$. Note that φ is completely determined by where it maps 1. Indeed, if $\varphi(1) = y$, then R-linearity of φ implies $\varphi = \mathrm{m}_y$. Thus we have $\mathrm{m}_y \mathrm{m}_x = 1_R$. In particular, $yx = 1$, which implies x is a unit. This is a contradiction. Thus R must be a field.

(4 implies 1) Suppose R is a field. Then an R-module is just an R-vector space. A standard argument using Zorn's Lemma tells us that every vector space has a basis (see Appendix for proof), and hence every vector space is free.

87.2 Tensor Product of Projective is Projective

Exercise 42. Let P and Q be projective R-modules. Show that $P \otimes_R Q$ is projective also.

Solution 36. It suffices to show that $\mathrm{Hom}_R(P \otimes_R Q, -)$ is exact. Let

$$M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be a short exact sequence of R-modules. Then since Q is projective, the induced sequence

$$0 \longrightarrow \mathrm{Hom}_R(Q, M_1) \longrightarrow \mathrm{Hom}_R(Q, M_2) \longrightarrow \mathrm{Hom}_R(Q, M_3) \longrightarrow 0$$

is exact. Then since P is projective, the induced sequence

$$0 \longrightarrow \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_1)) \longrightarrow \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_2)) \longrightarrow \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_3)) \longrightarrow 0$$

is exact. By tensor-hom adjointness, we have a commutative diagram[18]

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_1)) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_2)) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_3)) \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & \mathrm{Hom}_R(P \otimes_R Q, M_1) \arrow[r] & \mathrm{Hom}_R(P \otimes_R Q, M_2) \arrow[r] & \mathrm{Hom}_R(P \otimes_R Q, M_3) \arrow[r] & 0
\end{tikzcd}$$

where the columns are isomorphisms and where the top row is exact. It follows from the 3×3 lemma that the bottom row is exact too.

87.3 Overring of Valuation Domain is a Localization

Exercise 43. Prove that every overring of a valuation domain is a localization.

Solution 37. Let R be a valuation domain and let A be an overring of R. We will show A is a localization of R. Let $S = \{y \in R \mid 1/y \in A\}$. Observe that S is a multiplicatively closed subset of R since $1 \in S$ and if $y_1, y_2 \in S$, then $y_1 y_2 \in S$ since

$$1/(y_1 y_2) = (1/y_1)(1/y_2) \in A.$$

Since $R \subseteq A$, we see that any $x/y \in R_S$ is an element of A, thus $R_S \subseteq A$. To show the reverse inclusion, let $x/y \in A$ where $x, y \in R \backslash \{0\}$. Since R is a valuation domain, we have either $x \mid y$ or $y \mid x$. If $x \mid y$, then $ax = y$ for some $a \in R$. In this case,

$$\frac{x}{y} = \frac{x}{ax} = \frac{1}{a}.$$

In particular, we see that $a \in S$. Thus $x/y = 1/a \in R_S$. On the other hand, if $y \mid x$, then $x = by$ for some $b \in R$. In this case,

$$\frac{x}{y} = \frac{by}{y} = \frac{b}{1}.$$

Clearly $b/1 \in R_S$, thus $x/y = b/1 \in R_S$. In either case, we see that $x/y \in R_S$. It follows that $A \subseteq R_S$.

[18] Note how we need naturality in the third argument to get a commutative diagram.

87.4 Prufer Domain

Definition 87.1. We say that the integral domain R is a **Prüfer** domain if $R_\mathfrak{p}$ is a valuation domain for all prime ideals $\mathfrak{p}$ in R. They are the "global" analog of valuation domains.

Exercise 44. Show that any overring of a Prüfer domain is a Prüfer domain.

Solution 38. Let R be a Prüfer domain and let A be an overring of R. We will show A is a Prüfer domain. Let $\mathfrak{q}$ be any prime ideal in A. Then $\mathfrak{p} = R \cap \mathfrak{q}$ is a prime ideal in R. Since R is a Prüfer domain, we see that $R_\mathfrak{p}$ is a valuation domain. Furthermore, note that $A_\mathfrak{q}$ is an overring of $R_\mathfrak{p}$. Indeed, if $x/y \in R_\mathfrak{p}$, then $x \in R$ implies $x \in A$, and $y \notin \mathfrak{p}$ implies $y \notin \mathfrak{q}$, thus $x/y \in A_\mathfrak{q}$. Thus by problem 3, we see that $A_\mathfrak{q}$ is a localization of $R_\mathfrak{p}$. A localization of a valuation domain is a valuation domain (see Appendix for proof of this), thus $A_\mathfrak{q}$ is a valuation domain. Since $\mathfrak{q}$ was arbitrary, it follows that A is a Prüfer domain.

87.5 Valuation Domains

Exercise 45. Show that if v is a valuation on K then the set of elements with nonnegative value (and 0) form a valuation domain.

Solution 39. Let $(\Gamma, \geq)$ be a totally ordered abelian group and let $v \colon K^\times \to \Gamma$ be a valuation on K. Set $A = \{x \in K \mid v(x) \geq 0\} \cup \{0\}$. We will show A is a valuation domain. Suppose $a, b \in A \backslash \{0\}$, and without loss of generality, assume that $v(b) \geq v(a)$. Then

$$\begin{aligned} v(ba^{-1}) &= v(b) - v(a) \\ &\geq 0 \end{aligned}$$

implies $ba^{-1} \in A$. In particular, this implies $a \mid b$. It follows that A is a valuation domain.

Definition 87.2. Let $(A_1, \leq_1)$ and $(A_2, \leq_2)$ be totally ordered abelian groups. We order the group $A_1 \oplus A_2$ by declaring $(a_1, a_2) \leq (a_1', a_2')$ if $a_1 \leq_1 a_1'$ or $a_1 = a_1'$ and $a_2 \leq_2 a_2'$. This ordering is called the **lexicographical ordering**.

Remark 135. Note that lexicographical ordering is translate invariant in the sense that if $(a_1, a_2) \leq (a_1', a_2')$ implies $(a_1 + a_1'', a_2 + a_2'') \leq (a_1' + a_1'', a_2' + a_2'')$.

Exercise 46. Construct valuation domains with value groups $\mathbb{Z} \oplus \mathbb{R}$ and $\mathbb{R} \oplus \mathbb{Z}$ ordered lexicographically.

Solution 40. We first construct a valuation domain with value group $\mathbb{R} \oplus \mathbb{Z}$. Let K be any field and define $K[\mathbb{R} \oplus \mathbb{Z}]$ to be the set of elements of the form

$$\sum_{i=0}^{\infty} a_{\beta_i, n_i} X^{\beta_i} Y^{n_i} \tag{359}$$

where $a_{\beta_i, n_i} \in K$ and where $\{(\beta_i, n_i)\}_{i=0}^{\infty}$ is a linearly ordered subset of $\mathbb{R} \oplus \mathbb{Z}$ where we are viewing $\mathbb{R} \oplus \mathbb{Z}$ as a totally ordered abelian group with respect to the lexicographical ordering. To simplify our notation, we sometimes omit the subscripts in the sum (359) and simply write $\sum a_{\beta,n} X^\beta Y^n$ with the understanding that the sum is over a linearly ordered subset of $\mathbb{R} \oplus \mathbb{Z}$ with a least element. Addition in $K[\mathbb{R} \oplus \mathbb{Z}]$ is defined pointwise

$$\sum a_{\beta,n} X^\beta Y^n + \sum b_{\beta,n} X^\beta Y^n = \sum (a_{\beta,n} + b_{\beta,n}) X^\beta Y^n,$$

and multiplication in $K[\mathbb{R} \oplus \mathbb{Z}]$ is defined by

$$\left(\sum a_{\beta,n} X^\beta Y^n\right) \left(\sum b_{\beta,n} X^\beta Y^n\right) = \sum_{\beta,n} \left(\sum_{\substack{\beta' + \beta'' = \beta \\ n' + n'' = n}} a_{\beta',n'} b_{\beta'',n''} \right) X^\beta Y^n. \tag{360}$$

We simplify our notation again by omitting the subscpricts in the coefficient on the right hand side of (360) and simply write $\sum a_{\beta',n'} b_{\beta'',n''}$ with the understanding that the sum is over all $\beta' + \beta'' = \beta$ and $n' + n'' = n$. Alternatively, we can express multiplication in $K[\mathbb{R} \oplus \mathbb{Z}]$ as

$$\left(\sum_{i=0}^{\infty} a_{\alpha_i, m_i} X^{\alpha_i} Y^{m_i} \right) \left(\sum_{j=0}^{\infty} b_{\beta_j, n_j} X^{\beta_j} Y^{n_j} \right) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_{\alpha_i, m_i} b_{\beta_{k-i}, n_{k-i}} \right) X^{\beta_k} Y^{n_k}.$$

It is straightforward to check that addition and multiplication defined in this way give $K[\mathbb{R}\oplus\mathbb{Z}]$ the structure of a ring. The proof is nearly identical to the power series case. For instance, we have left distributivity of addition with respect to multiplication:

$$\begin{aligned}
\left(\sum a_{\beta,n}X^\beta Y^n\right)\left(\sum b_{\beta,n}X^\beta Y^n+\sum c_{\beta,n}X^\beta Y^n\right) &= \left(\sum a_{\beta,n}X^\beta Y^n\right)\left(\sum (b_{\beta,n}+c_{\beta,n})X^\beta Y^n\right)\\
&= \sum_{\beta,n}\left(\sum a_{\beta',n'}(b_{\beta'',n''}+c_{\beta'',n''})\right)X^\beta Y^n\\
&= \sum_{\beta,n}\left(\sum (a_{\beta',n'}b_{\beta'',n''}+a_{\beta',n'}c_{\beta'',n''})\right)X^\beta Y^n\\
&= \sum_{\beta,n}\left(\sum (a_{\beta',n'}b_{\beta'',n''}+a_{\beta',n'}c_{\beta'',n''})\right)X^\beta Y^n\\
&= \sum_{\beta,n}\left(\sum a_{\beta',n'}b_{\beta'',n''}+\sum a_{\beta',n'}c_{\beta'',n''}\right)X^\beta Y^n\\
&= \sum_{\beta,n}\left(\sum a_{\beta',n'}b_{\beta'',n''}\right)X^\beta Y^n+\sum_{\beta,n}\left(\sum a_{\beta',n'}c_{\beta'',n''}\right)X^\beta Y^n\\
&= \left(\sum a_{\beta,n}X^\beta Y^n\right)\left(\sum b_{\beta,n}X^\beta Y^n\right)+\left(\sum a_{\beta,n}X^\beta Y^n\right)\left(\sum c_{\beta,n}X^\beta Y^n\right).
\end{aligned}$$

We can even show $K[\mathbb{R}\oplus\mathbb{Z}]$ is a field with the proof being similar to the power series case. Indeed, let $f=\sum_{i=0}^\infty a_{\alpha_i,m_i}X^{\alpha_i}Y^{m_i}$ be a nonzero element in $K[\mathbb{R}\oplus\mathbb{Z}]$ with $a_{\alpha_0,m_0}\neq 0$. To construct an inverse of f, let us first assume that an inverse exists and see what conditions it needs to satisfy. Let $g=\sum_{j=0}^\infty a_{\beta_j,n_j}X^{\beta_j}Y^{n_j}$ and suppose $fg=0$. Then we obtain a sequence of equations

$$\begin{aligned}
1 &= a_{\alpha_0,m_0}b_{\beta_0,n_0}\\
0 &= a_{\alpha_0,m_0}b_{\beta_1,n_1}+a_{\alpha_1,m_1}b_{\beta_0,n_0}\\
&\vdots\\
0 &= \sum_{i=0}^k a_{\alpha_i,m_i}b_{\beta_{k-i},n_{k-i}}\\
&\vdots
\end{aligned}$$

Then $a_{\alpha_0,m_0}\neq 0$ forces $b_{\beta_0,n_0}=1/a_{\alpha_0,m_0}$. Similarly, $a_{\alpha_0,m_0}\neq 0$ forces $b_{\beta_1,n_1}=-a_{\alpha_1,m_1}b_{\beta_0,n_0}/a_{\alpha_0,m_0}$. More generally, in the kth step, we obtain

$$b_{\beta_k,n_k}=-\frac{1}{a_{\alpha_0,m_0}}\sum_{i=1}^k a_{\alpha_i,m_i}b_{\beta_{k-i},n_{k-i}}. \tag{361}$$

Conversely, any such g whose coefficients are defined inductively by (**??**) is easily seen to be an element of $K[\mathbb{R}\oplus\mathbb{Z}]$ which is an inverse to f.

Finally, we can define a valuation on $K[\mathbb{R}\oplus\mathbb{Z}]^\times$ with value group $\mathbb{R}\oplus\mathbb{Z}$ as follows: suppose $f\in K[\mathbb{R}\oplus\mathbb{Z}]^\times$. Express it as $f=\sum_{i=0}^\infty a_{\alpha_i,m_i}X^{\alpha_i}Y^{m_i}$ where $a_{\alpha_0,m_0}\neq 0$. Then we set $v(f)=(\alpha_0,m_0)$. We claim that v is a valuation on $K[\mathbb{R}\oplus\mathbb{Z}]^\times$. It clearly lands surjectively onto $\mathbb{R}\oplus\mathbb{Z}$. The fact that it is a group homomorphism follows from translation invariance of the lexicographical ordering. Finally, suppose $f=\sum_{i=0}^\infty a_{\alpha_i,m_i}X^{\alpha_i}Y^{m_i}$ and $g=\sum_{j=0}^\infty b_{\beta_j,n_j}X^{\beta_j}Y^{n_j}$ are two elements in $K[\mathbb{R}\oplus\mathbb{Z}]^\times$ with $a_{\alpha_0,m_0}\neq 0\neq b_{\beta_0,n_0}$. Assume without loss of generality that $v(f)\leq v(g)$. Thus $(\beta_0,n_0)\geq(\alpha_0,m_0)$. In this case, we clearly have $v(f+g)\geq v(f)=\min\{v(f),f(g)\}$. If $v(f)\neq v(g)$, then $(\beta_0,n_0)>(\alpha_0,m_0)$, which implies $v(f+g)=v(f)$. Thus v is a valuation on $K[\mathbb{R}\oplus\mathbb{Z}]^\times$ with value group $\mathbb{R}\oplus\mathbb{Z}$. An analagous construction shows that $\mathbb{Z}\oplus\mathbb{R}$ is a value group as well. Namely, we define $K[\mathbb{Z}\oplus\mathbb{R}]$ to be the set of elements of the form

$$\sum_{i=0}^\infty a_{n_i,\beta_i}X^{n_i}Y^{\beta_i} \tag{362}$$

where $a_{n_i,\beta_i}\in K$ and where $\{(n_i,\beta_i)\}_{i=0}^\infty$ is a linearly ordered subset of $\mathbb{Z}\oplus\mathbb{R}$ where we are viewing $\mathbb{Z}\oplus\mathbb{R}$ as a totally ordered abelian group with respect to the lexicographical ordering. Then if $f\in K[\mathbb{Z}\oplus\mathbb{R}]^\times$, we express it as $f=\sum_{i=0}^\infty a_{n_i,\beta_i}X^{n_i}Y^{\beta_i}$ with $a_{n_0,\beta_0}\neq 0$ and we set $v(f)=(n_0,\beta_0)$. Then v is a valuation on $K[\mathbb{Z}\oplus\mathbb{R}]^\times$ with value group $\mathbb{Z}\oplus\mathbb{R}$.

87.6 Appendix

87.6.1 Equivalent Criteria for an R-module to be Injective

Proposition 87.1. *Let E an R-module. The following statements are equivalent;*

1. *E is an injective R-module;*
2. *Every short exact sequence of the form*
$$0 \longrightarrow E \longrightarrow M \longrightarrow N \longrightarrow 0 \tag{363}$$
splits.
3. *If E is a submodule of an R-module M, then E is a direct summand of M.*

Proof. ($2 \implies 1$) Assume that any short exact sequence of the form (363) splits. This means, equivalently, that any injective R-linear map out of E splits. Let $\varphi \colon M \to N$ be an injective R-linear map and let $\psi \colon M \to E$ be any R-linear map. We need to construct a map $\widetilde{\psi} \colon N \to E$ such that $\widetilde{\psi}\varphi = \psi$. To do this, consider the pushout module
$$E +_M N = (E \times N)/\{(\psi(u), -\varphi(u)) \mid u \in M\}$$
together its natural maps $\iota_1 \colon E \to E +_M N$ and $\iota_2 \colon N \to E +_M N$, given by
$$\iota_1(v) = [v, 0] \qquad \text{and} \qquad \iota_2(w) = [0, w]$$
for all $v \in E$ and $w \in N$ where $[v, w]$ denotes the equivalence class in $E +_M N$ with (v, w) as one of its representatives. Observe that
$$\begin{aligned} \iota_1(\psi(u)) &= [\psi(u), 0] \\ &= [0, \varphi(u)] \\ &= \iota_2(\varphi(u)) \end{aligned}$$
for all $u \in M$. Therefore, we have a commutative diagram
$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi"'] & N \arrow[d, "\iota_2"] \\ E \arrow[r, "\iota_1"'] & E +_M N \end{tikzcd}$$
We claim that ι_1 is injective. Indeed, suppose $v \in \ker \iota_1$. Then $[v, 0] = [0, 0]$ implies if $(v, 0) = (\psi(u), -\varphi(u))$ for some $u \in M$. Then $\varphi(u) = 0$ implies $u = 0$ since φ is injective, and therefore
$$\begin{aligned} v &= \psi(u) \\ &= \psi(0) \\ &= 0. \end{aligned}$$
Thus ι_1 is injective. Therefore by hypothesis the map $\iota_1 \colon E \to E +_M N$ splits, say by $\lambda \colon E +_M N \to E$, where $\lambda\iota_1 = 1_E$. Finally, we obtain a map $\widetilde{\psi} \colon N \to E$ by setting $\widetilde{\psi} := \lambda\iota_2$. Then
$$\begin{aligned} \widetilde{\psi}\varphi &= \lambda\iota_2\varphi \\ &= \lambda\iota_1\psi \\ &= \psi, \end{aligned}$$
shows that $\widetilde{\psi}$ has the desired property.

($1 \implies 2$) Assume that E is an injective R-module. Let $\varphi \colon E \to M$ be an injective homomorphism. Since E is an injective R-module and since $1_E \colon E \to E$ is an injective R-module homomorphism, there exists an R-linear map $\widetilde{\varphi} \colon M \to E$ such that $\widetilde{\varphi} \circ \varphi = 1_E$. That is, $\widetilde{\varphi}$ splits $\varphi \colon E \to M$.

($2 \implies 3$) Assume that any short exact sequence of the form (363) splits. Let M be an R-module such that $E \subseteq M$. Then the short exact sequence
$$0 \longrightarrow E \xrightarrow{\iota} M \xrightarrow{\pi} M/E \longrightarrow 0$$

splits, where $\iota\colon E \to M$ denotes the inclusion map and $\pi\colon M \to M/E$ denotes the quotient map. Therefore we may choose a $\widetilde{\pi}\colon M/E \to M$ such that $\pi\widetilde{\pi} = 1_{M/E}$. We claim that

$$M = E \oplus \widetilde{\pi}(M/E).$$

Indeed, they are both submodules of M. Furthermore, observe that we have $E \cap \widetilde{\pi}(M/E) = \{0\}$. Indeed, suppose $u \in E \cap \widetilde{\pi}(M/E)$. Then $u \in E$ implies $\pi(u) = 0$. Also $u \in \widetilde{\pi}(M/E)$ implies $u = \widetilde{\pi}(\overline{v})$ for some $\overline{v} \in M/E$. Therefore

$$\begin{aligned} 0 &= \widetilde{\pi}(0) \\ &= \widetilde{\pi}\pi(u) \\ &= \widetilde{\pi}\pi\widetilde{\pi}(\overline{v}) \\ &= \widetilde{\pi}(\overline{v}) \\ &= u. \end{aligned}$$

Finally, note that if $u \in M$, then we can write

$$u = u - \widetilde{\pi}\pi(u) + \widetilde{\pi}\pi(u),$$

where $\widetilde{\pi}\pi(u) \in \widetilde{\pi}(M/E)$ and where $u - \widetilde{\pi}\pi(u) \in E$ since

$$\begin{aligned} \pi(u - \widetilde{\pi}\pi(u)) &= \pi(u) - \pi\widetilde{\pi}\pi(u) \\ &= \pi(u) - \pi(u) \\ &= 0 \end{aligned}$$

implies $u - \widetilde{\pi}\pi(u) \in \ker \pi = E$. This implies $M = E + \widetilde{\pi}(M/E)$.

($3 \implies 2$) Assume that E satisfies the property that if E is a submodule of an R-module M, then it must be a direct summand of M. We show that any short exact sequence of the form (363) splits by showing that any injective R-linear map out of E splits.

Step 1: Before we show that any injective R-linear map out of E splits, we need to show that if $\varphi\colon E \to F$ is an isomorphism of R-modules, then F satisfies the same property as E; namely if N is an R-module such that $F \subseteq N$, then F is a direct summand of N. Let $\varphi\colon E \to F$ be an isomorphism, let $\psi\colon F \to E$ denote its inverse, and let N be an R-module such that $F \subseteq N$. We define an R-module $\psi(N)$, where as a set we have

$$\psi(N) = E \cup \{\psi(v) \mid v \in N \backslash F\},$$

where $\psi(v)$ is understood to be a formal symbol if $v \in N\backslash F$ and is understood to be an element in E if $v \in F$. Here, E is *literally* a subset of $\psi(N)$. We extend the R-linear structure on E to an R-linear structure on $\psi(N)$ by defining addition and scalar multiplication by

$$\psi(v_1) + \psi(v_2) = \psi(v_1 + v_2) \quad \text{and} \quad a\psi(v) = \psi(av).$$

for all $v, v_1, v_2 \in N\backslash F$ and $a \in R$. Defining the R-linear structure on $\psi(N)$ in this way makes it so that $\psi\colon F \to E$ and $\varphi\colon E \to F$ extends to an isomorphism $\psi\colon N \to \psi(N)$ with corresponding inverse $\varphi\colon \psi(N) \to N$.

With this construction in place, we see that E is *literally* a submodule of $\psi(N)$. Therefore $\psi(N)$ is an internal direct sum, say

$$\psi(N) = E \oplus K,$$

where K is another submodule of $\psi(N)$ such that $E \cap K = \{0\}$ and $E + K = \psi(N)$. Then since $\varphi\colon \psi(N) \to N$ is an isomorphism, we see that

$$\begin{aligned} N &= \varphi(E) \oplus \varphi(K) \\ &= F \oplus \varphi(K). \end{aligned}$$

Step 2: Now we will show that any injective R-linear map out of E splits. Let $\varphi\colon E \to M$ be any injective R-linear map. We claim that $\varphi\colon E \to M$ splits if and only if $\iota\colon \varphi(E) \to M$ splits, where ι denotes the inclusion map. Indeed, denote $\varphi^{-1}\colon E \to \varphi(E)$ to be the inverse of $\varphi\colon E \to \varphi(E)$. If $\varphi\colon E \to M$ splits, then there exists an R-linear map $\widetilde{\varphi}\colon M \to E$ such that $\widetilde{\varphi}\varphi = 1_E$. Then $\varphi\widetilde{\varphi}\colon M \to \varphi(E)$ splits $\iota\colon \varphi(E) \to M$ since

$$\begin{aligned} (\varphi\widetilde{\varphi}\iota)(\varphi(u)) &= \varphi\widetilde{\varphi}(\varphi(u)) \\ &= \varphi(\widetilde{\varphi}\varphi(u)) \\ &= \varphi(u) \end{aligned}$$

for all $\varphi(u) \in \varphi(E)$. Similarly, if $\iota\colon \varphi(E) \to M$ splits, then there exists an R-linear map $\widetilde{\iota}\colon M \to \varphi(E)$ such that $\widetilde{\iota}\iota = 1_{\varphi(E)}$. Then $\varphi^{-1}\widetilde{\iota}\colon M \to E$ splits $\varphi\colon E \to M$ since

$$\begin{aligned}(\varphi^{-1}\widetilde{\iota}\varphi)(u) &= (\varphi^{-1}\widetilde{\iota})(\varphi(u)) \\ &= (\varphi^{-1}\widetilde{\iota})(\iota\varphi(u)) \\ &= (\varphi^{-1}\widetilde{\iota}\iota)(\varphi(u)) \\ &= (\varphi^{-1})(\varphi(u)) \\ &= u\end{aligned}$$

for all $u \in E$.

Thus, to show that $\varphi\colon E \to M$ splits, it suffices to show that $\iota\colon \varphi(E) \to M$ splits. In this case, $\varphi(E)$ is a submodule of M, and by step 1, we see that M is an internal direct sum, say

$$M = \varphi(E) \oplus K$$

for some R-module $K \subseteq M$. The projection map $\pi_1\colon M \to \varphi(E)$ is easily seen to split the inclusion map $\iota\colon \varphi(E) \to M$. □

87.6.2 Every Vector Space has a Basis

Proposition 87.2. *Every vector space has a basis.*

Proof. Let K be a field and let V be a K-vector space. We will show V has a basis over K. Let S be the set of all linearly independent sets in V. Note that for any nonzero $v \in V$, the singleton $\{v\}$ is a linearly independent set. Thus $S \neq \emptyset$. For two linearly independent sets L and L' in V, we say $L \leq L'$ if $L \subseteq L'$. This is the partial ordering on S by inclusion. Let us show that every totally ordered subset of S is bounded. Let $(L_\alpha)_{\alpha \in A}$ be a totally ordered subset of S. We claim that $L = \bigcup_{\alpha \in A} L_\alpha$ is an upper bound of (L_α). Indeed, clearly we have $L_\alpha \subseteq L$ for all $\alpha \in A$. It remains to check that L is a linearly independent set. Let $v_1, \dots, v_n \in L$. Then for each $1 \leq i \leq n$ there exists $\alpha_i \in A$ such that $v_i \in L_{\alpha_i}$. Since the L_α's are totally ordered, one of the sets $L_{\alpha_1}, \dots, L_{\alpha_n}$ contains the others. Thus $v_1, \dots, v_n$ all belong to a common L_α. In particular, they are linearly independent.

Thus by Zorn's Lemma, S contains a maximal element, say $\mathcal{B} \in S$. We claim that $\mathcal{B}$ is a basis for V. Indeed, since $\mathcal{B} \in S$, we see that $\mathcal{B}$ is linearly independent. Thus it suffices to show that $\operatorname{span}\mathcal{B} = V$. To see this, assume for a contradiction that $\operatorname{span}\mathcal{B} \neq V$. Choose $v \in V \backslash \operatorname{span}\mathcal{B}$. Then $\mathcal{B} \cup \{v\}$ is a linearly independent set. By maximality of $\mathcal{B}$, we must have $\mathcal{B} = \mathcal{B} \cup \{v\}$. Hence $v \in \mathcal{B}$, a contradiction. Thus $\operatorname{span}\mathcal{B} = V$, and hence $\mathcal{B}$ is a basis for V. □

87.6.3 Localization of Valuation Domain is a Valuation Domain

Proposition 87.3. *Let R be a valuation domain and let S be a multiplicatively closed subset of R. Then R_S is a valuation domain.*

Proof. Let a/s and b/t be two nonzero elements in R_S, so $a, b \in R \backslash \{0\}$ and $s, t \in S$. Since R is a valuation domain, either $a \mid b$ or $b \mid a$. Without loss of generality, say $a \mid b$, so $b = ax$ for some $x \in R$. Then observe that

$$\frac{b}{t} = \frac{ax}{t} = \frac{a}{s}\frac{sx}{t}$$

implies $a/s \mid b/t$. It follows that R_S is a valuation domain. □

88 Homework 5

88.1 GCDs

Definition 88.1. Let R be an integral domain with identity and suppose $x, y \in R \backslash \{0\}$. We say x and y have a **greatest common divisor** if there exists a $d \in R$ which satisfies the following two properties:

1. $d \mid x$ and $d \mid y$,
2. if there exists $d' \in R$ such that $d' \mid x$ and $d' \mid y$, then $d' \mid d$.

If such a d exists, then using the fact that R is a domain, it is easy to see that the set of all greatest common divisors of x and y is $\{ud \mid u \in R^\times\}$. Indeed, d and d' are greatest common divisors of x and y if and only if $d \mid d'$ and $d' \mid d$ if and only if $d' = ud$ for some $u \in R^\times$. If a greatest common divisor of x and y exists, then we often choose one of their greatest common divisors and denote it by $\gcd(x, y)$. Thus $\gcd(x, y)$ is well-defined up to a unit. If we write $\gcd(x, y) = \gcd(x', y')$, then it is understood that this means $\gcd(x, y) \mid \gcd(x', y')$ and $\gcd(x', y') \mid \gcd(x, y)$. We say R is a **GCD domain** if every pair of nonzero elements in R has a greatest common divisor.

Exercise 47. Let R be a GCD domain and let $a, b, c, x \in R$ be nonzero. Show the following.

1. $\gcd(ax, bx) = x \gcd(a, b)$
2. if $d = \gcd(a, b)$, then $\gcd(a/d, b/d) = 1$.
3. If $\gcd(x, a) = \gcd(x, b) = 1$, then $\gcd(x, ab) = 1$.
4. If $\gcd(x, a) = 1$ and x divides ab, then x divides b.
5. Show that R is integrally closed.
6. Show that R is Bezout if and only if $\gcd(a, b)$ is a linear combination of a and b.

Solution 41. 1. Let $d = \gcd(a, b)$ and let $e = \gcd(ax, bx)$. Write

$$\begin{aligned} a_1 d &= a \\ b_1 d &= b \\ a_2 e &= ax \\ b_2 e &= bx \end{aligned}$$

where $a_1, a_2, b_1, b_2 \in R$. Then observe that $a_1 x d = ax$ and $b_1 x d = bx$ implies $xd \mid ax$ and $xd \mid bx$. Since e is the greatest common divisor of ax and bx, it follows that $xd \mid e$. Thus we have $yxd = e$ for some $y \in R$. In particular, note that $e/x = dy \in R$. Next observe that $a_2(e/x) = ax/x = a$ and $b_2(e/x) = bx/x = b$ implies $(e/x) \mid a$ and $(e/x) \mid b$. Since d is the greatest common divisor of a and b, it follows that $d \mid (e/x)$, and hence $dx \mid e$. Since both $dx \mid e$ and $e \mid dx$, we see that $e = dx$.

2. Let $e = \gcd(a/d, b/d)$. By 1, we have

$$\begin{aligned} de &= d \gcd(a/d, b/d) \\ &= \gcd(d(a/d), d(b/d)) \\ &= \gcd(a, b) \\ &= d. \end{aligned}$$

Since $d \neq 0$, it follows that $e = 1$ since R is a domain.

3. Let $d = \gcd(x, ab)$. Since $d \mid x$ and $d \mid ab$, we see that in particular, we have $d \mid xb$ and $d \mid ab$. Since

$$\begin{aligned} \gcd(xb, ab) &= b \gcd(x, a) \\ &= b \cdot 1 \\ &= b, \end{aligned}$$

it follows that $d \mid b$. Thus $d \mid x$ and $d \mid b$. Since $\gcd(x, b) = 1$, it follows that $d \mid 1$. Since we already have $1 \mid d$, we see that $\gcd(x, ab) = 1$.

4. We have

$$\begin{aligned}\gcd(xb, ab) &= b\gcd(x, a)\\ &= b \cdot 1\\ &= b,\end{aligned}$$

Thus if $x \mid ab$, then since already $x \mid xb$, we see that $x \mid b$.

5. Let K be the field of fractions of R and let $c/d \in K^\times$ where we may assume that $\gcd(c, d) = 1$. Indeed, if $\gcd(c, d) = e$, then write $c'e = c$ and $d'e = d$ where $c', d' \in R$ and replace c/d with c'/d'. Then we have $c/d = c'e/d'e = c'/d'$ and by part 2 of this problem we have $\gcd(c', d') = 1$). Suppose c/d is integral over R, say

$$\frac{c^n}{d^n} + a_{n-1}\frac{c^{n-1}}{d^{n-1}} + a_{n-1}\frac{c^{n-2}}{d^{n-2}} + \cdots + a_0 = 0$$

for some $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in R$. Clearing denominators and rearranging terms gives us

$$c^n = -d(a_{n-1}c^{n-1} + a_{n-2}dc^{n-2} + \cdots + a_0 d^{n-1})$$

In particular, we see that $d \mid c^n$. On the other hand, note that $\gcd(c, d) = 1$ implies $\gcd(c^2, d) = 1$ by part 3 of this problem. An easy induction argument also shows $\gcd(c^n, d) = 1$ too. Since $d \mid c^n$ and $d \mid d$, it follows that $d \mid 1$. In other words, d must be a unit in R, which implies $c/d \in R$. Thus R is integrally closed.

6. Suppose R is a Bezout domain. Then $\langle a, b\rangle = \langle d\rangle$ for some $d \in R$. We claim that d is a greatest common divisor of a and b. Indeed, we clearly have $a'd = a$ and $b'd = b$ for some $a', b' \in R$ since $\langle a, b\rangle = \langle d\rangle$. Thus $d \mid a$ and $d \mid b$, which means d is a divisor of a and b. Moreover, suppose there exists $d' \in R$ such that $d' \mid a$ and $d' \mid b$, say $a''d' = a$ and $b''d' = b$ for some $a'', b'' \in R$. Since $\langle a, b\rangle = \langle d\rangle$ there exists $x, y \in R$ such that $ax + by = d$. Then observe that

$$\begin{aligned}d &= ax + by\\ &= a''d'x + b''d'y\\ &= (a''x + b''y)d'\end{aligned}$$

implies $d' \mid d$ since R is a domain. It follows that $d = \gcd(a, b)$. Then $d = ax + by$ shows us that $\gcd(a, b)$ is a linear combination of a and b.

Conversely, let $d = \gcd(a, b)$ and suppose d is a linear combination of a and b, say $ax + by = d$ for some $x, y \in R$. Then this implies $\langle a, b\rangle \subseteq \langle d\rangle$. Furthermore, since d is a divisor of a and b, we have $a = a'd$ and $b = b'd$ for some $a', b' \in R$. This implies $\langle a, b\rangle \supseteq \langle d\rangle$. Thus we have $\langle a, b\rangle = \langle d\rangle$. It follows that R is a Bezout domain.

88.2 Invertible Ideal in Semiquasilocal Domain is Principal

Exercise 48. Let R be a semiquasilocal domain and let I be an invertible ideal. Then I is principal.

Solution 42. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the maximal ideals of R. Since I is invertible, we have $II^{-1} = R$. In particular, for each $1 \leq i \leq n$ there exists $x_i \in I$ and $y_i \in I^{-1}$ such that $x_i y_i \notin \mathfrak{m}_i$. For each $i \neq j$, choose $z_{ji} \in \mathfrak{m}_j \backslash \mathfrak{m}_i$. Setting $z_i = \prod_{i \neq j} z_{ji}$, we see that $z_i \in \mathfrak{m}_j$ for all $i \neq j$ and $z_i \notin \mathfrak{m}_i$. Finally set

$$z = \sum_{i=1}^{n} z_i y_i.$$

Clearly $z \in I^{-1}$, and thus zI is an ideal in R. We claim that $zI = R$. To see this, assume for a contradiction that zI is contained in a maximal ideal. By relabeling indices if necessary, we may assume that $zI \subseteq \mathfrak{m}_1$. First note that

$$zx_1 = z_1 y_1 x_1 + \sum_{i=2}^{n} z_i y_i x_1.$$

By construction, we have $z_1 y_1 x_1 \notin \mathfrak{m}_1$ and $z_i y_i x_i \in \mathfrak{m}_1$ for all $i \neq 1$. Thus zx_1 is the sum of an element in $\mathfrak{m}_1$ with an element not in $\mathfrak{m}_1$. This is a contradiction since $zx_1 \in \mathfrak{m}_1$. It follows that $zI = R$, and hence $I = \langle z^{-1}\rangle$ is principal.

88.3 Noetherian Domain of Infinite Krull Dimension

Notation: We write $\mathbb{N} = \{1, 2, \dots\}$, so $0 \notin \mathbb{N}$.

Exercise 49. Build a Noetherian domain of infinite Krull dimension.

Solution 43. Let K be a field and let $R = K[\{x_n \mid n \in \mathbb{N}\}]$. For each $k \in \mathbb{N}$, let $\mathfrak{p}_k = \langle x_{2^{k-1}}, x_{2^{k-1}+1}, \dots, x_{2^k-1} \rangle$. The sequence of ideals $(\mathfrak{p}_k)$ starts out as

$$\begin{aligned}
\mathfrak{p}_1 &= \langle x_1 \rangle \\
\mathfrak{p}_2 &= \langle x_2, x_3 \rangle \\
\mathfrak{p}_3 &= \langle x_4, x_5, x_6, x_7 \rangle \\
&\vdots
\end{aligned}$$

Note that each $\mathfrak{p}_k$ is a prime ideal. Indeed, suppose $f, g \in R$ such that $fg \in \mathfrak{p}_k$. Since f and g are polynomials, we must have $f, g \in R_N$ where $R_N = K[x_1, x_2, \dots, x_N]$ for some $N \in \mathbb{N}$. By choosing N large enough, we may assume that $2^k - 1 \leq N$ (in fact we already have this since $fg \in \mathfrak{p}_k$). Then $\mathfrak{p}_k \cap R_N$ is a prime ideal, so either $f \in \mathfrak{p}_k \cap R_N$ or $g \in \mathfrak{p}_k \cap R_N$. We already have $f, g \in R_N$, so either $f \in \mathfrak{p}_k$ or $g \in \mathfrak{p}_k$. It follows that each $\mathfrak{p}_k$ is prime.

Now let S be the multiplicative set

$$S = R \backslash \left(\bigcup_{k \in \mathbb{N}} \mathfrak{p}_k \right).$$

This set is multiplicatively closed since each $\mathfrak{p}_k$ is a prime ideal. We claim that R_S is a Noetherian ring of infinite dimension. We will show this in two steps.

Step 1: We prove a generalized prime avoidance for R. In particular, suppose I is an ideal of R such that $I \subseteq \bigcup_{k \in \mathbb{N}} \mathfrak{p}_k$. We claim that $I \subseteq \mathfrak{p}_k$ for some $k \in \mathbb{N}$. Indeed, assume for a contradiction that $I \not\subseteq \mathfrak{p}_k$ for any $k \in \mathbb{N}$. Clearly then $I \neq 0$. Choose a nonzero polynomial $f \in I$ and express it in terms of its monomials as

$$f = a_1 x^{\alpha_1} + \cdots + a_m x^{\alpha_m} \tag{364}$$

where $a_1, \dots, a_m \in K \backslash \{0\}$ and $\alpha_1, \dots, \alpha_m \in \mathcal{F}$ where $\alpha_i \neq \alpha_{i'}$ for all $1 \leq i < i' \leq m$.

Before proceeding with the proof, let us explain our notation in (364). Given a function $\alpha \colon \mathbb{N} \to \mathbb{Z}_{\geq 0}$, we define its **support**, denoted $\operatorname{supp} \alpha$, to be the set

$$\operatorname{supp} \alpha = \{m \in \mathbb{N} \mid \alpha(m) \neq 0\}.$$

We denote by $\mathcal{F}$ to be the set

$$\mathcal{F} = \{\alpha \colon \mathbb{N} \to \mathbb{Z}_{\geq 0} \mid \operatorname{supp} \alpha \text{ is finite}\}.$$

We also denote by $\mathcal{M}$ to be the set of all monomials in R. There is a bijection from $\mathcal{F}$ to $\mathcal{M}$ given by assigning $\alpha \in \mathcal{F}$ to the monomial

$$x^\alpha := \prod_{m \in \mathbb{N}} x_m^{\alpha(m)} = \prod_{m \in \operatorname{supp} \alpha} x_m^{\alpha(m)}.$$

For instance, suppose $\alpha \colon \mathbb{N} \to \mathbb{N}$ is defined by

$$\alpha(m) = \begin{cases} 3 & \text{if } m = 2 \\ 2 & \text{if } m = 6 \\ 4 & \text{if } m = 11 \\ 0 & \text{if } m \in \mathbb{N} \backslash \{2, 6, 11\} \end{cases}$$

Then $x^\alpha = x_3^3 x_6^2 x_{11}^4$ and $\operatorname{supp} \alpha = \{2, 6, 11\}$. We often pass back and forth between functions $\alpha \in \mathcal{F}$ and monimals $x^\alpha \in \mathcal{M}$. For example, given a monimal $x^\alpha \in \mathcal{M}$, we define its **support**, denoted $\operatorname{supp} x^\alpha$, to be $\operatorname{supp} x^\alpha = \operatorname{supp} \alpha$. Finally, in the monomial expansion of f given in (364), we refer to the $a_i x^{\alpha_i}$ as the **terms** of f, and we refer to the x^{α_i} as the **monomials** of f.

With our notation explained, we now proceed with the proof. For each $k \in \mathbb{N}$, we denote by C_k to be the set

$$C_k = \{2^{k-1}, 2^{k-1} + 1, \dots, 2^k - 1\}.$$

Observe that $f \in \mathfrak{p}_k$ if and only if $\operatorname{supp} x^{\alpha_i} \cap C_k \neq \emptyset$ for all monomials x^{α_i} of f. Or from the contrapositive point of view, we have $f \notin \mathfrak{p}_k$ if and only if $\operatorname{supp} x^{\alpha_i} \cap C_k = \emptyset$ for some monomial x^{α_i} of f. Since $\operatorname{supp} x^{\alpha_i}$ is finite for all monomials x^{α_i} of f, it follows that $\operatorname{supp} x^{\alpha_i} \cap C_k \neq \emptyset$ for only finitely many $k \in \mathbb{N}$. Since f has only finitely many monomials, it follows that there exists finitely many C_k's such that $\operatorname{supp} x^{\alpha_i} \cap C_k \neq \emptyset$ for some monomial x^{α_i} of f. Let $C_{k_1}, \dots, C_{k_s}$ be this finite collection, where $k_r \in \mathbb{N}$ for each $1 \leq r \leq s$ and $k_1 \neq \cdots \neq k_s$. So given $k \in \mathbb{N}$, if $k \neq k_r$ for any $1 \leq r \leq s$, then

$$\operatorname{supp} x^{\alpha_i} \cap C_k = \emptyset \tag{365}$$

for all monomials x^{α_i} of f. In particular, this implies $f \notin \mathfrak{p}_k$. Thus f is contained in at most finitely many of the $\mathfrak{p}_k$'s.

Now note that if $I \subseteq \bigcup_{r=1}^s \mathfrak{p}_{k_r}$, then by the usual prime avoidance argument, we would obtain $I \subseteq \mathfrak{p}_{k_r}$ for some $1 \leq r \leq s$, which would be a contradiction, thus we cannot have we $I \subseteq \bigcup_{r=1}^s \mathfrak{p}_{k_r}$. Hence there exists a $g \in I$ and an $l \in \mathbb{N}$ such that $l \neq k_r$ for any $1 \leq r \leq s$ and $g \in \mathfrak{p}_l \backslash \bigcup_{r=1}^s \mathfrak{p}_{k_r}$. Express g in terms of its monomials as

$$g = b_1 x^{\beta_1} + \cdots + b_n x^{\beta_n} \tag{366}$$

where $b_1, \dots, b_n \in K\backslash\{0\}$ and $\beta_1, \dots, \beta_n \in \mathcal{F}$ where $\beta_j \neq \beta_{j'}$ for all $1 \leq j < j' \leq m$. Since $g \in \mathfrak{p}_l$, we see that $\operatorname{supp} x^{\beta_j} \cap C_l \neq \emptyset$ for all monomials x^{β_j} of g. Since $\operatorname{supp} x^{\alpha_i} \cap C_l = \emptyset$ for all monomials x^{α_i} of f (take $k = l$ in (365)), it follows that $\alpha_i \neq \beta_j$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. It follows that $x^{\alpha_i} \neq x^{\beta_j}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. Thus every monomial of $f + g$ has the form x^{α_i} for some $1 \leq i \leq m$ or x^{β_j} for some $1 \leq j \leq n$ (there is no combination between a monomial of f and a monomial in g in the monomial expansion of $f + g$). We claim that $f + g \notin \mathfrak{p}_k$ for any $k \in \mathbb{N}$. Indeed, let $k \in \mathbb{N}$. We consider two cases:

Case 1: Suppose $k = k_r$ for some $1 \leq r \leq s$. Then since $g \notin \mathfrak{p}_{k_r}$, there exists a monomial x^{β_j} of g such that $\operatorname{supp} x^{\beta_j} \cap C_{k_r} = \emptyset$. Since x^{β_j} is also a monomial of $f + g$, it follows that $f + g \notin \mathfrak{p}_{k_r}$.

Case 2: Suppose $k \neq k_r$ for any $1 \leq r \leq s$. Then $\operatorname{supp} x^{\alpha_i} \cap C_l = \emptyset$ for all monomials x^{α_i} of f (as in (365)), so in particular $\operatorname{supp} x^{\alpha_1} \cap C_l = \emptyset$. Since x^{α_1} is also a monomial of $f + g$, it follows that $f + g \notin \mathfrak{p}_l$.

Thus we have constructed a polynomial $f + g$ in I which does not belong to $\mathfrak{p}_k$ for any $k \in \mathbb{N}$. This is a contradiction since $I \subseteq \bigcup_{k \in \mathbb{N}} \mathfrak{p}_k$.

Step 2: We show that R_S satisfies the conditions of (88.1) (stated and proved in appendix) which implies R_S is Noetherian. We will also show that $\dim R_S = \infty$. First, let us describe the maximal ideals in R_S. Recall that the prime ideals in R_S correspond to the prime ideals in R which are disjoint from S. For any prime ideal $\mathfrak{p}$ in R, we have

$$\begin{aligned} \mathfrak{p} \cap S = \emptyset &\iff \mathfrak{p} \subseteq \bigcup_{k \in \mathbb{N}} \mathfrak{p}_k \\ &\iff \mathfrak{p} \subseteq \mathfrak{p}_k \text{ for some } k \in \mathbb{N}, \end{aligned}$$

where the last if and only if follows from step 1. In particular, we see that the maximal ideals of R_S are precisely the localizations of the $\mathfrak{p}_k$'s, that is, they are of the form $\mathfrak{p}_{k,S} = S^{-1}\mathfrak{p}_k$ for some $k \in \mathbb{N}$. By transitivity of localization, we have $(R_S)_{\mathfrak{p}_{k,S}} \cong R_{\mathfrak{p}_k}$, and $R_{\mathfrak{p}_k}$ is Noetherian since it is a localization of a Noetherian ring, namely

$$R_{\mathfrak{p}_k} \cong K(\{x_m \mid \{x_n \mid n \in \mathbb{N}\backslash C_k\})[\{x_n \mid n \in C_k\}]_{\langle \{x_n \mid n \in C_k\} \rangle}. \tag{367}$$

Thus the first condition in (88.1) is satisfied. As for the second condition, recall in step 1 we showed that every nonzero $f \in R$ is contained in only finitely many of the $\mathfrak{p}_k$'s, and so certainly every nonzero $f/s \in R_S$ is contained in only finitely many of the $\mathfrak{p}_{k,S}$'s. Thus both conditions of (88.1) hold, and hence R_S is Noetherian. Finally, note that the isomorphism (367) also shows us that

$$\begin{aligned} \dim R_S &\geq \dim R_{\mathfrak{p}_k} \\ &= 2^{k-1}. \end{aligned}$$

Taking $k \to \infty$ gives us $\dim R_S = \infty$.

88.4 Appendix

88.4.1 If $R_\mathfrak{m}$ is noetherian and $\mathrm{V}_{\max}(x)$ is finite for all maximal ideals $\mathfrak{m}$ of R and nonzero $x \in R$, then R is noetherian.

Lemma 88.1. *Let R be a commutative ring with identity such that*

1. *for each maximal ideal $\mathfrak{m}$ of R, the local ring $R_\mathfrak{m}$ is Noetherian;*
2. *for each $x \in R\backslash\{0\}$, the set of maximal ideals of R which contain x is finite.*

Then R is Noetherian.

Proof. Let I be a nonzero ideal in R. By the hypothesis of R, only finitely many maximal ideals can contain I, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. Choose any nonzero x_0 in I and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_{r+s}$ be the maximal ideals which contain x_0. Since $\mathfrak{m}_{r+1}, \ldots, \mathfrak{m}_{r+s}$ do not contain I, there exists $x_j \in I$ such that $x_j \notin \mathfrak{m}_{r+j}$ for each $1 \leq j \leq s$. Since for each $1 \leq i \leq r$ the localization $R_{\mathfrak{m}_i}$ is Noetherian, we see that $I_{\mathfrak{m}_i}$ is finitely-generated. Thus there exists $x_{s+1}, \ldots, x_t$ in I whose images in $R_{\mathfrak{m}_i}$ generated $I_{\mathfrak{m}_i}$ for all $1 \leq i \leq r$.

We claim that $I_{\mathfrak{m}} = \langle x_0, \ldots, x_t \rangle_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R. Indeed, if $\mathfrak{m} \neq \mathfrak{m}_k$ for any $1 \leq k \leq r+s$, then $x_0 \notin \mathfrak{m}$. Thus the image of x_0 is a unit in $I_{\mathfrak{m}}$ and $\langle x_0, \ldots, x_t \rangle_{\mathfrak{m}}$, and hence

$$I_{\mathfrak{m}} = R_{\mathfrak{m}} = \langle x_0, \ldots, x_t \rangle_{\mathfrak{m}}.$$

If $\mathfrak{m} = \mathfrak{m}_{r+j}$ for some $1 \leq j \leq s$, then $x_j \notin \mathfrak{m}$ and $I \cap (R \backslash \mathfrak{m}) \neq \emptyset$. Thus again we have

$$I_{\mathfrak{m}} = R_{\mathfrak{m}} = \langle x_0, \ldots, x_t \rangle_{\mathfrak{m}}.$$

Finally, if $\mathfrak{m} = \mathfrak{m}_i$ for some $1 \leq i \leq r$, then by construction, we have $I_{\mathfrak{m}} = \langle x_0, \ldots, x_t \rangle_{\mathfrak{m}}$. Thus our claim is proved. Since $I_{\mathfrak{m}} = \langle x_0, \ldots, x_t \rangle_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R, it follows that $I = \langle x_0, \ldots, x_t \rangle$. In particular, we see that I is finitely-generated, and hence R is Noetherian. □

89 Homework 6

89.1 Prufer Domains

Exercise 50. Let R be an integral domain. Show that R is a Prüfer domain if and only if every overring of R is integrally closed. (Hint: consider $R_{\mathfrak{m}}$ for some maximal ideal and if $x, y \in R_{\mathfrak{m}}$, consider $R_{\mathfrak{m}}[y^2/x^2]$.

Solution 44. Suppose that R is a Prüfer domain and let A be an overring of R. By homework 4, problem 4, we know that A is itself a Prüfer domain. Every Prüfer domain is integrally closed (see Appendix), so A is integrally closed. Since A was arbitrary, it follows that every overring of R is integrally closed.

Conversely, suppose every overring of R is integrally closed and let $\mathfrak{p}$ be a prime ideal of R. We need to show that $R_{\mathfrak{p}}$ is a valuation domain. First note that $R_{\mathfrak{p}}$ is integrally closed since integral closures commute with localization.

89.2 Every Maximal Ideal of $K[T_1, \ldots, T_n]$ can be Generated by n Elements

Exercise 51. Show that if K is a field then any maximal ideal of $K[T_1, \ldots, T_n]$ can be generated by n elements.

Solution 45. By Hilbert's Nullstellensatz, the maximal $\mathfrak{m}$ is in the kernel of a K-algebra homomorphism from $K[T_1, \ldots, T_n]$ to L where L/K. is a finite field extension. For each $1 \leq i \leq n$ let α_i be the images of T_i under this homomorphism. We will build a sequence of polynomials $f_1, \ldots, f_n$ in $K[T_1, \ldots, T_n]$ such that $\mathfrak{m} = \langle f_1, \ldots, f_n \rangle$ and such that f_k is a polynomial in $K[T_1, \ldots, T_k]$ for all $1 \leq k \leq n$.

First we set $f_1(T_1)$ to be the minimal polynomial of α_1 over K. Next let $\pi_2(X)$ be the minimal polynomial of α_2 over $K(\alpha_1)$. The coefficients of $\pi_2(X)$ can be expressed as polynomials in α_1, and so in particular we can find a polynomial f_2 in $K[T_1, T_2]$ such that $f_2(\alpha_1, X) = \pi_2(X)$. Proceeding inductively, at the kth step, where $1 \leq k \leq n$, we let $\pi_k(X)$ be the minimal polynomial of α_k over $K(\alpha_1, \ldots, \alpha_{k-1})$ and we choose a polynomial a polynomials f_k in $K[T_1, \ldots, T_k]$ such that

$$f_k(\alpha_1, \ldots, \alpha_{k-1}, X) = \pi_k(X).$$

We claim that $\mathfrak{m} = \langle f_1, \ldots, f_n \rangle$. Indeed, we have $\mathfrak{m} \supseteq \langle f_1, \ldots, f_n \rangle$ since $\langle f_1, \ldots, f_n \rangle$ is in the kernel of the K-algebra homomorphism from $K[T_1, \ldots, T_n]$ to L. To see this, note that for each $1 \leq k \leq n$ we have

$$f_k(\alpha_1, \ldots, \alpha_{k-1}, \alpha_k) = \pi_k(\alpha_k) = 0.$$

We also have $\mathfrak{m} \subseteq \langle f_1, \ldots, f_n \rangle$ since $\langle f_1, \ldots, f_n \rangle$ is a maximal ideal. Indeed, we prove by induction on n that $K[T_1, \ldots, T_n]/\langle f_1, \ldots, f_n \rangle \cong K(\alpha_1, \ldots, \alpha_n)$. If $n = 1$, then

$$K[T_1]/\langle f_1 \rangle \cong K[X]/\pi_1(X) \cong K(\alpha_1).$$

Now suppose $n > 1$ and we have shown this to be true for all $1 \leq k < n$. Then we have

$$\begin{aligned}
K[T_1, \ldots, T_{n-1}, T_n]/\langle f_1, \ldots, f_{n-1}, f_n \rangle &\cong (K[T_1, \ldots, T_{n-1}]/\langle f_1, \ldots, f_{n-1} \rangle)\, [T_n]/\langle f_n(\overline{T_1}, \ldots, \overline{T_{n-1}}, T_n) \\
&\cong K(\alpha_1, \ldots, \alpha_{n-1})[T_n]/\langle f_n(\alpha_1, \ldots, \alpha_{n-1}, T_n) \rangle \\
&\cong K(\alpha_1, \ldots, \alpha_{n-1})[X]/\langle \pi_n(X) \rangle \\
&\cong K(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n),
\end{aligned}$$

where we used the induction step to get from the first line to the second line.

89.3 Localization and Completion

Exercise 52. Let R be an integral domain and let $S \subseteq R$ be a multiplicatively closed subset not containing 0.

1. Show that $R[x]_S = R_S[x]$.
2. Show that $R[[x]]_S \subseteq R_S[[x]]$.
3. Show that equality in 2 holds if and only if for every countable collection (s_n) of elements of S we have $\bigcap_{n \in \mathbb{N}} \langle s_n \rangle \neq 0$.
4. Show that if R is a PID then every $S \subseteq R$ satisfies the above property if and only if R is a field.

Solution 46. 1. Define $\varphi \colon R[x]_S \to R_S[x]$ by

$$\varphi\left(\left(\sum_{i=0}^{n} a_i x^i\right)/s\right) = \sum_{i=0}^{n}(a_i/s)x^i.$$

where $a_i \in R$ and $s \in S$. The map φ is clearly a well-defined injective ring homomorphism. Furthermore, it is surjective. Indeed, if $\sum_{i=0}^{n}(a_i/s_i)x^i \in R_S[x]$, then

$$\begin{aligned}\sum_{i=0}^{n}(a_i/s_i)x^i &= \frac{a_0}{s_0} + \frac{a_1}{s_1}x + \cdots + \frac{a_n}{s_n}x^n \\ &= \frac{a_0 s_1 \cdots s_n}{s_0 s_1 \cdots s_n} + \frac{s_0 a_1 s_2 \cdots s_n}{s_0 s_1 \cdots s_n}x + \cdots + \frac{s_0 \cdots s_{n-1} a_n}{s_0 s_1 \cdots s_n}x^n \\ &= \varphi\left(\frac{a_0 s_1 \cdots s_n + s_0 a_1 s_2 \cdots s_n x + \cdots + s_0 \cdots s_{n-1} a_n x^n}{s_0 s_1 \cdots s_n}\right)\end{aligned}$$

Thus $R[x]_S \cong R_S[x]$.

2. Define $\varphi \colon R[[x]]_S \to R_S[[x]]$ by

$$\varphi\left(\left(\sum_{n=0}^{\infty} a_n x^n\right)/s\right) = \sum_{n=0}^{\infty}(a_n/s)x^n \tag{368}$$

for all $\left(\sum_{n=0}^{\infty} a_n x^n\right)/s \in R[[x]]_S$. Let's check that (368) is well-defined. Suppose $\left(\sum_{n=0}^{\infty} a_n x^n\right)/s = \left(\sum_{n=0}^{\infty} a'_n x^n\right)/s'$. Then

$$\begin{aligned}\left(\sum_{n=0}^{\infty} a_n x^n\right)/s = \left(\sum_{n=0}^{\infty} a'_n x^n\right)/s' &\iff s'\left(\sum_{n=0}^{\infty} a_n x^n\right) = s\left(\sum_{n=0}^{\infty} a'_n x^n\right) \\ &\iff \sum_{n=0}^{\infty} s' a_n x^n = \sum_{n=0}^{\infty} s a'_n x^n \\ &\iff s' a_n = s a'_n \text{ for each } n \in \mathbb{N} \\ &\iff a_n/s = a'_n/s' \text{ for each } n \in \mathbb{N} \\ &\iff \sum_{n=0}^{\infty}(a_n/s)x^n = \sum_{n=0}^{\infty}(a'_n/s')x^n.\end{aligned}$$

This implies (368) is well-defined. Now we check that φ is injective. Note that

$$\begin{aligned}\left(\sum_{n=0}^{\infty} a_n x^n\right)/s \in \ker\varphi &\iff \sum_{n=0}^{\infty}(a_n/s)x^n = 0 \\ &\iff a_n/s = 0 \text{ for all } n \in \mathbb{N} \\ &\iff a_n = 0 \text{ for all } n \in \mathbb{N} \\ &\iff \sum_{n=0}^{\infty} a_n x^n = 0 \\ &\iff \left(\sum_{n=0}^{\infty} a_n x^n\right)/s = 0.\end{aligned}$$

It follows that φ is injective.

3. Keeping the same notation as before, we show φ is surjective if and only if S has the property that for every sequence (s_n) in S we have $\bigcap_{n\in\mathbb{N}}\langle s_n\rangle \neq 0$. Suppose S has the stated property. Let $\sum_{n=0}^{\infty}(a_n/s_n)x^n$ be an element of $R_S[[x]]$. Since $\bigcap_{n\in\mathbb{N}}\langle s_n\rangle \neq 0$, there exists a nonzero $t \in \bigcap_{n\in\mathbb{N}}\langle s_n\rangle$. Write $t = b_n s_n$ for all $n \in \mathbb{N}$ where $b_n \in R$. Note that this implies $b_1 s_1 = b_n s_n$ or $b_1/s_n = b_n/s_1$. We have

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{b_1 a_n}{s_n}x^n &= \sum_{n=0}^{\infty}\frac{b_n a_n}{s_1}x^n \\ &= \left(\sum_{n=0}^{\infty} b_n a_n x^n\right)/s_1\end{aligned}$$

In particular, it follows that

$$\varphi\left(\left(\sum_{n=0}^{\infty} b_n a_n x^n\right)/b_1 s_1\right) = \sum_{n=0}^{\infty}\frac{b_1 a_n}{s_n}x^n,$$

thus φ is surjective.

89.4 Weak Ass

Definition 89.1. Let R be a commutative ring with identity and let M be an R-module. A prime $\mathfrak{p}$ of R is **weakly associated** to M if there exists an element $u \in M$ such that $\mathfrak{p}$ is minimal among the prime ideals containing the annihilator $0 : u = \{a \in R \mid au = 0\}$. The set of all such primes is denoted $\mathrm{WeakAss}\, M$.

Proposition 89.1. *Let R be a commutative ring with identity. Then the set of all zerodivisors of R is given by the set*

$$\bigcup_{\mathfrak{p}\in\mathrm{WeakAss}\,R}\mathfrak{p}.$$

Proof. Suppose $x \in R$ is a zerodivisor. Then $0 : x$ is a proper ideal of R. Choose a minimal prime $\mathfrak{p}$ over $0 : x$. Then $\mathfrak{p}$ is a weakly associated prime to R and $x \in \mathfrak{p}$ implies

$$\{\text{set of zerodivisors of } R\} \subseteq \bigcup_{\mathfrak{p}\in\mathrm{WeakAss}\,R}\mathfrak{p}.$$

Conversely, suppose $x \in \bigcup_{\mathfrak{p}\in\mathrm{WeakAss}\,R}\mathfrak{p}$. Then $x \in \mathfrak{p}$ for some prime $\mathfrak{p}$ which is weakly associated to R. Since $\mathfrak{p}$ is weakly associated to R, there exists a $y \in R$ such that $\mathfrak{p}$ is a minimal prime over $0 : y$. Since localization is exact, we see that $\mathfrak{p}_\mathfrak{p}$ is a weakly associated prime to $R_\mathfrak{p}$, with $\mathfrak{p}_\mathfrak{p}$ being minimal over the annihiliator of $y/1$. Since $R_\mathfrak{p}$ is local and $\mathfrak{p}_\mathfrak{p}$ is minimal over the annihilator $0 : (y/1)$, we have $\mathrm{rad}(0 : (y/1)) = \mathfrak{p}_\mathfrak{p}$. In particular, there exists $n \in \mathbb{N}$ and a $z \in R\backslash\mathfrak{p}$ such that $x^n z \in 0 : y$, or in other words, such that $x^n zy = 0$. Note that $zy \neq 0$ as $z \notin \mathfrak{p}$, so if $n = 1$, then $xzy = 0$ implies x is a zerodivisor. Assume $n > 1$. Choose $m \in \mathbb{N}$ such that $m \leq n$ and $x^m zy = 0$ and $x^{m-1}zy \neq 0$. Then $x(x^{m-1}zy) = x^m zy = 0$ implies x is a zerodivisor. Thus

$$\{\text{set of zerodivisors of } R\} \supseteq \bigcup_{\mathfrak{p}\in\mathrm{WeakAss}\,R}\mathfrak{p}.$$

□

Exercise 53. Let R be a 0-dimensional ring. Then any nonunit of R is a zerodivisor.

Solution 47. We have

$$\begin{aligned}\{\text{set of zerodivisors of } R\} &= \bigcup_{\mathfrak{p}\in\mathrm{WeakAss}\,R}\mathfrak{p} \\ &= \bigcup_{\mathfrak{p}\in\mathrm{Spec}\,R}\mathfrak{p} \\ &= \{\text{nonunits of } R\},\end{aligned}$$

where we obtained the second line from the first line from the fact that R is 0-dimensional. Indeed, clearly we have

$$\bigcup_{\mathfrak{p}\in\mathrm{WeakAss}\,R}\mathfrak{p} \subseteq \bigcup_{\mathfrak{p}\in\mathrm{Spec}\,R}\mathfrak{p}.$$

Conversely, suppose $\mathfrak{p}$ is a prime ideal of R and choose $x \in \mathfrak{p}$. Then since $x \in \mathfrak{p}$ and $\mathfrak{p}$ is prime we have $\mathfrak{p} \supseteq 0 : x$ and since R is 0-dimensional we see that $\mathfrak{p}$ is minimal over $0 : x$. Thus $\mathfrak{p}$ is a weakly associated prime to R. It follows that

$$\bigcup_{\mathfrak{p}\in\mathrm{WeakAss}\,R}\mathfrak{p} \supseteq \bigcup_{\mathfrak{p}\in\mathrm{Spec}\,R}\mathfrak{p}.$$

89.5 Appendix

89.5.1 Prüfer domains are integrally closed

Lemma 89.1. *Let R be an integral domain, let K be its quotient field, and let $\overline{R}$ be the integral closure of R in K. Then*

$$\overline{R} \subseteq \bigcap_{R \subseteq A \subseteq K} A$$

where the intersection runs over all valuation overrings A of R.

Proof. This follows from the fact the every valuation ring is integrally closed. Indeed, let A be a valuation overring of R. Then since A is integrally closed and $R \subseteq A$, it follows that $\overline{R} \subseteq A$. Since A was arbitrary, we see that $\overline{R} = \bigcap_{R \subseteq A \subseteq K} A$ where the intersection runs over all valuation overrings A of R. □

Proposition 89.2. *Let R be a Prüfer domain. Then R is integrally closed.*

Proof. Let $\overline{R}$ be the integral closure of R. Observe that

$$\begin{aligned}
R &= \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} R_{\mathfrak{p}} && \text{(Homework 1, Problem 4)} \\
&\supseteq \bigcap_{A \text{ valuation overring of } R} A && \text{(Because } R \text{ is Prüfer)} \\
&\supseteq \overline{R} && \text{(Lemma above)} \\
&\supseteq R.
\end{aligned}$$

It follows that $R = \overline{R}$. Hence R is integrally closed. □

90 Homework 7

90.1 Strong Finite Type Ideals

Definition 90.1. Let R be a commutative ring with identity and let I be an ideal of R. We say that I is of **strong finite type** (SFT) if there is a finitely generated ideal $\mathfrak{a} \subseteq I$ and an integral $n \in \mathbb{N}$ such that $x^n \in \mathfrak{a}$ for all $x \in I$. We also say that the ring R is SFT if every ideal of R is SFT.

Exercise 54. Let R be a commutative ring with identity.

1. Show that R is SFT if and only if every prime ideal of R is SFT.

2. Show that if R is SFT then R satisfies the ascending chain condition on radical ideals.

3. Given an example of a ring that is SFT but not Noetherian.

4. Given an example of a ring that satisfies the ascending chain condition on radical ideals but is not SFT.

Solution 48. 1. If R is SFT, then every prime ideal of R is SFT by definition. Conversely, suppose every prime ideal of R is SFT and assume for a contradiction that R is not SFT. Let $(\mathcal{F}, \subseteq)$ be the partially ordered set where the underlying set $\mathcal{F}$ is

$$\mathcal{F} = \{\text{ideals } I \text{ of } R \text{ which are not SFT}\},$$

and where the partial order $\subseteq$ is inclusion. Since R is not SFT, the set $\mathcal{F}$ is nonempty. Furthermore, note that if $(I_\lambda)_{\lambda \in \Lambda}$ is a chain in $\mathcal{F}$, then $\bigcup_{\lambda \in \Lambda} I_\lambda \in \mathcal{F}$. Indeed, assume for a contradiction that $\bigcup_{\lambda \in \Lambda} I_\lambda$ is SFT. Then there exists a finitely generated ideal $\mathfrak{a} \subseteq \bigcup_{\lambda \in \Lambda} I_\lambda$ and an $n \in \mathbb{N}$ such that $x^n \in \mathfrak{a}$ for all $x \in \bigcup_{\lambda \in \Lambda} I_\lambda$. Writing $\mathfrak{a} = \langle x_1, \dots, x_n \rangle$, we see that since $\mathfrak{a} \subseteq \bigcup_{\lambda \in \Lambda} I_\lambda$, we must have $x_i \in \bigcup_{\lambda \in \Lambda} I_\lambda$ for each $1 \leq i \leq n$. This means $x_i \in I_{\lambda_i}$ for some $\lambda_i \in \Lambda$ for each $1 \leq i \leq n$. In particular, since $(I_\lambda)_{\lambda \in \Lambda}$ is a chain, there exists a $\lambda \in \Lambda$ such that $x_i \in I_\lambda$ for all $1 \leq i \leq n$. Thus $\mathfrak{a} \subseteq I_\lambda$ and we have $x^n \in \mathfrak{a}$ for all $x \in I_\lambda$ since this is true for all $x \in \bigcup_{\lambda \in \Lambda} I_\lambda$. However this contradicts the fact that I_λ is SFT. Therefore every chain in $(\mathcal{F}, \subseteq)$ has an upper bound in $(\mathcal{F}, \subseteq)$.

Now we apply Zorn's lemma to obtain an ideal I which is maximal in $(\mathcal{F}, \subseteq)$. We claim that I is a prime ideal. Indeed, assume for a contradiction that I is not prime. Choose $x, y \in R \backslash I$ such that $xy \in I$. By maximality of I, both $I + \langle x \rangle$ and $I + \langle y \rangle$ are SFT, so there exists finitely generated ideals $\mathfrak{a} \subseteq I + \langle x \rangle$ and $\mathfrak{b} \subseteq I + \langle y \rangle$ and integers

$m, n \in \mathbb{N}$ such that $z^m \in \mathfrak{a}$ for all $z \in I + \langle x \rangle$ and $z^n \in \mathfrak{b}$ for all $z \in I + \langle y \rangle$. Observe that $\mathfrak{ab}$ is a finitely generated ideal, and furthermore we have

$$\begin{aligned}\mathfrak{ab} &\subseteq (I + \langle x \rangle)(I + \langle y \rangle) \\ &\subseteq I^2 + \langle x \rangle I + I \langle y \rangle + \langle xy \rangle \\ &\subseteq I.\end{aligned}$$

Moreover, for any $z \in I$, we have $z^{m+n} = z^m z^n \in \mathfrak{ab}$ since $z^m \in \mathfrak{a}$ for all $z \in I + \langle x \rangle \supseteq I$ and $z^n \in \mathfrak{b}$ for all $z \in I + \langle y \rangle \supseteq I$. Thus I is SFT, which is a contradiction. Thus I is a prime ideal. However this contradicts the fact that all prime ideals are assumed to be SFT. Thus $\mathcal{F}$ is empty, which implies R is SFT.

2. Suppose R is SFT. Let (I_k) be an ascending chain of radical ideals of R. Since $\bigcup_{k=1}^{\infty} I_k$ is SFT, there exists a finitely generated ideal $\mathfrak{a} \subseteq \bigcup_{k=1}^{\infty} I_k$ and an $n \in \mathbb{N}$ such that $x^n \in \mathfrak{a}$ for all $x \in \bigcup_{k=1}^{\infty} I_k$. Since $\mathfrak{a}$ is finitely generated, we must have $\mathfrak{a} \subseteq I_N$ for some $N \in \mathbb{N}$ (see argument in proof of part 1 for justification). Since I_N is radical and $x^n \in \mathfrak{a} \subseteq I_N$ for all $x \in \bigcup_{k=1}^{\infty} I_k$, we must in fact have $I_N = \bigcup_{k=1}^{\infty} I_k$. Thus R satisfies the ascending chain condition on radical ideals.

3. Let $R = \mathbb{F}_2[\{x_n \mid n \in \mathbb{N}\}]$ and let $\mathfrak{m} = \langle \{x_n \mid n \in \mathbb{N}\} \rangle$ and set $A = R_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}^2$. The prime ideals of A are in bijection with prime ideals $\mathfrak{p}$ of R such that $\mathfrak{m}^2 \subseteq \mathfrak{p} \subseteq \mathfrak{m}$. There is only one such prime, namely $\mathfrak{m}$, so A contains just one prime ideal, namely $\mathfrak{n} = \mathfrak{m}_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}^2$. To see that A is SFT, it suffices to show that $\mathfrak{n}$ is SFT, by part 1. However this is clear since the zero ideal is finitely generated and $\gamma^2 = 0$ for all $\gamma \in \mathfrak{n}$. Indeed, suppose $f/g \in R_{\mathfrak{m}}$ represents γ where $f \in \mathfrak{m}$ and $g \in R \backslash \mathfrak{m}$. Express f in terms of its monomials as

$$f = a_1 x^{\alpha_1} + \cdots + a_n x^{\alpha_n}$$

where $a_i \in \mathbb{F}_2$. Here, the x^{α_i} are the monomials of f (see my HW 5, problem 3 for more detail about this notation). Since $f \in \mathfrak{m}$, we may as well assume that $\operatorname{supp} x^{\alpha_i} \neq \emptyset$ for each $1 \leq i \leq n$ (note that $\operatorname{supp} x^{\alpha} = \emptyset$ means $x^{\alpha} = 1$). Now observe that

$$f^2 = a_1 x^{2\alpha_1} + \cdots + a_n x^{2\alpha_n}$$

since we are working over a characteristic 2 ring. In particular, each monomial $x^{2\alpha_i}$ lands in $\mathfrak{m}^2$. In particular, $f^2 \in \mathfrak{m}^2$, and this implies $(f/g)^2 = f^2/g^2$ represents the zero element in $\mathfrak{n}$.

So A is indeed SFT as claimed, however it is not Noetherian as $\mathfrak{n}$ is not finitely-generated. To see why, note that $\mathfrak{n}$ is generated by $\{\overline{x}_n \mid n \in \mathbb{N}\}$

4. Let K be a field, let p be a prime, let $R = \bigcup_{n=0}^{\infty} K[x^{1/p^n}]$, and let $\mathfrak{m} = \bigcup_{n=0}^{\infty} \langle x^{1/p^n} \rangle$. Observe that $\mathfrak{m}$ is a maximal ideal since it is the kernel of the unique ring homomorphism $R \to K$ given by mapping x^{1/p^n} to 0 for all $n \in \mathbb{Z}_{\geq 0}$. Furthermore we have $\operatorname{ht} \mathfrak{m} = 1$. To see this, first note that R is a domain. Indeed, suppose $fg = 0$ for some $f, g \in R$. Since $(K[x^{1/p^n}])$ is an ascending sequence of rings and $R = \bigcup_{n=0}^{\infty} K[x^{1/p^n}]$, we see that $f, g \in K[x^{1/p^N}]$ for some $N \in \mathbb{Z}_{\geq 0}$. Then since $K[x^{1/p^N}]$ is a domain, we must have either $f = 0$ or $g = 0$. Thus we have a chain of prime ideals $0 \subseteq \mathfrak{m}$. Furthermore, suppose that $\mathfrak{p}$ is a nonzero prime ideal of R such that $\mathfrak{p} \subseteq \mathfrak{m}$. Let f be a nonzero element in $\mathfrak{p}$. Again, we must have $f \in K[x^{1/p^N}]$ for some $N \in \mathbb{Z}_{\geq 0}$ and so we can express f as polynoimal in x^{1/p^N} with coefficients in K. Furthermore since $f \in \mathfrak{m}$, the coefficient of f in degree zero must vanish, so if we denote $\gamma = x^{1/p^N}$, then f has the form

$$f = \gamma^m (a_k \gamma^k + a_{k-1} \gamma^{k-1} \cdots + a_1 \gamma + a_0)$$

where $m \geq 1$ and where $a_0, a_1, \ldots, a_{k-1}, a_k \in K$, where we may assume without loss of generality that $a_k \neq 0$ since $f \neq 0$.

$$\begin{aligned}f &= a_k x^{k/p^N} + a_{k-1} x^{(k-1)/p^N} \cdots + a_1 x^{1/p^N} \\ &= x^{1/n_1} \left(a_1 + a_2 x^{1/n_2 - 1/n_1} \cdots + a_r x^{1/n_r - 1/n_1} \right) \\ &= x^{1/n_1} \left(a_1 + a_2 x^{(n_1 - n_2)/n_1 n_2} \cdots + a_r x^{(n_1 - n_r)/n_1 n_r} \right).\end{aligned}$$

This impies $x^{1/n_1} \in \mathfrak{p}$ since $\mathfrak{p}$ is prime and $\sum_{i=1}^{r} a_i x^{(n_1 - n_i)/n_1 n_i} \notin \mathfrak{m} \supseteq \mathfrak{p}$. Furthermore, for any $n \in \mathbb{N}$, we obtain $x^{1/n} \in \mathfrak{p}$. Indeed, we have $x^{1/nn_1} \in \mathfrak{p}$ since $\mathfrak{p}$ is prime and $(x^{1/nn_1})^n = x^{1/n_1} \in \mathfrak{p}$, and thus $x^{1/n} = (x^{1/nn_1})^{n_1} \in \mathfrak{p}$. Therefore $\mathfrak{p} \supseteq \mathfrak{m}$, and since already we have $\mathfrak{p} \subseteq \mathfrak{m}$, we see that $\mathfrak{p} = \mathfrak{m}$.

So by localizing at $\mathfrak{m}$, we see that $R_{\mathfrak{m}}$ has exactly one nonzero prime ideal, and thus easily satisfies the ascending chain condition on radical ideals (all radical ideals are intersection of prime ideals). Note that R is a domain (if $fg = 0$ for some $f, g \in R$, then since $R = \bigcup_{n=1}^{\infty} K[x^{1/n}]$, we have $f, g \in K[x^{1/N}]$ for some $N \in \mathbb{N}$, and since

$K[x^{1/N}]$ is a domain, this implies either $f = 0$ or $g = 0$). Thus we may identify $R_{\mathfrak{m}}$ with a subring of the field of fractions of R and we may identify the localization map $\rho\colon R \to R_{\mathfrak{m}}$ with the inclusion map $R \subseteq R_{\mathfrak{m}}$. With this in mind, we will now show that $R_{\mathfrak{m}}$ is not SFT by showing that $\mathfrak{m}_{\mathfrak{m}}$ is not SFT. Assume for a contradiction that there exists a finitely generated ideal $\mathfrak{a} \subseteq \mathfrak{m}_{\mathfrak{m}}$ and an $N \in \mathbb{N}$ such that $\gamma^N \in \mathfrak{a}$ for all $\gamma \in \mathfrak{m}_{\mathfrak{m}}$. In particular, we must have $x^{N/n} \in \mathfrak{a}$ for all $n \in \mathbb{N}$, and by setting $n = Nm$, we see that this implies $x^{1/m} \in \mathfrak{a}$ for all $m \in \mathbb{N}$. This implies $\mathfrak{a} = \mathfrak{m}_{\mathfrak{m}}$, however we have a contradiction here because $\mathfrak{m}_{\mathfrak{m}}$ is not finitely generated. To see this, assume for a contradiction that $\mathfrak{m}_{\mathfrak{m}}$ is finitely generated. Then since $\mathfrak{m}_{\mathfrak{m}}$ is generated by $\{x^{1/n} \mid n \in \mathbb{N}\}$, and $\mathfrak{m}_{\mathfrak{m}}$ is finitely generated, it follows from Lemma (90.1) that $\mathfrak{m}_{\mathfrak{m}}$ can be generated by finitely many of the $x^{1/n}$, say $\mathfrak{m}_{\mathfrak{m}} = \langle x^{1/n_1}, \dots, x^{1/n_r} \rangle$. Choose $N \in \mathbb{N}$ such that $N > \max\{n_1, \dots, n_r\}$. Then there must exists a $g \in R \backslash \mathfrak{m}$ and polynomials $p_1, \dots, p_s \in R$ such that

$$gx^{1/N} = p_1 x^{1/n_1} + \cdots + p_s x^{1/n_s}.$$

Since $g \notin \mathfrak{m}$, one of the monomials in $gx^{1/N}$ will be

$$R_{\mathfrak{m}} = \left\{ \frac{f}{g} \mid f, g \in \bigcup_{n=1}^{\infty} K[x^{1/n}] \text{ and } g \notin \mathfrak{m} \right\}$$

but is not SFT. Indeed, let us first show that is satisfies the ascending chain condition on radical ideals. In fact, we will show that $R_{\mathfrak{m}}$ has exactly one nonzero prime ideal, namely $\mathfrak{m}_{\mathfrak{m}}$. To see this, suppose $\mathfrak{p}_{\mathfrak{m}}$ is a nonzero prime ideal of $R_{\mathfrak{m}}$, where $\mathfrak{p}_{\mathfrak{m}}$ is the localization of the nonzero prime ideal $\mathfrak{p}$ of R where $\mathfrak{p} \subseteq \mathfrak{m}$. Let $f \in \mathfrak{p}_{\mathfrak{m}}$. Since $f \in \mathfrak{m}_{\mathfrak{m}}$, we can express it as

$$f = a_1 x^{1/n_1} + \cdots + a_r x^{1/n_r}$$

for some $a_1, \dots, a_r \in R \backslash \{0\}$. By relabeling if necessary, we may assume that $n_1 = \max\{n_1, \dots, n_r\}$. Then we can express f as

$$\begin{aligned} f &= a_1 x^{1/n_1} + \cdots + a_r x^{1/n_r} \\ &= x^{1/n_1} \left(a_1 + a_2 x^{1/n_2 - 1/n_1} \cdots + a_r x^{1/n_r - 1/n_1} \right) \\ &= x^{1/n_1} \left(a_1 + a_2 x^{(n_1 - n_2)/n_1 n_2} \cdots + a_r x^{(n_1 - n_r)/n_1 n_r} \right). \end{aligned}$$

This impies $x^{1/n_1} \in \mathfrak{p}$ since $\mathfrak{p}$ is prime and $\sum_{i=1}^r a_i x^{(n_1 - n_i)/n_1 n_i} \notin \mathfrak{m} \supseteq \mathfrak{p}$. Furthermore, for any $n \in \mathbb{N}$, we obtain $x^{1/n} \in \mathfrak{p}$. Indeed, we have $x^{1/nn_1} \in \mathfrak{p}$ since $\mathfrak{p}$ is prime and $(x^{1/nn_1})^n = x^{1/n_1} \in \mathfrak{p}$, and thus $x^{1/n} = (x^{1/nn_1})^{n_1} \in \mathfrak{p}$. In particular this implies $\mathfrak{p} \supseteq \mathfrak{m}$. Since already we have $\mathfrak{p} \subseteq \mathfrak{m}$, we see that $\mathfrak{p} = \mathfrak{m}$.

90.2 Finitely Generated Ideals

Lemma 90.1. *Let R be a ring and let $\{x_\lambda\}_{\lambda \in \Lambda}$ be a collection of elements of R. If the ideal generated by $\{x_\lambda\}_{\lambda \in \Lambda}$ is finitely-generated, then it can be generated by finitely many of the x_λ's*

Proof. Indeed, suppose $\langle \{x_\lambda\}_{\lambda \in \Lambda} \rangle = \langle f_1, \dots, f_r \rangle$ where

$$f_i = a_{i1} x_{\lambda_{i1}} + \cdots + a_{in_i} x_{\lambda_{in_i}}$$

for each $1 \leq i \leq r$ where $a_{ij} \in R$. Then observe that

$$\begin{aligned} \langle \{x_\lambda\}_{\lambda \in \Lambda} \rangle &= \langle f_1, \dots, f_r \rangle \\ &\supseteq \langle \{x_{\lambda_{ij}} \mid 1 \leq i \leq r \text{ and } 1 \leq j \leq n_i\} \rangle \\ &\supseteq \langle \{x_\lambda\}_{\lambda \in \Lambda} \rangle \\ &= \langle f_1, \dots, f_r \rangle. \end{aligned}$$

□

Exercise 55. Let R be a domain with quotient field K with the property that every overring of R is Noetherian. Show that $\dim R \leq 1$.

Solution 49. Assume for a contradiction that $\dim R > 1$. Then there exists nonzero prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of R such that $0 \subset \mathfrak{p} \subset \mathfrak{q}$ where the inclusions are proper. Choose a nonzero $x \in \mathfrak{p}$, choose $y \in \mathfrak{q} \backslash \mathfrak{p}$, and let $S = \{x/y^n \mid n \in \mathbb{N}\}$. Since the overring $R[S]$ is Noetherian, we see that the ideal $\langle S \rangle$ of $R[S]$ must be finitely generated, say $\langle S \rangle = \langle x/y^{n_1}, \dots, x/y^{n_r} \rangle$. Here we are using the fact that a finite subset of S can be used as a generating set of $\langle S \rangle$ (see Lemma (90.1). In fact, setting $n = \max\{n_1, \dots, n_r\}$, it is easy to see that $\langle S \rangle = \langle x/y^n \rangle$. In particular, we have

$$\frac{x}{y^{n+1}} = \left(a_0 + a_1 \frac{x}{y} + a_2 \frac{x}{y^2} + \cdots + a_k \frac{x}{y^k} \right) \frac{x}{y^n} \tag{369}$$

for some $k \in \mathbb{N}$ and $a_i \in \mathbb{R}$ for all $1 \leq i \leq k$. Multiplying both sides of (369) by y^{n+k+1}/x gives us

$$y^k = a_0 y^{k+1} + a_1 x y^k + a_2 x y^{k-1} + \cdots + a_k x y.$$

In particular we see that $y^k(1 - a_0 y) \in \langle x \rangle \subseteq \mathfrak{p}$. Since $y \notin \mathfrak{p}$, it follows that $1 - a_0 y \in \mathfrak{p}$. However since $y \in \mathfrak{q}$, this implies $1 \in \mathfrak{q}$, a contradiction.

90.3 One-Dimensional Domain and Overrings

Exercise 56. Let A be 1-dimensional Noetherian domain, let $\mathfrak{p}$ be a prime ideal of A, and let B be an overring of A. Then there are only finitely many prime ideals of B which lie over $\mathfrak{p}$.

Solution 50. By a Theorem shown in class, we see that B is Noetherian. Thus $B/\mathfrak{p}B$ is a 0-dimensional Noetherian ring, hence must be Artinian. Since Artinian rings have only finitely many maximal ideals, we see that $B/\mathfrak{p}B$ has only finitely many maximal ideals. In particular, $B/\mathfrak{p}B$ has only finitely many prime ideals since $B/\mathfrak{p}B$ is 0-dimensional. Since the prime ideals in $B/\mathfrak{p}B$ are in bijection with the prime ideals in B which lie over $\mathfrak{p}$, this implies there exists only finitely many prime ideals of B which lie over $\mathfrak{p}$.

90.4 Von Neumann Rings

Exercise 57. Let R be a commutative ring. We recall that R is von Neumann if for all $x \in R$ there is a $y \in R$ such that $x = xyx$. Suppose that R is 0-dimensional and commutative with no nonzero nilpotent elements. Then R is von Neumann regular.

Solution 51. Let x be a nonzero element of R (clearly $x = 0$ then we just choose $y = 0$ to get $x = xyx$). To show that there exists a $y \in R$ such that $x = xyx = x^2 y$, it suffices to show that $\langle x \rangle = \langle x^2 \rangle$. Let $\mathfrak{m}$ be any maximal ideal of R. Note that since R is 0-dimensional, we see that $R_\mathfrak{m}$ is also 0-dimensional, and since R is reduced, we see that $R_\mathfrak{m}$ is reduced. Thus we have $\mathfrak{m}_\mathfrak{m} = \mathrm{N}(R_\mathfrak{m}) = 0$, and in particular, this implies $R_\mathfrak{m}$ is a field. Every nonzero ideal of a field is just the field itself, and thus

$$\langle x \rangle_\mathfrak{m} = R_\mathfrak{m} = \langle x^2 \rangle_\mathfrak{m}.$$

Since $\mathfrak{m}$ was arbitrary, we see that $\langle x \rangle_\mathfrak{m} = \langle x^2 \rangle_\mathfrak{m}$ for all maximal ideals of R. This implies $\langle x \rangle = \langle x^2 \rangle$. Since x was arbitrary, we see that R is von Neumann regular.

91 Homework 8

91.1 Every Ideal in a Dedekind Domain can be Generated by Two Elements

Exercise 58. Let R be a Dedekind domain and let I be an ideal of R. Show that I can be generated by two elements.

Solution 52. Write $I = \prod_{i=1}^r \mathfrak{p}_i^{a_i}$ where $\mathfrak{p}_i$'s are pairwise distinct prime ideals and where the a_i are nonnegative integers. Let $\alpha \in I$. If $I = \langle \alpha \rangle$ then we are done, so assume $\langle \alpha \rangle \subset I$ where the inclusion is strict. Since $\langle \alpha \rangle \subset I$, the prime factorization of $\langle \alpha \rangle$ must have the form

$$\langle \alpha \rangle = \prod_{i=1}^r \mathfrak{p}_i^{b_i} \prod_{j=1}^s \mathfrak{q}_j^{d_j},$$

where the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are all pairwise relatively prime, where $b_i \geq a_i$ for each i, and where d_j is a nonnegative integer for each j. For each i, choose $\beta_i \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$. Note that $\mathfrak{p}_i$ and $\mathfrak{q}_j$ being relatively prime implies $\mathfrak{p}_i^{a_i+1}$ and $\mathfrak{q}_j$ are relatively prime. Thus by the Chinese Remainder Theorem, we can find a $\beta \in R$ such that

$$\beta \equiv \beta_i \bmod \mathfrak{p}_i^{a_i+1} \quad \text{and} \quad \beta \equiv 1 \bmod \mathfrak{q}_j$$

for all i and j. In particular, $\beta \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$ for all i and $\beta \notin \mathfrak{q}_j$ for all j. Indeed, it is clear that $\beta \notin \mathfrak{q}_j$ since $\beta \equiv 1 \bmod \mathfrak{q}_j$ for all j. To see that $\beta \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$ for all i, observe that $\beta \equiv \beta_i \bmod \mathfrak{p}_i^{a_i+1}$ implies $\beta = \beta_i + \alpha_i$ for some

$\alpha_i \in \mathfrak{p}_i^{a_i+1}$. Thus clearly $\beta \in \mathfrak{p}_i^{a_i}$. If $\beta \in \mathfrak{p}_i^{a_i+1}$, then since $\beta_i = \alpha_i - \beta$, we would then have $\beta_i \in \mathfrak{p}_i^{a_i+1}$, which is a contradiction.

Note that since $\beta \in \mathfrak{p}_i^{a_i}$ for all i, we have

$$\begin{aligned}\beta &\in \bigcap_{i=1}^{r} \mathfrak{p}_i^{a_i} \\ &= \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} \\ &= I.\end{aligned}$$

Thus the prime factorization of $\langle \beta \rangle$ must have the form

$$\langle \beta \rangle = \prod_{i=1}^{r} \mathfrak{p}_i^{c_i} \prod_{k=1}^{t} \widetilde{\mathfrak{q}}_k^{e_k},$$

where the $\mathfrak{p}_i$ and $\widetilde{\mathfrak{q}}_k$ are all pairwise relatively prime, where $c_i \geq a_i$ for each i, and where e_k is a nonnegative integer for each j. However note that we must have $c_i \leq a_i$ since $\beta \notin \mathfrak{p}_i^{a_i+1}$ for each i and we cannot have $\mathfrak{q}_j = \widetilde{\mathfrak{q}}_k$ for some j and k since $\beta \notin \mathfrak{q}_j$ for all j. It follows that

$$\begin{aligned}\langle \alpha, \beta \rangle &= \prod_{i=1}^{r} \mathfrak{p}_i^{\min(b_i, c_i)} \prod_{j=1}^{s} \mathfrak{q}_j^{\min(d_j, 0)} \prod_{k=1}^{t} \widetilde{\mathfrak{q}}_k^{\min(0, e_k)} \\ &= \prod_{i=1}^{r} \mathfrak{p}_i^{\min(b_i, a_i)} \prod_{j=1}^{s} \mathfrak{q}_j^{\min(d_j, 0)} \prod_{k=1}^{t} \widetilde{\mathfrak{q}}_k^{\min(0, e_k)} \\ &= \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} \prod_{j=1}^{s} \mathfrak{q}_j^{0} \prod_{k=1}^{t} \widetilde{\mathfrak{q}}_k^{0} \\ &= \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} \\ &= I.\end{aligned}$$

91.2 Discriminant

Exercise 59. Let $d \in \mathbb{Z}\backslash\{0,1\}$ be squarefree, let $K = \mathbb{Q}(\sqrt{d})$, let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K, and let $\gamma = (1+\sqrt{d})/2$. Then show that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \bmod 4 \\ \mathbb{Z}[\gamma] & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

Solution 53. Clearly $\sqrt{d} \in \mathcal{O}_K$ since it is a root of the monic $X^2 - d$. Thus $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. We first want to show that either $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ or $\mathcal{O}_K = \mathbb{Z}[\gamma]$ depending on the congruence class of d modulo 4. Let $\alpha \in \mathcal{O}_K$ and express it as $\alpha = a + b\sqrt{d}$ for unique $a, b \in \mathbb{Q}$. Note that both rational numbers

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \alpha + \overline{\alpha} \quad \text{and} \quad \mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha}$$

are algebraic integers and thus must belong to $\mathbb{Z}$. Given that $\overline{\alpha} = a - b\sqrt{d}$, a quick computation gives us $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 2a$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = a^2 - db^2$. It follows that $2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$. In particular, $2a \in \mathbb{Z}$ implies either $a \in \mathbb{Z}$ or $a = n/2$ where n is an odd integer.

Case 1: First assume that $a \in \mathbb{Z}$. Then since $a^2 - db^2 \in \mathbb{Z}$, we see that $db^2 \in \mathbb{Z}$. But d is squarefree, so integrality db^2 tells us that we cannot have a prime p occuring in the denominator of b as a reduced-form fraction (we would not be able to cancel the denominator factor p^2 for b^2). It follows that $b \in \mathbb{Z}$, so $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

Case 2: Assume that $a = n/2$ for some integer n. Thus, $a^2 - db^2 = n^2/4 - db^2$ is an integer. In particular we have $db^2 = n^2/4 + k$ for some $k \in \mathbb{Z}$. Observe that

$$\begin{aligned}db^2 &= \frac{n^2}{4} + k \\ &= \frac{n^2 + 4k}{4}.\end{aligned}$$

Since n is odd, it follows that $n^2 + 4k$ is odd, and thus db^2 must have a denominator of 4 when written in reduced form. Again, since d is squarefree, it follows that $b = m/2$ for some odd integer m. Thus we can write

$$\gamma = \left(\frac{n-1}{2} + \frac{m-1}{2}\sqrt{d} \right) - \alpha$$

with $(n-1)/2 \in \mathbb{Z}$ and $(m-1)/2 \in \mathbb{Z}$. In particular, we have $\gamma \in \mathcal{O}_K$

Thus in either case, we see that $\mathcal{O}_K \subseteq \mathbb{Z}[\gamma]$. In fact, combining these two cases together tells us $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if and only if $\gamma \notin \mathcal{O}_K$. Indeed, clearly if $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, then $\gamma \notin \mathcal{O}_K$. Conversely, if $\gamma \notin \mathcal{O}_K$ then every $a + b\sqrt{d} \in \mathcal{O}_K$ must have $a \in \mathbb{Z}$ (otherwise we would get $\gamma \in \mathcal{O}_K$ by case 2, a contradiction), and thus by case 1, every $a + b\sqrt{d} \in \mathcal{O}_K$ belongs to $\mathbb{Z}[\sqrt{d}]$.

Now note that $\gamma \in \mathcal{O}_K$ if and only if $d \equiv 1 \bmod 4$. Indeed, if $\gamma \in \mathcal{O}_K$, then $(1-d)/4 = \mathrm{N}_{K/\mathbb{Q}}(\gamma) \in \mathbb{Z}$, which is equivalent to $d \equiv 1 \bmod 4$. Conversely, if $d \equiv 1 \bmod 4$, then we have $d = 1 + 4k$ for some $k \in \mathbb{Z}$. Thus

$$\begin{aligned}
\gamma^2 &= \left(\frac{1+\sqrt{d}}{2} \right)^2 \\
&= \frac{1 + d + 2\sqrt{d}}{4} \\
&= \frac{2 + 4k + 2\sqrt{d}}{4} \\
&= \frac{1 + 2k + \sqrt{d}}{2} \\
&= \frac{1+\sqrt{d}}{2} + k. \\
&= \gamma + k
\end{aligned}$$

It follows that $\gamma \in \mathcal{O}_K$. Thus

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}[\gamma] & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

91.3 Almost Integral

Exercise 60. Let R be a domain with quotient field K. We say $\omega \in K$ is **almost integral** over R if there is a nonzero $a \in R$ such that $a\omega^n \in R$ for all $n \in \mathbb{N}$. We say that R is completely integrally closed if it contains all of its almost integral elements.

1. Show that if $\omega \in K$ is integral, then ω is almost integral over R.
2. Show that if R is Noetherian and $\omega \in K$ is almost integral over R, then ω is integral over R.
3. Given an example of a domain R and an element $\omega \in K$ (where K is the quotient field of R) that is almost integral over R, but not integral over R.
4. Show that any UFD is completely integrally closed.

Solution 54. 1. Let $\omega \in K$ be integral over R. Write $\omega = a/b$ where $a, b \in R$ with $b \neq 0$. Choose $k \geq 1$ minimal and $a_0, a_1, \ldots, a_{k-1} \in R$ such that

$$\omega^k + a_{k-1}\omega^{k-1} + \cdots + a_1\omega + a_0 = 0. \tag{370}$$

We claim that for any for any $n \geq 0$, we have $b^k\omega^n \in R$. Indeed, first note that if $n > k$, then we can use the fact that ω is integral (so $R[\omega] = \sum_{i=0}^{k-1} R\omega^i$) to write

$$\omega^n = a_{k-1,n}\omega^{k-1} + \cdots + a_{1,n}\omega + a_{0,n}$$

for some $a_{0,n}, a_{1,n}, \ldots, a_{k-1,n} \in R$, so it suffices to show that $b^k\omega^n \in R$ when $n \leq k$. This is clear though since

$$\begin{aligned}
b^k\omega^n &= b^k \frac{a^n}{b^n} \\
&= b^{k-n}a^n \\
&\in R.
\end{aligned}$$

It follows that ω is almost integral over R.

2. Suppose R is a Noetherian domain and let $\omega \in K$ be almost integral over R. Choose $a \in R \backslash \{0\}$ such that $a\omega^n \in R$ for all $n \in \mathbb{N}$. Consider the ascending chain of ideals (I_n) where

$$\begin{aligned} I_0 &= \langle a \rangle \\ I_1 &= \langle a, a\omega \rangle \\ &\vdots \\ I_n &= \langle a, a\omega, \dots, a\omega^n \rangle \\ &\vdots \end{aligned}$$

for all $n \in \mathbb{N}$. The ascending chain of ideals (I_n) must terminate since R is Noetherian, say at $m \in \mathbb{N}$. It follows that $a\omega^{m+1} \in I_m$, which implies

$$a\omega^{m+1} = a_m a\omega^m + \cdots + a_1 a\omega + a_0 a \tag{371}$$

for some $a_0, a_1, \dots, a_m \in R$. Canceling a from both sides of (353) (we can do this since A is a domain) and rearranging terms gives us

$$\omega^{m+1} - a_m\omega^m - \cdots - a_1\omega - a_0 = 0.$$

This implies ω is integral over R.

3. Consider ring $A = K[y, \{x/y^n \mid n \in \mathbb{N}\}]$. We have a strict inclusion of rings

$$K[x,y] \subset A \subset K[x,y,1/y].$$

In particular, A is a domain with fraction field $K(x,y)$. Note that $1/y \in K(x,y)$ is almost integral over A since $1/y \notin A$ and $x/y^n \in A$ for all $n \in \mathbb{N}$. On the other hand, $1/y$ is not integral over A. Indeed, if it were, then there would exists $m \in \mathbb{N}$ and $f_0, \dots, f_{m-1} \in A$ such that

$$\frac{1}{y^m} = \frac{f_{m-1}}{y^{m-1}} + \cdots + \frac{f_1}{y} + f_0. \tag{372}$$

Multilpying y^m on both sides of (349) gives us

$$1 = (f_{m-1} + \cdots + f_1 y^{m-2} + f_0 y^{m-1})y. \tag{373}$$

Evaluating $x = 0$ to both sides of (350) gives us

$$1 = (\widetilde{f}_{m-1} + \cdots + \widetilde{f}_1 y^{m-2} + \widetilde{f}_0 y^{m-1})y. \tag{374}$$

where $\widetilde{f}_0, \widetilde{f}_1, \dots, \widetilde{f}_{m-1}$ are polynomials over K in the variable y. Evaluating $y = 0$ to both sides of (351) gives us $1 = 0$, which is a contradiction.

4. Let R be a UFD, let K denote its fraction field, and let $\omega \in K$ be almost integral over R. Choose a nonzero $a \in R$ such that $a\omega^n \in R$ for all $n \in \mathbb{N}$.

Part IX
Algebra Prelim Solutions

92 Winter 2020

92.1 Linear Algebra

92.1.1 Cyclic Vectors

Exercise 61. Let V be an n-dimensional vector space over a field K and let $T\colon V \to V$ be a linear map. We say $v \in V$ is a **cyclic vector** for T if $\{v, Tv, \dots, T^{n-1}v\}$ is a basis for V. Let $\chi_T(X) \in K[X]$ be the characteristic polynomial of T and let $\pi_T(X) \in K[X]$ be the minimal polynomial of T over K. Prove the following:

1. Let $v \in V$ and suppose $T^{n-1}v \neq 0$ but $T^n v = 0$. Then v is a cyclic vector for T.

2. If V has a cyclic vector for T, then $\chi_T = \pi_T$.

3. If T is diagonalizable and $\chi_T = \pi_T$, then V has a cyclic vector for T.

4. If V has a cyclic vector for T and $S\colon V \to V$ is a linear map which commutes with T, then S is a polynomial in T.

Solution 55. 1. We first show $\{v, Tv, \dots, T^{n-1}v\}$ is linearly independent. Suppose we have

$$a_0 v + a_1 Tv + \cdots + a_{n-1}T^{n-1}v = 0 \tag{375}$$

for some $a_0, a_1, \dots, a_{n-1} \in K$. Applying T^{n-1} to both sides of (375) gives us $a_0 T^{n-1}v = 0$. Since $T^{n-1}v \neq 0$, we must have $a_0 = 0$. Thus (375) becomes

$$a_1 Tv + a_2 T^2 v + \cdots + a_{n-1}T^{n-1}v = 0 \tag{376}$$

Applying T^{n-2} to both sides of (376) gives us $a_1 T^{n-1}v = 0$. Since $T^{n-1}v \neq 0$, we must have $a_1 = 0$. Proceeding inductively, we have

$$a_k T^k v + a_{k+1}T^{k+1}v + \cdots + a_{n-1}T^{n-1}v = 0 \tag{377}$$

for some $1 \leq k \leq n-1$. Applying T^{n-1-k} to both sides of (377) gives us $a_k T^{n-1}v = 0$. Since $T^{n-1}v \neq 0$, we must have $a_k = 0$. This implies $a_1 = a_2 = \cdots = a_{n-1} = 0$, and thus $\{v, Tv, \dots, T^{n-1}v\}$ is linearly independent. Finally, observe that $\{v, Tv, \dots, T^{n-1}v\}$ spans V since $\operatorname{span}_K(\{v, Tv, \dots, T^{n-1}v\}) \subseteq V$ and $\dim V = n = \#\{v, Tv, \dots, T^{n-1}v\}$. Therefore $\{v, Tv, \dots, T^{n-1}v\}$ is a basis for V.

2. Let $v \in V$ be a cyclic vector for T. Express the minimal polynomial of T over K as

$$\pi_T(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0,$$

where $1 \leq k \leq n$. As π_T is the minimal polynomial of T over K, we must have

$$T^k v + a_{k-1}T^{k-1}v + \cdots + a_1 T + a_0 = 0. \tag{378}$$

If $k \leq n-1$, then (378) gives a nontrivial relation in $\{v, Tv, \dots, T^{n-1}v\}$, contradicting the fact that $\{v, Tv, \dots, T^{n-1}v\}$ is linearly independent. Thus $k = n$, which implies $\pi_T = \chi_T$ since $\pi_T \mid \chi_T$ and both π_T and χ_T are monic of the same degree.

3. Suppose T is diagonalizable and $\pi_T = \chi_T$. Let $\{v_1, \dots, v_n\}$ be an eigenbasis for T with corresponding eigenvalues $\{\lambda_1, \dots, \lambda_n\}$. Suppose we have

$$a_0 v + a_1 Tv + \cdots + a_{n-1}T^{n-1}v = 0 \tag{379}$$

for some $a_0, a_1, \dots, a_{n-1} \in K$. Then we have

$$\begin{aligned} 0 &= a_0 v + a_1 Tv + \cdots + a_{n-1}T^{n-1}v \\ &= \sum_{i=0}^{n-1} a_i \lambda_k^i v \end{aligned}$$

92.1.2 Hom

Exercise 62. Let V and W be real vector spaces, and let $\operatorname{Hom}_{\mathbb{R}}(W, V)$ denote the set of linear transformations $W \to V$, which is a real vector space.

1. Let $z \in \mathbb{C}$ and $\phi \in \operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Define $z\phi\colon \mathbb{C} \to V$ by the formula

$$(z\phi)(w) = \phi(zw) \tag{380}$$

for all $w \in \mathbb{C}$. Prove that $z\phi \in \operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, V)$.

2. Prove that $\operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ is a complex vector space using (380) to define scalar multiplication.

3. Prove that if $d = \dim_{\mathbb{R}}(V) < \infty$, then $\dim_{\mathbb{C}}(\operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, V)) = d$.

4. Prove that if $f\colon V \to W$ is a linear transformation over $\mathbb{R}$, then the function $f_*\colon \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V) \to \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, W)$, defined by

$$f_*(\phi) = f \circ \phi$$

for all $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$, is a linear transformation over $\mathbb{C}$.

5. Prove that if $\lambda \in \mathbb{R}$ is an eigenvalue for a linear transformation $f\colon V \to V$, then λ is an eigenvalue for $f_*\colon \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V) \to \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$.

Solution 56. 1. Let $z_1, z_2 \in \mathbb{C}$ and let $a_1, a_2 \in \mathbb{R}$. Then we have

$$\begin{aligned}(z\phi)(a_1z_1 + a_2z_2) &= \phi(z(a_1z_1 + a_2z_2)) \\ &= \phi(a_1zz_1 + a_2zz_2) \\ &= a_1\phi(zz_1) + a_2\phi(zz_2) \\ &= a_1(z\phi)(z_1) + a_2(z\phi)(z_2).\end{aligned}$$

It follows that $z\phi$ is $\mathbb{R}$-linear, and hence $z\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$.

2. We give $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ a complex vector space structure via the scalar multiplication

$$z \cdot \phi = z\phi$$

for all $z \in \mathbb{C}$ and $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$, where $z\phi$ is the $\mathbb{R}$-linear map defined in (380). First note that $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ is an abelian since it already has the structure of an $\mathbb{R}$-vector space, so we just need to show that $\mathbb{C}$ acts on $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ by additive maps. Clearly $1 \cdot \phi = \phi$ for all $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Let $z_1, z_2 \in \mathbb{C}$ and let $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Then for all $w \in \mathbb{C}$, we have

$$\begin{aligned}(z_1 \cdot (z_2 \cdot \phi))(w) &= (z_1(z_2\phi))(w) \\ &= (z_2\phi)(z_1w) \\ &= \phi(z_2z_1w)) \\ &= \phi(z_1z_2w) \\ &= ((z_1z_2)\phi)(w) \\ &= (z_1z_2 \cdot \phi)(w).\end{aligned}$$

It follows that $z_1 \cdot (z_2 \cdot \phi) = z_1z_2 \cdot \phi$.

Next, let $z \in \mathbb{C}$ and let $\phi_1, \phi_2 \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Then for all $w \in \mathbb{C}$, we have

$$\begin{aligned}(z \cdot (\phi_1 + \phi_2))(w) &= (z(\phi_1 + \phi_2))(w) \\ &= (\phi_1 + \phi_2)(zw) \\ &= \phi_1(zw) + \phi_2(zw) \\ &= (z\phi_1)(w) + (z\phi_2)(w) \\ &= (z \cdot \phi_1)(w) + (z \cdot \phi_2)(w) \\ &= (z \cdot \phi_1 + z \cdot \phi_2)(w).\end{aligned}$$

It follows that $z \cdot (\phi_1 + \phi_2) = z \cdot \phi_1 + z \cdot \phi_2$. A similar calculation also shows that if $z_1, z_2 \in \mathbb{C}$ and $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$, then $(z_1 + z_2) \cdot \phi = z_1 \cdot \phi + z_2 \cdot \phi$.

3. Before we prove this, let us prove another result:

Proposition 92.1. *Let L/K be a finite extension of fields and let V be a finite dimensional L-vector space (so V is a K-vector space by restriction of scalars). Then we have*

$$\dim_L V = [L : K] \cdot \dim_K V.$$

Proof. Denote $m = [L : K]$ and denote $n = \dim_K V$. Let $\mathbf{e} = (e_1, \dots, e_m)$ be an ordered basis for L as a K-vector space, and let $\mathbf{v} = (v_1, \dots, v_n)$ be an ordered basis for V as an L-vector space. We claim that $\mathbf{e} \otimes \mathbf{v} = (e_1v_1, \dots, e_1v_n, e_2v_1, \dots, e_2v_n, \dots, e_mv_1, \dots, e_mv_n)$ is an ordered basis for V as a K-vector space. Indeed, let us first show that $\mathbf{e} \otimes \mathbf{v}$ spans V as a K-vector space. Let $v \in V$. Since $\mathbf{v}$ spans V as a L-vector space, we have

$$v = b_1v_1 + \cdots + b_nv_n$$

for some $b_1, \dots, b_n \in L$. Since $\mathbf{e}$ spans L as a K-vector space, for each $1 \leq j \leq n$ we have

$$b_j = a_{1j}e_1 + \cdots + a_{mj}e_m.$$

for some $a_{1j}, \ldots, a_{mj} \in K$. Therefore, we have

$$\begin{aligned} v &= \sum_{j=1}^{n} b_j v_j \\ &= \sum_{i=1}^{n} \left(\sum_{i=1}^{m} a_{ij} e_i \right) v_j \\ &= \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{ij} e_i v_j. \end{aligned}$$

Therefore $\mathbf{e} \otimes \mathbf{v}$ spans V as K-vector space. Next we show that $\mathbf{e} \otimes \mathbf{v}$ is linearly independent. Suppose we have

$$\sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{ij} e_i v_j = 0$$

for some $a_{ij} \in K$. Since $\mathbf{v}$ is linearly independent, this implies

$$\sum_{i=1}^{m} a_{ij} e_i = 0$$

for each $1 \le j \le n$. Since $\mathbf{e}$ is linearly independent, this implies $a_{ij} = 0$ for each $1 \le i \le m$ and for each $1 \le j \le n$. Thus $\mathbf{e} \otimes \mathbf{v}$ is linearly independent. $\square$

Now we continue with our original problem. First note that as an $\mathbb{R}$-vector space, we have $\dim_{\mathbb{R}}(\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)) = 2d$. Thus, the proposition above tells us that as $\mathbb{C}$-dimensional vector space, we must have $\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)) = d$.

4. Let $z_1, z_2 \in \mathbb{C}$ and let $\phi_1, \phi_2 \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Then for all $w \in \mathbb{C}$, we have

$$\begin{aligned} f_*(z_1\phi_1 + z_2\phi_2)(w) &= (f \circ (z_1\phi_1 + z_2\phi_2))(w) \\ &= f((z_1\phi_1 + z_2\phi_2)(w)) \\ &= f(z_1(\phi_1(w)) + z_2(\phi_2(w))) \\ &= z_1 f(\phi_1(w)) + z_2 f(\phi_2(w)) \\ &= z_1(f \circ \phi_1)(w) + z_2(f \circ \phi_2)(w) \\ &= z_1(f_*\phi_1)(w) + z_2(f_*\phi_2)(w) \\ &= (z_1(f_*\phi_1) + z_2(f_*\phi_2))(w). \end{aligned}$$

It follows that f_* is $\mathbb{C}$-linear.

5. Choose an eigenvector $v \in V$ for f corresponding to the eigenvalue $\lambda \in \mathbb{R}$. Let $\phi\colon \mathbb{C} \to V$ be the unique $\mathbb{R}$-linear map given by mapping $1 \mapsto v$ and $i \mapsto 0$ (note that $(1, i)$ is an ordered basis for $\mathbb{C}$ as an $\mathbb{R}$-vector space and hence any $\mathbb{R}$-linear map out of $\mathbb{C}$ is completely determined by where it maps the ordered basis $(1, i)$). Then observe that for all $a + ib \in \mathbb{C}$, we have

$$\begin{aligned} (f_*\phi)(a + ib) &= (f \circ \phi)(a + ib) \\ &= f(\phi(a + ib)) \\ &= f(a\phi(1) + b\phi(i)) \\ &= f(av) \\ &= af(v) \\ &= a\lambda v \\ &= \lambda a v \\ &= \lambda(a\phi(1) + b\phi(i)) \\ &= \lambda\phi(a + ib). \end{aligned}$$

It follows that $f_*\phi = \lambda\phi$. Thus λ is an eigenvalue for f_* with ϕ being a corresponding eigenvector.

92.1.3 Action of $K[t]$ on V via linear map

Exercise 63. Let $f\colon V \to V$ be any linear map of vector spaces over a field K. Define an action of $K[X]$ on V as follows: for any polynomial $p(X)$

Solution 57.

We give V the structure of a $K[X]$-module by defining

$$p(X) \cdot v = p(f)(v) \tag{381}$$

for all $p(X) \in K[X]$ and for all $v \in V$. Let $v, w \in \ker(p(X))$ and let $a, b \in K$. Then

$$\begin{aligned}
p(X) \cdot (av + bw) &= p(f)(av + bw) \\
&= \sum_{i=0}^{n} c_i f^i(av + bw) \\
&= \sum_{i=0}^{n} c_i(af^i(v) + bf^i(w)) \\
&= a\sum_{i=0}^{n} c_i f^i(v) + b\sum_{i=0}^{n} c_i f^i(w) \\
&= a(p(X) \cdot v) + b(p(X) \cdot w) \\
&= 0 + 0 \\
&= 0.
\end{aligned}$$

Thus $av + bw \in \ker(p(X))$ which implies $\ker(p(X))$ is a linear subspace of V. In particular, when $p(X) = X - \lambda$ where $\lambda \in K$, we have

$$\begin{aligned}
v \in \ker(p(X)) &\iff v \in \ker(X - \lambda) \\
&\iff (X - \lambda) \cdot v = 0 \\
&\iff (f - \lambda)(v) = 0 \\
&\iff f(v) = \lambda v.
\end{aligned}$$

Thus $v \in \ker(p(X))$ if and only if v is an eigenvector of f with eigenvalue λ. Therefore $\ker(p(X)) = E_\lambda$ where E_λ is the eigenspace of f with respect to λ.

Now write

$$p(X) = \sum_{i=0}^{m} c_i X^i \quad \text{and} \quad q(X) = \sum_{j=0}^{n} d_j X^j$$

We first show that

$$\ker(p(X)q(X)) = \ker(p(X)) + \ker(q(X)). \tag{382}$$

Let $v \in \ker(p(X)) + \ker(q(X))$. Write $v = v_1 + v_2$ where $v_1 \in \ker(p(X))$ and $v_2 \in \ker(q(X))$. Then

$$\begin{aligned}
(p(X)q(X)) \cdot v &= p(X) \cdot (q(X) \cdot v) \\
&= p(X) \cdot (q(X) \cdot (v_1 + v_2)) \\
&= p(X) \cdot (q(X) \cdot v_1 + q(X) \cdot v_2) \\
&= p(X) \cdot (q(X) \cdot v_1) \\
&= (p(X)q(X)) \cdot v_1 \\
&= (q(X)p(X)) \cdot v_1 \\
&= q(X) \cdot (p(X) \cdot v_1) \\
&= q(X) \cdot 0 \\
&= 0
\end{aligned}$$

implies $v \in \ker(p(X)q(X))$. Thus $\ker(p(X)) + \ker(q(X)) \subseteq \ker(p(X)q(X))$. For the reverse inclusion, choose $a(X), b(X) \in K[X]$ so that

$$a(X)p(X) + b(X)q(X) = 1. \tag{383}$$

Let $v \in \ker(p(X)q(X))$. Using (91), write $v = v_1 + v_2$ where

$$v_1 = (b(X)q(X)) \cdot v \quad \text{and} \quad v_2 = (a(X)p(X)) \cdot v.$$

Then $v_2 \in \ker(q(X))$ since

$$\begin{aligned} q(X) \cdot v_2 &= q(X) \cdot ((a(X)p(X)) \cdot v) \\ &= (q(X)a(X)p(X)) \cdot v \\ &= (a(X)p(X)q(X)) \cdot v \\ &= a(X) \cdot (p(X)q(X) \cdot v) \\ &= a(X) \cdot 0 \\ &= 0. \end{aligned}$$

Similarly, $v_1 \in \ker(p(X))$ since

$$\begin{aligned} p(X) \cdot v_1 &= p(X) \cdot ((b(X)q(X)) \cdot v) \\ &= (p(X)b(X)q(X)) \cdot v \\ &= (b(X)p(X)q(X)) \cdot v \\ &= b(X) \cdot (p(X)q(X) \cdot v) \\ &= b(X) \cdot 0 \\ &= 0. \end{aligned}$$

Therefore $v \in \ker(p(X)) + \ker(q(X))$, and this implies $\ker(p(X)) + \ker(q(X)) \supseteq \ker(p(X)q(X))$.

To see that (382) is a direct sum, let $v \in \ker(p(X)) \cap \ker(q(X))$. Then

$$\begin{aligned} v &= 1 \cdot v \\ &= (a(X)p(X) + b(X)q(X)) \cdot v \\ &= (a(X)p(X)) \cdot v + (b(X)q(X)) \cdot v \\ &= a(X) \cdot (p(X) \cdot v) + b(X) \cdot (q(X) \cdot v) \\ &= a(X) \cdot 0 + b(X) \cdot 0 \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Thus $\ker(p(X)) \cap \ker(q(X)) = 0$ and so the sum (382) is direct.

We first prove by induction on $m \geq 2$ that for polynomials $p_i(X) \in K[X]$ such that $\gcd(p_i(X), p_j(X)) = 1$ for all $1 \leq i < j \leq m$, we have

$$\ker(p_1(X)p_2(X) \cdots p_m(X)) = \ker(p_1(X)) \oplus \ker(p_2(X)) \oplus \cdots \oplus \ker(p_m(X)). \tag{384}$$

The base case $m = 2$ was established in problem b.2. Now assume (93) is true for some $m \geq 2$. Let $p_i(X) \in K[X]$ such that $\gcd(p_i(X), p_j(X)) = 1$ for all $1 \leq i < j \leq m+1$. Since $\gcd(p_1(X), p_i(X)) = 1$ for all $2 \leq i \leq m+1$, we have $\gcd(p_1(X), p_2(X) \cdots p_{m+1}(X)) = 1$. Therefore

$$\begin{aligned} \ker(p_1(X)p_2(X) \cdots p_{m+1}(X)) &= \ker(p_1(X)) \oplus \ker(p_2(X) \cdots p_{m+1}(X)) \\ &= \ker(p_1(X)) \oplus \ker(p_2(X)) \oplus \cdots \oplus \ker(p_{m+1}(X)), \end{aligned}$$

where we used the base case on the first line and where we used the induction hypothesis to get from the first line to the second line.

To finish the problem, we just need to show that $V = \ker(c(X))$. Let $v \in V$. Then

$$\begin{aligned} c(X) \cdot v &= c(f)(v) \\ &= 0(v) \\ &= 0 \end{aligned}$$

implies $v \in \ker(c(X))$. Therefore $V \subseteq \ker(c(X))$, which implies $V = \ker(c(X))$ (since $\ker(c(X))$ was already shown to be a subspace of V in problem b.1).

Let $E = \sum_{i=1}^{t} E_{\lambda_i}$ and let $c(X)$ be given by

$$c(X) = (X - \lambda_1) \cdots (X - \lambda_t),$$

where $\lambda_1, \ldots, \lambda_t$ are the distinct eigenvalues of f. Since $(X - \lambda_i)$ and $(X - \lambda_j)$ are relatively prime for all $1 \leq i < j \leq t$ and since $c(f) = 0$ on E, we can apply problem b.3 and obtain

$$E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_t}$$

In particular $B_1 \cup B_2 \cup \cdots \cup B_t$ must be linearly independent: Suppose

$$\sum_{i=1}^{t} \sum_{j=1}^{m_i} a_{ij} u_{ij} = 0. \tag{385}$$

Then for each $1 \leq i \leq t$, we must have $\sum_{j=1}^{m_i} a_{ij} u_{ij} = 0$. Indeed, if $\sum_{j=1}^{m_k} a_{kj} u_{kj} \neq 0$ for some $1 \leq k \leq t$, then we can rearrange (94) to get

$$\sum_{j=1}^{m_k} a_{kj} u_{kj} = - \sum_{\substack{1 \leq i \leq t \\ i \neq k}} \sum_{j=1}^{m_i} a_{ij} u_{ij},$$

and so

$$\begin{aligned} 0 &\neq \sum_{j=1}^{m_k} a_{kj} u_{kj} \\ &\in E_{\lambda_k} \cap \bigoplus_{\substack{1 \leq i \leq t \\ i \neq k}} E_{\lambda_i} \\ &= \{0\}, \end{aligned}$$

gives us our desired contradiction. Thus, for each $1 \leq i \leq t$, we have

$$\sum_{j=1}^{m_i} a_{ij} u_{ij} = 0.$$

But this implies $a_{ij} = 0$ for all $1 \leq j \leq m_i$ since B_i is a basis for all $1 \leq i \leq t$. Thus $a_{ij} = 0$ for all $1 \leq i \leq t$ and $1 \leq j \leq m_i$, and hence $B_1 \cup B_2 \cup \cdots \cup B_t$ is linearly independent.

92.2 Abstract Algebra

92.2.1 Commutator Subgroup

Exercise 64. Let G be a group. If $x, y \in G$, we define the commutator of x and y to be $[x, y] = x^{-1}y^{-1}xy$ and denote the commutator subgroup by $[G, G]$. (recall that the commutator subgroup of G is the subgroup of G that is *generated* by the commutators of G).

1. Show that the inverse of a commutator is a commutator and that any conjugate of a commutator is a commutator.
2. Show that $[G, G]$ is a normal subgroup of G.
3. Show that if $\psi \in \mathrm{Aut}(G)$, then $\psi([G, G])$ is a subgroup of $[G, G]$.
4. Show that if $\varphi\colon G \to H$ is a homomorphism of groups, then $\operatorname{im} \varphi$ is abelian if and only if $[G, G]$ is a subgroup of $\ker \varphi$.
5. Show that if N is a subgroup of G which contains $[G, G]$, then N is a normal subgroup of G.

Solution 58. 1. Let $x, y \in G$. Then note that

$$\begin{aligned} [x, y]^{-1} &= (x^{-1}y^{-1}xy)^{-1} \\ &= y^{-1}x^{-1}yx \\ &= [y, x]. \end{aligned}$$

2. First note that if $x, y, z \in G$, then we have

$$\begin{aligned} z[x, y]z^{-1} &= zx^{-1}y^{-1}xyz^{-1} \\ &= zx^{-1}z^{-1}zy^{-1}z^{-1}zxz^{-1}zyz^{-1} \\ &= [zxz^{-1}, zyz^{-1}]. \end{aligned}$$

Therefore if $S = \{[x, y] \mid x, y \in G\}$, then $zSz^{-1} \subseteq S$ for all $z \in G$. This implies $z[G, G]z^{-1} \subseteq [G, G]$ for all $z \in G$. Thus $[G, G]$ is a normal subgroup of G.

3. We first note that $\psi([G,G])$ is a nonempty subset of $[G,G]$. Indeed, it is clearly nonempty since $e \in \psi([G,G])$. Also, for any $[x,y] \in [G,G]$, we have

$$\begin{aligned}\psi([x,y]) &= \psi(x^{-1}y^{-1}xy)\\ &= \psi(x)^{-1}\psi(y)^{-1}\psi(x)\psi(y)\\ &= [\psi(x),\psi(y)].\end{aligned}$$

Since $[G,G]$ is generated by all commutators, it follows that $\psi([G,G]) \subseteq [G,G]$. Finally note that if $H \leq G$, then $\psi(H) \leq G$. Indeed, $\psi(H)$ is nonempty since $e \in \psi(H)$, and if $\psi(x),\psi(y) \in \psi(H)$, then $\psi(x)\psi(y)^{-1} = \psi(xy^{-1}) \in \psi(H)$. In particular, $\psi([G,G]) \leq G$, and since $[G,G] \leq G$ and $\psi([G,G]) \subseteq [G,G]$, we see that $\psi([G,G]) \leq [G,G]$.

4. First suppose $\operatorname{im}\varphi$ is abelian. Then for any $x,y \in G$, we have

$$\begin{aligned}\varphi([x,y]) &= \varphi(x^{-1}y^{-1}xy)\\ &= \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y)\\ &= \varphi(x)^{-1}\varphi(x)\varphi(y)^{-1}\varphi(y)\\ &= e,\end{aligned}$$

where we used the fact that $\operatorname{im}\varphi$ is abelian in order to get the third line from the second line. Thus all commutators belong to the kernel of φ, and since $[G,G]$ is generated by all commutators, it follows that $[G,G] \subseteq \ker\varphi$.

Conversely, suppose $[G,G] \subseteq \ker\varphi$. By the first isomorphism theorem, we have $\operatorname{im}\varphi \cong G/\ker\varphi$, so to show $\operatorname{im}\varphi$ is abelian, we just need to show that $G/\ker\varphi$ is abelian. Let $\overline{x},\overline{y} \in G/\ker\varphi$. Then observe that

$$\begin{aligned}\overline{xy} &= \overline{xy[y,x]}\\ &= \overline{xyy^{-1}x^{-1}yx}\\ &= \overline{yx}.\end{aligned}$$

It follows that $G/\ker\varphi$ is abelian.

5. Let $x \in G$ and let $y \in N$. Then note that $(xyx^{-1})y^{-1} = [x^{-1},y^{-1}] \in N$. It follows that $xyx^{-1} \in N$ since $y^{-1} \in N$. Thus N is a normal subgroup of G.

92.2.2 Saturated multiplicative sets

Exercise 65. Let R be a commutative ring with idenitty and let S be a nonempty subset of R. We say that S is **multiplicatively closed** if $s,t \in S$ implies $st \in S$. Additionally, we say that the set S is **saturated** if $st \in S$ implies $s,t \in S$.

1. Let $I \subseteq R$ be an ideal. Show that its complement $S := R\backslash I$ is saturated.

2. Let $I \subseteq R$ be an ideal. Show that its complement $S := R\backslash I$ is multiplicatively closed if and only if R/I is an integral domain.

3. Suppose that S is a multiplicatively closed subset of R that does not contain 0. Show that there is an ideal $\mathfrak{p}$ in R that is maximal with respect to the property that $\mathfrak{p} \cap S = \emptyset$.

4. Suppose that S is a multiplicatively closed subset of R that does not contain 0 and suppose that $\mathfrak{p}$ is maximal with respect to the property that $\mathfrak{p} \cap S = \emptyset$. Show that $\mathfrak{p}$ is necessarily prime.

Solution 59. 1. Suppose $s,t \in R$ and $st \in S$. Assume for a contradiction that $s \notin S$. Then $s \in I$, and since I is an ideal, this implies $st \in I$, which is a contradiction since $st \in S$. Therefore $s \in S$. A similar argument shows that $t \in S$.

2. Suppose S is multiplicatively closed. We will show that I is prime, which will imply R/I is an integral domain. Assume for a contradiction that I is not prime, so there exists $s,t \in R\backslash I$ such that $st \in I$. However this contradicts the fact that $S = R\backslash I$ is multiplicatively closed.

Conversely, suppose R/I is an integral domain, so I is a prime ideal. Assume for a contradiction that S is not multiplicatively closed. Then there exists $s,t \in S$ such that $st \notin S$. In other words, $s,t \notin I$ and $st \in I$. This contradicts the fact that I is a prime ideal.

(3 and 4). We appeal to Zorn's Lemma. We define a partial order $(\mathcal{F}, \subseteq)$ as follows: the underlying set is given by

$$\mathcal{F} = \{I \subseteq R \mid I \text{ is an ideal and } I \cap S = \emptyset\}.$$

The partial order $\subseteq$ is set inclusion. Note that $\mathcal{F}$ is nonempty since $0 \in \mathcal{F}$. Let $(I_\lambda)_{\lambda \in \Lambda}$ be a totally ordered subset of $\mathcal{F}$. We claim that $\bigcup_{\lambda \in \Lambda} I_\lambda$ is an upper bound for $(I_\lambda)_{\lambda \in \Lambda}$. To see this, first we will show that $\bigcup_{\lambda \in \Lambda} I_\lambda$ is an ideal in R. First note that $\bigcup_{\lambda \in \Lambda} I_\lambda$ is nonempty since $0 \in \bigcup_{\lambda \in \Lambda} I_\lambda$. Next, let $a, b \in R$ and let $x, y \in \bigcup_{\lambda \in \Lambda} I_\lambda$. Then $x \in I_\lambda$ and $y \in I_\mu$ for some $\lambda, \mu \in \Lambda$. Without loss of generality, say $\lambda \leq \mu$, thus $x, y \in I_\mu$. Then since I_μ is an ideal, we have $ax + by \in I_\mu \subseteq \bigcup_{\lambda \in \Lambda} I_\lambda$. Thus $\bigcup_{\lambda \in \Lambda} I_\lambda$ is an ideal as claimed. Now we need to show that $\bigcup_{\lambda \in \Lambda} I_\lambda$ has nonempty intersection with S. This is clear though since

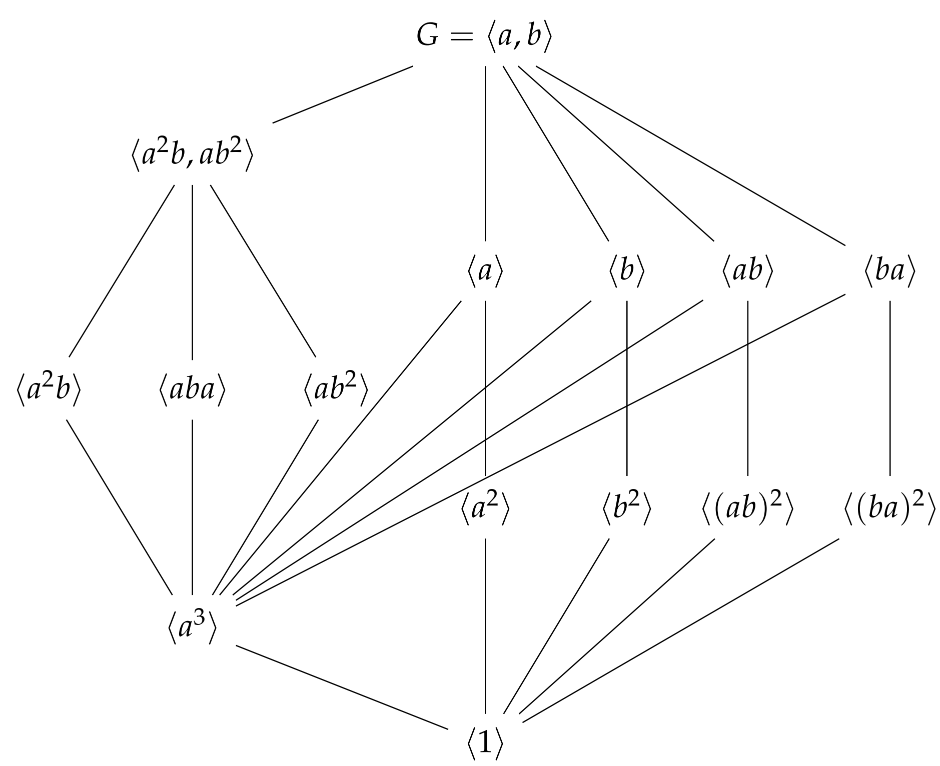
$$\begin{aligned} S \cap \left(\bigcup_{\lambda \in \Lambda} I_\lambda \right) &= \bigcup_{\lambda \in \Lambda} (S \cap I_\lambda) \\ &= \bigcup_{\lambda \in \Lambda} \emptyset \\ &= \emptyset. \end{aligned}$$

So we have shown that every totally ordered subset of $\mathcal{F}$ has an upper bound. We may therefore apply Zorn's Lemma to get an ideal $\mathfrak{p} \subseteq R$ which is maximal which respect to the property that $\mathfrak{p} \cap S = \emptyset$.

We now want to show now that $\mathfrak{p}$ is necessarily a prime ideal. Assume for a contradiction that $\mathfrak{p}$ is not a prime ideal. Then there exists $x, y \in R \backslash \mathfrak{p}$ such that $xy \in \mathfrak{p}$. Since S is multiplicatively closed, we cannot have both $x \in S$ and $y \in S$. Without loss of generality, say $x \notin S$. Then $\mathfrak{p} + \langle x \rangle$ is an ideal which has nonempty intersection with S (since $x \notin S$) and which strictly contains $\mathfrak{p}$. This contradicts maximality of $\mathfrak{p}$.

92.2.3 Lattice of subgroups

Exercise 66. In this problem G refers to the group of order 24 whose subgroup lattice appears below. You must fully justify each answer for full credit.



1. Show that in any group, a subgroup of order 2 is normal if and only if it is contained in the center.
2. Partition the fifteen subgroups into equivalence classes by conjugacy.
3. Is G solvable? Nilpotent?
4. What familiar group is the qoutient $G/\langle a^3 \rangle$ isomorphic to? Justify your answer by drawing its subgroup lattice.
5. What familiar group is the subgroup $\langle a^2b, ab^2 \rangle$ isomorphic to? Justify your answer by drawing its subgroup lattice.
6. What familiar group is the quotient $\langle a^2b, ab^2 \rangle / \langle a^3 \rangle$ isomorphic to? Use the isomorphism theorems to justify your answer.

Solution 60. 1. Let H be any group and let N be a subgroup of H of order 2. If N is contained in the center of H, then it is clear that N is normal in H. Indeed, let $h \in H$ and $n \in N$. Then

$$\begin{aligned} hnh^{-1} &= nhh^{-1} \\ &= n \\ &\in N. \end{aligned}$$

implies N is normal in H. Now suppose N is normal in H. Write $N = \{e, n\}$, where e is the identity, and let $h \in H$. If $hnh^{-1} = e$, then $hn = h$, which implies $n = e$, a contradiction. Thus we must have $hnh^{-1} = n$. This implies N is contained in the center of H.

2. The table below partitions the fifteen subgroups by conjugacy.

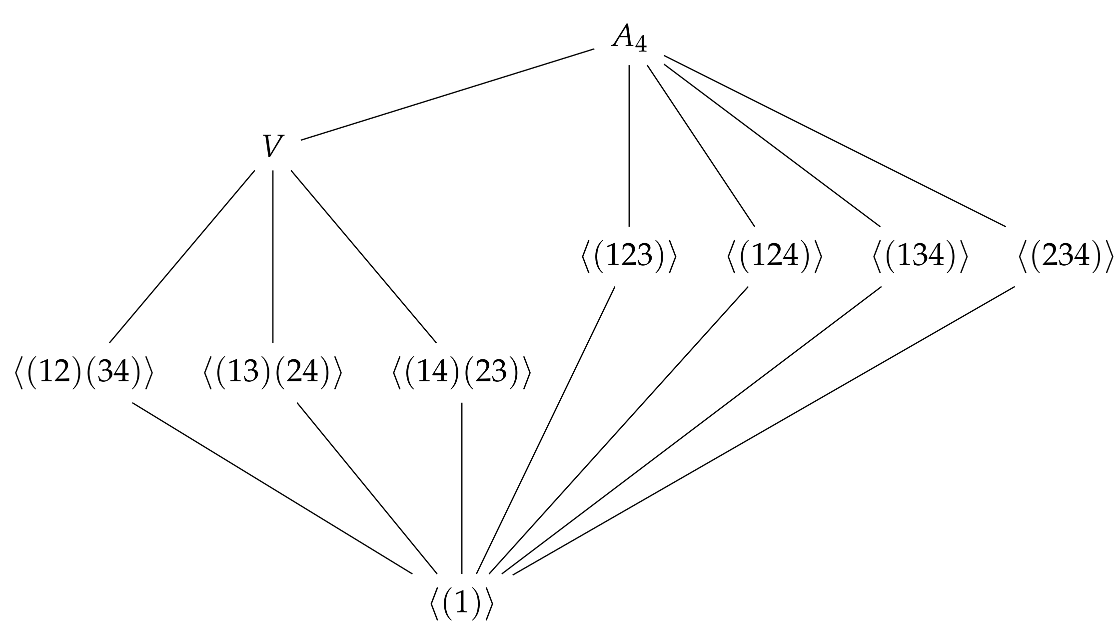
Equivalence Classes of Subgroups by Conjugacy
$\langle a \rangle$, $\langle b \rangle$, $\langle ab \rangle$, $\langle ba \rangle$
$\langle a^2 \rangle$, $\langle b^2 \rangle$, $\langle (ab)^2 \rangle$, $\langle (ba)^2 \rangle$
$\langle a^3 \rangle$
$\langle a^2 b \rangle$, $\langle aba \rangle$, $\langle ab^2 \rangle$
$\langle a^2 b, ab^2 \rangle$
$\langle a, b \rangle$

3. The group G is solvable. A composition series for G is given by

$$\langle 1 \rangle \triangleright \langle a^3 \rangle \triangleright \langle aba \rangle \triangleright \langle a^2 b, ab^2 \rangle \triangleright \langle a, b \rangle \tag{386}$$

with cyclic factors C_2, C_2, C_2, and C_3 respectively. On the other hand, G is *not* nilpotent. Indeed, if it were, then the quotient $G/\langle a^3 \rangle$ must be nilpotent as well. However, we shall see in the next part to this problem that $G/\langle a^3 \rangle \cong A_4$ which is not nilpotent.

4. The quotient group $G/\langle a^3 \rangle$ is isomorphic to A_4. The subgroup lattice of A_4 is given below.

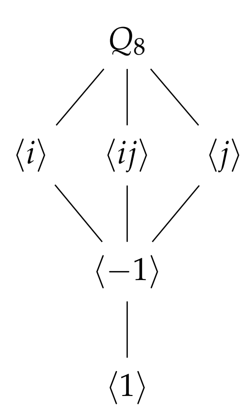


where $V = \langle (12)(34), (14)(23) \rangle$.

5. The group $\langle a^2 b, ab^2 \rangle$ is isomorphic to the quaternion group

$$Q_8 = \langle i, j \mid i^2 = -1, j^2 = -1, ij = -ij \rangle.$$

The subgroup lattice of Q_8 is given below



An isomorphism from $\langle a^2b, ab^2\rangle$ is given by $a^2b \mapsto i$ and $ab^2 \mapsto j$.

6. The group $\langle a^2b, ab^2\rangle / \langle a^3\rangle$ is isomorphic to the Klein four-group K_4. Indeed, we obtain a group homomorphism $\langle a^2b, ab^2\rangle \to K_4$ by the composition

$$\langle a^2b, ab^2\rangle \xrightarrow{\cong} Q_8 \to Q_8/\langle -1\rangle \cong K_4.$$

The kernel of the group homomorphism $\langle a^2b, ab^2\rangle$ is $\langle a^3\rangle$. Thus by the first isomorphism theorem, we have

$$\langle a^2b, ab^2\rangle / \langle a^3\rangle \cong K_4.$$

93 Summer 2019

93.1 Linear Algebra

93.1.1 Integral inner product

Exercise 67. Fix an integer $d \geq 2$ and consider the real vector space

$$V_d = \mathbb{R}[x]_{<d} = \{a_0 + a_1x + \cdots + a_{d-1}x^{d-1} \mid a_0, \ldots, a_{d-1} \in \mathbb{R}\}.$$

For all $f, g \in V_d$, define

$$\langle f, g\rangle = \int_0^1 fg\mathrm{d}x$$

where fg is the usual product of f and g from calculus.

1. Prove that $\langle \cdot, \cdot\rangle$ is an inner product on V_d.
2. In the case $d = 3$, apply Gram-Schmidt process to the ordered basis $(1, x, x^2)$ to find an orthonormal ordered basis for V_3. Then consider the subspace $W = \mathrm{span}_{\mathbb{R}}(1 - 2x)$ and find a basis for $W^{\perp}$.
3. Let $D\colon V_d \to V_d$ be the differentiation operator

$$D(f) = f' = \frac{\mathrm{d}f}{\mathrm{d}x},$$

which is a linear transformation. Find the matrix representing D with respect to the order basis $(1, x, \ldots, x^{d-1})$. Prove or disprove: D is an isomorphism.

4. Prove or disprove: D is diagonalizable.
5. Compute $D^*(a_0 + a_1x + \cdots + a_{d-1}x^{d-1})$ where $D^*\colon V \to V$ is the adjoint of D.

Solution 61. 1. First we show linearity in the first argument when the second argument is fixed. In fact, this follows from linearity of multiplication and linearity of integration: let $a, b \in \mathbb{R}$ and $f, g, h \in V_d$, then

$$\begin{aligned}
\langle af + bg, h\rangle &= \int_0^1 (af + bg)h\mathrm{d}x \\
&= \int_0^1 (afh + bgh)\mathrm{d}x \\
&= a\int_0^1 fh\mathrm{d}x + b\int_0^1 gh\mathrm{d}x \\
&= a\langle f, h\rangle + b\langle g, h\rangle.
\end{aligned}$$

Next we show $\langle \cdot, \cdot\rangle$ is symmetric. This follows from commutativity of multiplication: let $f, g \in V_d$, then

$$\begin{aligned}
\langle f, g\rangle &= \int_0^1 fg\mathrm{d}x \\
&= \int_0^1 gf\mathrm{d}x \\
&= \langle g, f\rangle.
\end{aligned}$$

Finally, we show positive-definiteness of $\langle \cdot, \cdot \rangle$. This follows from the following fact about Lebesgue integration (or more generally integration over any measurable space): if f is any nonnegative Lebesgue measurable function, then $\int_0^1 f \mathrm{d}x = 0$ implies $f = 0$ almost everywhere. In particular, if $f \in V_d$, then

$$0 = \langle f, f \rangle = \int_0^1 f^2 \mathrm{d}x$$

implies $f^2 = 0$ almost everywhere, and since f^2 is just a polynomial, we in fact have $f^2 = 0$ everywhere, thus $f = 0$.

2. We first set $u_1 = 1$. Next we set

$$\begin{aligned} u_2 &= x - \frac{\langle x, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 \\ &= x - \frac{\int_0^1 x \mathrm{d}x}{\int_0^1 \mathrm{d}x} \\ &= x - 1/2. \end{aligned}$$

Finally we set

$$\begin{aligned} u_3 &= x^2 - \frac{\langle x^2, u_2 \rangle}{\langle u_2, u_2 \rangle} u_2 - \frac{\langle x^2, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 \\ &= x^2 - \frac{\int_0^1 x^2 (x - 1/2) \mathrm{d}x}{\int_0^1 (x - 1/2)^2 \mathrm{d}x} (x - 1/2) - \frac{\int_0^1 x^2 \mathrm{d}x}{\int_0^1 \mathrm{d}x} \\ &= x^2 - 1(x - 1/2) - \frac{1}{3} \\ &= x^2 - x + 1/6. \end{aligned}$$

So (u_1, u_2, u_3) is an ordered orthogonal basis. To get an orthonormal basis, we set

$$\begin{aligned} v_1 &= \frac{u_1}{\|u_1\|} \\ &= \frac{1}{\sqrt{\int_0^1 \mathrm{d}x}} \\ &= 1. \end{aligned}$$

Next we set

$$\begin{aligned} v_2 &= \frac{u_2}{\|u_2\|} \\ &= \frac{x - 1/2}{\sqrt{\int_0^1 (x - 1/2)^2 \mathrm{d}x}} \\ &= \sqrt{12}(x - 1/2). \end{aligned}$$

Finally we set

$$\begin{aligned} v_3 &= \frac{u_3}{\|u_3\|} \\ &= \frac{x^2 - x + 1/6}{\sqrt{\int_0^1 (x^2 - x + 1/6)^2 \mathrm{d}x}} \\ &= \sqrt{180}(x^2 - x + 1/6). \end{aligned}$$

So (v_1, v_2, v_3) is an ordered orthonormal basis.

3. For each $0 \leq i \leq d - 1$, we have

$$D(x^i) = i x^{i-1}.$$

Thus the matrix representation of D with respect to the ordered basis $\mathbf{x} = (1, x, \ldots, x^{d-1})$ is given by

$$[D]_{\mathbf{x}} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & d-1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

From this, it's easy to see that $\det D = 0$, which implies D is not an injective (and hence not an isomorphism).

4. The map D cannot be diagonalizable since the only eigenvectors for D are the constant polynomials. Indeed, if f is a nonconstant polynomial of degree i where $1 \leq i \leq d-1$, then $D(f)$ will have degree $i-1$, and thus f cannot be a constant multiple times $D(f)$. So D cannot have an eigenbasis, which means D cannot be diagonalizable.

Alternatively, if we let $\mathbf{x}' = (1, x, x^2/2, \ldots, x^{d-1}/(d-1))$. Then the matrix representation of D with respect to $\mathbf{x}'$ is given by

$$[D]_{\mathbf{x}'} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

This matrix respresentation also gives the Jordan canonical form of D. In particular D is not diagonalizable.

5. Using the fact that $[D^*]_{\mathbf{x}^*} = [D]_{\mathbf{x}}^{\top}$, we have

$$\begin{aligned} [D^*]_{\mathbf{x}^*} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{pmatrix} &= \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \ddots & \vdots \\ 0 & 2 & 0 & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d-1 & 0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ a_0 \\ 2a_1 \\ \vdots \\ (d-1)a_{d-2} \end{pmatrix}. \end{aligned}$$

Therefore

$$D^*(a_0 + a_1 x + \cdots + a_{d-1} x^{d-1}) = a_0 x + 2a_1 x^2 + \cdots + (d-1)a_{d-2} x^{d-1}.$$

93.1.2 Jordan normal form and minimal polynomial of 3×3 matrix over $\mathbb{R}$

Exercise 68. Let $p \in \mathbb{R}$ and let

$$A_p = \begin{pmatrix} 4 & 1 & p \\ 0 & 5 & 1 \\ 0 & 1 & 5 \end{pmatrix}.$$

1. Find the characteristic and the minimal polynomial of A_p.
2. Find the Jordan normal form J of A_p and a matrix S such that $A = SJS^{-1}$.
3. Prove that
$$V[A_p] = \{a_0 I + a_1 A_p + \cdots + a_n A_p^n \mid a_i \in \mathbb{R}, n \in \mathbb{N}\}$$
with the usual matrix addition and scalar multiplication is a vector space over $\mathbb{R}$.
4. Find the dimension and a basis for $V[A_p]$.

Solution 62. 1. The characteristic polynomial of A_p is given by

$$\begin{aligned}\chi_{A_p}(T) &= \det\begin{pmatrix} T-4 & -1 & -p \\ 0 & T-5 & -1 \\ 0 & -1 & T-5\end{pmatrix} \\ &= (T-4)((T-5)^2+1) \\ &= (T-4)^2(T-6).\end{aligned}$$

Since the minimal polynomial divides χ_{A_p} and shares the same roots as χ_{A_p}, we see that the minimal polynomial is either given by

$$\pi_{A_p}(T) = (T-4)(T-6) \quad \text{or} \quad \pi_{A_p}(T) = (T-4)^2(T-6).$$

Let us check for which values of $p \in \mathbb{R}$ do we have $\pi_{A_p}(T) = (T-4)(T-6) = T^2 - 10T + 24$. We calculate

$$\begin{aligned}\begin{pmatrix} 4 & 1 & p \\ 0 & 5 & 1 \\ 0 & 1 & 5\end{pmatrix}^2 - 10\begin{pmatrix} 4 & 1 & p \\ 0 & 5 & 1 \\ 0 & 1 & 5\end{pmatrix} + 24 &= \begin{pmatrix} 16 & 9+p & 1+9p \\ 0 & 26 & 10 \\ 0 & 10 & 26\end{pmatrix} - 10\begin{pmatrix} 4 & 1 & p \\ 0 & 5 & 1 \\ 0 & 1 & 5\end{pmatrix} + 24\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1\end{pmatrix} \\ &= \begin{pmatrix} 16-40+24 & (9+p)-10 & (1+9p)-10p \\ 0 & 26-50+24 & 10-10 \\ 0 & 10-10 & 26-50+24\end{pmatrix} \\ &= \begin{pmatrix} 0 & p-1 & 1-p \\ 0 & 0 & 0 \\ 0 & 0 & 0\end{pmatrix}.\end{aligned}$$

Thus we have

$$\pi_{A_p}(T) = \begin{cases} (T-4)(T-6) & \text{if } p = 1 \\ (T-4)^2(T-6) & \text{else}\end{cases}$$

2. First suppose $p = 1$. In this case, we have

$$\ker(A_1 - 6) = \mathbb{R}\begin{pmatrix} 1 \\ 1 \\ 1\end{pmatrix} \quad \text{and} \quad \ker(A_1 - 4) = \mathbb{R}\begin{pmatrix} 1 \\ 0 \\ 0\end{pmatrix} + \mathbb{R}\begin{pmatrix} 1 \\ 1 \\ -1\end{pmatrix}.$$

Thus

$$J_1 = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4\end{pmatrix} \quad \text{and} \quad S_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & -1\end{pmatrix}.$$

Now suppose $p \neq 1$. In this case, we have

$$\ker(A_p - 6) = \mathbb{R}\begin{pmatrix} 1+p \\ 2 \\ 2\end{pmatrix}, \quad \ker(A_p - 4) = \mathbb{R}\begin{pmatrix} 1-p \\ 0 \\ 0\end{pmatrix}, \quad \text{and} \quad \ker((A_p-4)^2) = \mathbb{R}\begin{pmatrix} 0 \\ 1 \\ -1\end{pmatrix} + \mathbb{R}\begin{pmatrix} 1-p \\ 0 \\ 0\end{pmatrix}.$$

Thus

$$J_p = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4\end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 1+p & 1-p & 0 \\ 2 & 0 & 1 \\ 2 & 0 & -1\end{pmatrix}.$$

3 and 4. Observe that

$$\mathbb{R}[X]/\langle \pi_{A_p}(X)\rangle \cong V[A_p]$$

via the map $\overline{X} \mapsto A_p$. In particular, $\dim V[A_p] = \deg(\pi_{A_p}(X))$. Thus if $p = 1$, then $\dim V[A_p] = 2$ and (I, A_p) is an ordered basis for $V[A_p]$. If $p \neq 1$, then $\dim V[A_p] = 3$ and (I, A_p, A_p^2) is an ordered basis for $V[A_p]$.

93.1.3 Eigenvalues

Solution 63. 2. Assume for a contradiction that x and y do not correspond to the same eigenvalue, say $Tx = \lambda x$ and $Ty = \mu y$ with $\lambda \neq \mu$. Then x and y are linearly independent: suppose $ax + by = 0$ for some $a, b \in K$. Then

$$\begin{aligned} 0 &= T(0) \\ &= T(ax+by) \\ &= \lambda ax + \mu by \\ &= -\lambda by + \mu by \\ &= (\mu - \lambda)by. \end{aligned}$$

Since $\mu \neq \lambda$, we must have $by = 0$, which implies $b = 0$. Thus $ax = 0$, which implies $a = 0$. This shows that x and y are linearly independent.

Now suppose that $T(x+y) = \gamma(x+y)$. Then

$$\begin{aligned} \lambda x + \mu y &= Tx + Ty \\ &= T(x+y) \\ &= \gamma(x+y) \\ &= \gamma x + \gamma y \end{aligned}$$

implies $\lambda = \gamma$ and $\mu = \gamma$ by linear independence of x and y. This is a contradiction. Thus x and y must correspond to the same eigenvalue.

3. Let v be an eigenvector of T corresponding to the eigenvalue λ. Then we have

$$\begin{aligned} \lambda\langle v, v\rangle &= \langle \lambda v, v\rangle \\ &= \langle Tv, v\rangle \\ &= \langle v, Tv\rangle && \text{(self adjointness of } T) \\ &= \langle v, \lambda v\rangle \\ &= \overline{\lambda}\langle v, v\rangle. \end{aligned}$$

Since $v \neq 0$ by definition of being an eigenvector, we must have $\langle v, v\rangle \neq 0$ by positive-definiteness of the inner-product. This implies $\lambda = \overline{\lambda}$, and hence λ is real.

4. Let A be a self-adjoint complex $n \times n$ matrix satisfying $A^3 = 2A + 4I$ and let $\pi_A(X)$ be the minimal polynomial of A over $\mathbb{C}$. Since $X^3 - 2X - 4$ kills A, we see that $\pi_A(X) \mid X^3 - 2X - 4$. Now observe that

$$X^3 - 2X - 4 = (X-2)(X+1-i)(X+1+i).$$

The minimal polynomial of A over $\mathbb{C}$ cannot have complex roots, otherwise A would have complex eigenvalues (which contradicts the fact that A is self-adjoint). So we must have $\pi_A(X) \mid X - 2$, which implies $\pi_A(X) = X - 2$. In particular, A must have the form

$$A = UDU^{-1} = 2I$$

where U is a unitary matrix and where

$$D = \begin{pmatrix} 2 & 0 & \cdots & 0 \\ 0 & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 2 \end{pmatrix}$$

93.2 Abstract Algebra

93.2.1 Orbits, stabilizers, kernels, and fixed points of group action

Exercise 69. Let G be a finite group acting on itself by conjugation. In this problem, you may assume basic results, such as the orbit-stabilizer theorem, or classification of finite abelian groups, provided that you properly state them.

1. Characterize the orbits, stabilizers, kernels, and fixed points of this action. Your answer should be in terms of familiar group-theoretic objects, not just the definitions of these terms.

2. Prove that the size of any conjugacy class divides $|G|$.

3. Show that if G contains an element $x \in G$ that has exactly two conjugates, then G cannot be simple.

4. Prove that if G is a p-group, then its center is non-trivial.

5. Classify all simple p-groups, with proof. You may use the results of the previous parts, even if you could not prove them.

Solution 64. 1. First let us introduce some notation. Let $x \in G$. The orbit of x with respect to the conjugacy action is denoted $\mathrm{Orb}_G(x)$ and is given by

$$\mathrm{Orb}_G(x) = \{yxy^{-1} \mid y \in G\} = \mathrm{K}_x$$

where K_x is the conjugacy class of x. The stabilizer of x with respect to the conjugacy action is denoted $\mathrm{Stab}_G(x)$ and is given by

$$\begin{aligned}\mathrm{Stab}_G(x) &= \{y \in G \mid yxy^{-1} = x\} \\ &= \{y \in G \mid yx = xy\} \\ &= \mathrm{Z}(x),\end{aligned}$$

where $\mathrm{Z}(x)$ is the centralizer of x (the set of all elements in G which commute with x). Note that the conjugacy class of x has the same size as the index of its centralizer:

$$|\mathrm{K}_x| = [G : \mathrm{Z}(x)]. \tag{387}$$

Indeed, we obtain (387) by applying the orbit-stablizer theorem with respect to the conjugacy action. The kernel of the action is denoted $\mathrm{Ker}_G(G)$ and is given by

$$\begin{aligned}\mathrm{Ker}_G(G) &= \{x \in G \mid xyx^{-1} = y \text{ for all } y \in G\} \\ &= \{x \in G \mid xy = yx \text{ for all } y \in G\} \\ &= \mathrm{Z}(G)\end{aligned}$$

where $\mathrm{Z}(G)$ is the center of G (the set of all elements in G which commute with everything). The fixed points of the conjugacy action is denoted $\mathrm{Fix}_G(G)$ and is given by

$$\begin{aligned}\mathrm{Fix}_G(G) &= \{x \in G \mid yxy^{-1} = x \text{ for all } y \in G\} \\ &= \{x \in G \mid yx = xy \text{ for all } y \in G\} \\ &= \mathrm{Z}(G).\end{aligned}$$

2. Any conjugacy class in G has the form K_x for some $x \in G$. The identity (387) implies $|\mathrm{K}_x|$ divides $|G|$.

3. Suppose contains a conjugacy class which has exactly two elements, say K_x. Then $\mathrm{Z}(x)$ has index 2 in G. This implies $\mathrm{Z}(x)$ is normal in G. To see this, consider the more general situation where H is subgroup of G having index 2. We claim that group multiplication in G induces a group structure on G/H. Indeed, write $G/H = \{\overline{e}, \overline{x}\}$ where e is the identity in G and x is an element in G which represents the nontrivial coset (so $x \notin H$). We want to show that multiplication in G gives rise to the multiplication table in G/H given by

$\cdot$	$\overline{e}$	$\overline{x}$
$\overline{e}$	$\overline{e}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{e}$

showing that $G/H \cong \mathbb{Z}/2\mathbb{Z}$. Clearly we have $\overline{ex} = \overline{x} = \overline{xe}$ and $\overline{ee} = \overline{e}$. The only nontrivial multiplication that we need to show is $\overline{x}^2 = \overline{e}$. Assume for a contradiction that $\overline{x}^2 = \overline{x}$. Then $x = x^2y$ for some $y \in H$. This implies $e = xy$ which implies $x = y^{-1}$. However $x \notin H$ which is a contradiction (as H is closed under inverses). Thus G/H inherits a group structure from multiplication in G, and the natural quotient map $\pi\colon G \to G/H$ has H as its kernel. It follows that H is normal.

4. Suppose G is a p-group, say $|G| = p^n$, and assume for a contradiction that $|Z(G)| = 1$. Let $x_1, \dots, x_k$ represent the nontrivial conjugacy classes of G: so $|\mathrm{K}_{x_i}| > 1$ and $\mathrm{K}_{x_i} \cap \mathrm{K}_{x_j}$ for each $1 \leq i < j \leq k$ and

$$G = \mathrm{Z}(G) \cup \mathrm{K}_{x_1} \cup \cdots \cup \mathrm{K}_{x_k}.$$

Then the class equation gives us

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} [G : \mathrm{Z}(x_i)]. \tag{388}$$

Note that $p \mid [G : \mathrm{Z}(x_i)]$ for each $1 \leq i \leq k$. Indeed, $\mathrm{Z}(x_i)$ is a proper subgroup (otherwise x_i would not represent a nontrivial conjugacy class). Its order must divide the order of G by Lagrange's Theorem, thus $|\mathrm{Z}(x_i)| = p^{m_i}$ where for some $m_i < n$. It follows that $[G : \mathrm{Z}(x_i)] = p^{n-m_i}$. With this understood, we now reduce (27) modulo p to get

$$0 \equiv 1 \bmod p,$$

which is a contradiction.

5. Suppose G is a simple p-group. By the previous problem, its center is nontrivial, in particular $\mathrm{Z}(G) \neq \{e\}$. Since the center of a group is always a normal subgroup and since G is simple, it follows that $G = \mathrm{Z}(G)$. Thus G is abelian. Any subgroup of an abelian group is a normal subgroup, so since G is simple abelian, it must contain no subgroups. Cauchy's Theorem tells us that there exists a subgroup of G whose order is p. This subgroup must be G itself. Thus $|G| = p$ which implies $G \cong C_p$ where C_p is the cyclic group of order p.

93.2.2 Isomorphism theorems

Exercise 70. The *First Isomorphism Theorem* holds for a variety of algebraic structures, and it relates the quotient of the domain of a homomorphism to its kernel and image.

1. Prove that the kernel of a group homomorphism is a subgroup and that it is normal.
2. State and prove the First Isomorphism Theorem for groups.
3. Prove that the kernel of a ring homomorphism is a two-sided ideal.
4. State and prove the First Isomorphism Theorem for rings.

Solution 65. (1 and 2). The first isomorphism theorem for groups is stated and proved as follows:

Theorem 93.1. *Let G and H be groups and let $\varphi\colon G \to H$ be a group homomorphism. Then*

1. *The kernel of φ is a normal subgroup of G.*
2. *The image of φ is a subgroup of H and moreover we have the isomorphism $G/\ker\varphi \cong \operatorname{im}\varphi$.*

Proof. 1. First let us check $\ker\varphi$ is a subgroup of G. It is nonempty since $\varphi(e) = e$ implies $e \in \ker\varphi$. Let $g_1, g_2 \in \ker\varphi$. Then observe that

$$\begin{aligned} \varphi(g_1 g_2^{-1}) &= \varphi(g_1)\varphi(g_2)^{-1} \\ &= ee \\ &= e \end{aligned}$$

implies $g_1 g_2^{-1} \in \ker\varphi$. It follows that $\ker\varphi$ is a subgroup of G.

Next, we check that $\ker\varphi$ is a normal subgroup of G. Let $g \in G$ and let $x \in \ker\varphi$. Then observe that

$$\begin{aligned} \varphi(gxg^{-1}) &= \varphi(g)\varphi(x)\varphi(g)^{-1} \\ &= \varphi(g)e\varphi(g)^{-1} \\ &= \varphi(g)\varphi(g)^{-1} \\ &= e \end{aligned}$$

implies $gxg^{-1} \in \ker\varphi$. It follows that $\ker\varphi$ is a normal subgroup of G.

2. First let us check $\operatorname{im}\varphi$ is a subgroup of H. It is nonempty since $\varphi(e) = e$ implies $e \in \operatorname{im}\varphi$. Let $\varphi(g_1), \varphi(g_2) \in \operatorname{im}\varphi$. Then observe that

$$\varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1 g_2^{-1})$$

implies $\varphi(g_1)\varphi(g_2)^{-1} \in \operatorname{im}\varphi$. It follows that $\operatorname{im}\varphi$ is a subgroup of H.

Next, we define $\overline{\varphi}\colon G/\ker\varphi \to \operatorname{im}\varphi$ by

$$\overline{\varphi}(\overline{g}) = \varphi(g) \tag{389}$$

for all $\overline{g} \in G/\ker\varphi$. We need to check that (5) is well-defined. Let gx be another coset representative of $\overline{g}$ (so $\varphi(x) = e$). Then

$$\begin{aligned}\overline{\varphi}(\overline{gx}) &= \varphi(gx) \\ &= \varphi(g)\varphi(x) \\ &= \varphi(g)e \\ &= \varphi(g) \\ &= \overline{\varphi}(\overline{g}).\end{aligned}$$

Thus (5) is well-defined. Now we show $\overline{\varphi}$ gives us an isomorphism from $G/\ker\varphi$ to $\operatorname{im}\varphi$. It is a group homomorphism since if $g_1, g_2 \in G$, then

$$\begin{aligned}\overline{\varphi}(\overline{g}_1\overline{g}_2) &= \varphi(g_1g_2) \\ &= \varphi(g_1)\varphi(g_2) \\ &= \overline{\varphi}(\overline{g}_1)\overline{\varphi}(\overline{g}_2).\end{aligned}$$

It is also surjective since if $\varphi(g) \in \operatorname{im}\varphi$, then $\overline{\varphi}(\overline{g}) = \varphi(g)$. Finally, it is injective since

$$\begin{aligned}\overline{\varphi}(\overline{g}) = e &\implies \varphi(g) = e \\ &\implies g \in \ker\varphi \\ &\implies \overline{g} = e.\end{aligned}$$

Thus $\overline{\varphi}$ is in fact a group isomorphism. □

(3 and 4) The first isomorphism theorem for rings is stated and proved as follows:

Theorem 93.2. *Let R and S be rings and let $\varphi\colon R \to S$ be a ring homomorphism. Then*

1. *The kernel of φ is a two-sided ideal in R.*
2. *The image of φ is a subring of S and moreover we have the ring isomorphism $R/\ker\varphi \cong \operatorname{im}\varphi$.*

Proof. 1. First let us check $\ker\varphi$ is a two-sided ideal in R. First note that $\ker\varphi$ is an additive subgroup of R. Indeed, this follows from the first isomorphism theorem for groups. So to show that $\ker\varphi$ is a two-sided ideal in R, it suffices to show that it is closed under scalar multiplication: let $a \in R$ and let $x \in \ker\varphi$. Then

$$\begin{aligned}\varphi(ax) &= a\varphi(x) \\ &= a \cdot 0 \\ &= 0\end{aligned}$$

implies $ax \in \ker\varphi$. A similar computation shows that $xa \in \ker\varphi$. Thus $\ker\varphi$ is a two-sided ideal in R.

2. First let us check $\operatorname{im}\varphi$ is a subring of S. Again, it follows from the first isomorphism theorem for groups that $\operatorname{im}\varphi$ is an additive subgroup of S. So to show that $\operatorname{im}\varphi$ is a subring of R, it suffices to show that $\operatorname{im}\varphi$ is closed under multiplication in S and shares the same identity: let $\varphi(a), \varphi(b) \in \operatorname{im}\varphi$ where $a, b \in R$. Then since φ is a ring homomorphism, we have

$$\begin{aligned}\varphi(a)\varphi(b) &= \varphi(ab) \\ &\in \operatorname{im}\varphi.\end{aligned}$$

It follows that $\operatorname{im}\varphi$ is closed under multiplication in S. It also shares the same identity as S since ring homomoprhisms by definition maps the multiplicative identity in R to the multiplicative identity in S.

Next, we define $\overline{\varphi}\colon R/\ker\varphi \to \operatorname{im}\varphi$ by

$$\overline{\varphi}(\overline{a}) = \varphi(a) \tag{390}$$

for all $\overline{a} \in R/\ker\varphi$. By the first isomorphism theorem for groups, $\overline{\varphi}$ is a well-defined group isomorphism. To see that $\overline{\varphi}$ is a *ring* isomorphism, it suffices to show that φ respects multiplication and that it maps the multiplicative identity in $R/\ker\varphi$ to the multiplicative identity in $\operatorname{im}\varphi$: let $\overline{a}, \overline{b} \in R/\ker\varphi$. Then

$$\begin{aligned}\overline{\varphi}(\overline{a}\overline{b}) &= \overline{\varphi}(\overline{ab}) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b}).\end{aligned}$$

Also $\overline{\varphi}(\overline{1}) = \varphi(1) = 1$. It follows that $\overline{\varphi}$ gives a ring isomorphism from $R/\ker\varphi$ to $\operatorname{im}\varphi$. □

93.2.3 Euclidean domains and unique factorization domains

Exercise 71. Prove or disprove each of the following:

1. Every Euclidean domain is a principal ideal domain.
2. Every principal ideal domain is a Euclidean domain.
3. Every principal ideal domain is a unique factorization domain.
4. Every unique factorization domain is a principal ideal domain.
5. Every integral domain is a unique factorization domain.

Solution 66. 1. This is true. Let R be a Euclidean domain with respect to the Euclidean function $\mathrm{d}\colon R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ and let $I \subseteq R$ be an ideal. If $I = 0$, then we are done, so assume $I \neq 0$. Choose $x \in I\backslash\{0\}$ such that $\mathrm{d}(x)$ is minimal; that is, if $y \in I$, then $\mathrm{d}(x) \leq \mathrm{d}(y)$. We claim that $I = \langle x \rangle$. Indeed, let $y \in I$. Since R is a Euclidean domain, we have

$$y = qx + r \tag{391}$$

for some $q, r \in R$ where either $r = 0$ or $\mathrm{d}(r) < \mathrm{d}(x)$. Assume for a contradiction that $r \neq 0$, so $\mathrm{d}(r) < \mathrm{d}(x)$. Rewriting (35) as

$$r = y - qx$$

shows us that $r \in I$ since $x, y \in I$. However, this contradicts our choice of x with $\mathrm{d}(x)$ being minimal, since $r \in I$ and $\mathrm{d}(r) < \mathrm{d}(x)$. Therefore $r = 0$, which implies $y \in \langle x \rangle$. Thus $I \subseteq \langle x \rangle$, and since clearly $\langle x \rangle \subseteq I$, we in fact have $I = \langle x \rangle$. So every ideal in R is principal, which means R is a principal ideal domain.

2. This is false. For example, the ring $R = \mathbb{Z}\left[(1+\sqrt{-19})/2\right]$ is a principal ideal domain which is not a Euclidean domain. To see why it is not a Euclidean domain, first note that R is not a field since $\mathbb{Z} \subseteq R$ but $1/2 \notin R$. Therefore to prove R is not Euclidean, we will show that for no nonunit $a \in R$ is R/a represented by 0 and units. First we compute the norm of a typical element $\alpha = x + y(1+\sqrt{-19})/2$:

$$\mathrm{N}(\alpha) = x^2 + xy + 5y^2 = \left(x + \frac{y}{2}\right)^2 + \frac{19y^2}{4}. \tag{392}$$

This norm always takes values ≥ 0 (this is cleary from the second expression) and once $y \neq 0$ we have

$$\begin{aligned} \mathrm{N}(\alpha) &\geq \frac{19y^2}{4} \\ &\geq \frac{19}{4} \\ &> 4. \end{aligned}$$

In particular, the units are solutions to $\mathrm{N}(\alpha) = 1$, which are ± 1:

$$R^\times = \{\pm 1\}.$$

The first few norm values are $0, 1, 4, 5, 7$, and 9. In particular, there is no element of R with norm 2 or 3. This and the fact that $R^\times \cup \{0|$ has size 3 are the key facts we will use.

If R were Euclidean, then there would be a nonunit a in R such that R/a is represented by 0 and units, so 0, 1, and -1. Perhaps $1 \equiv -1 \mod a$, but we definitely have $\pm 1 \not\equiv 0 \mod a$. Thus R/a has size 2 (if $1 \equiv -1 \mod a$) or size 3. We show this can't happen.

If R/a has size 2 then $2 \equiv 0 \mod a$, so $a \mid 2$ in R. Therefore $\mathrm{N}(a) \mid 4$ in $\mathbb{Z}$. There are no elements of R with norm 2, so the only nonunits with norm dividing 4 are elements with norm 4. A check using (36) shows the only such numbers are ± 2. However, $R/\langle 2 \rangle = R/\langle -2 \rangle$ does not have size 2. For instance, 0, 1, and $(1+\sqrt{-19})/2$ are incongruent modulo ± 2: the difference of two of these (different) numbers, divided by two, is never of the form $x + y(1+\sqrt{-19})/2$ for x and y in $\mathbb{Z}$.

Similarly, if $R/\langle a \rangle$ has size 3, then $a \mid 3$ in R, so $\mathrm{N}(a) \mid 9$ in $\mathbb{Z}$. There is no element of R with norm 3, so a must have norm 9 (it doesn't have norm 1 since it is not a unit). The only elements of R with norm 9 are ± 3, so $a = \pm 3$. The ring $R/\langle 3 \rangle - R/\langle -3 \rangle$ does not have size 3: 0, 1, 2, and $(1+\sqrt{-19})/2$ are incongruent modulo ± 3. Since $R^\times \cup \{0\}$ has size 3 and R has no element a such that $R/\langle a \rangle$ has size 2 or 3, R can't be a Euclidean domain.

3. This is true. Let R be a principal ideal domain. Then R is a Noetherian, which means in particular that we can express any nonzero nonunit in R as a product of irreducibles. To see that such a factorization is unique, let a be a nonzero nonunit in R and let

$$p_1 p_2 \cdots p_r = a = q_1 q_2 \cdots q_s$$

be two factorizations of a into irreducibles. By relabeling terms if necessary, we may assume that $r \leq s$. We will prove by induction on $r \geq 1$ that (after reordering terms if necessary) $p_i \sim q_i$ for all $1 \leq i \leq r$, and $q_{r+1} \cdots q_s$ is a unit. In the base case, we have

$$p_1 = q_1 q_2 \cdots q_s.$$

Since R is a principal ideal domain, the irreducible element p_1 is in fact prime. Therefore $p_1 \mid q_j$ for some $1 \leq j \leq s$. Without loss of generality, say $p_1 \mid q_1$, so $q_1 = x_1 p_1$ for some $x_1 \in R$. Then we have

$$0 = p_1(1 - x_1 q_2 \cdots q_s).$$

Since R is a domain and $p_1 \neq 0$, this implies $1 = x_1 q_2 \cdots q_s$. Thus $q_2 \cdots q_s$ is a unit, and hence $p_1 \sim q_1$.

Now assume that $r > 1$ and that we have shown our claim to be true for all $1 \leq r' < r$. Again, p_1 is prime, and again we may assume without loss of generality that $q_1 = x_1 p_1$ for some $x_1 \in R$. Note that x_1 is necessarily a unit since q_1 is irreducible and since p_1 is a nonunit. So we have

$$0 = p_1(p_2 \cdots p_r - x_1 q_2 \cdots q_s).$$

Again, since R is a domain and $p_1 \neq 0$, this implies $p_2 \cdots p_r = x_1 q_2 \cdots q_s$. Now denote $q_2' = x_1 q_2$, so

$$p_2 \cdots p_r = q_2' \cdots q_s.$$

Now we can proceed by induction to conclude that $r = s$ and $p_i \sim q_i$ for all $1 \leq i \leq r$.

4. This is false. The ring $K[X, Y]$ provides a counterexample. Indeed, if R is a unique factorization domain, then $R[X]$ is a unique factorization domain. Let us state this in the form of a proposition and prove it:

Proposition 93.1. *Let R be a unique factorization domain. Then $R[T]$ is a unique factorization domain.*

Proof. Let $a(T)$ be a nonzero nonunit in $R[T]$ and let K be the fraction field of R. First note that $R[T]$ is Noetherian, and thus $a(T)$ has an irreducible factorization. Suppose

$$p_1(T) \cdots p_m(T) = a(T) = q_1(T) \cdots q_n(T)$$

are two irreducible factorizations of $a(T)$ in $R[T]$. By Gauss' Lemma, each $p_i(T)$ and $q_j(T)$ is irreducible in $K[T]$. Since $K[T]$ is a unique factorization domain, we see that $m = n$ and (perhaps after relabeling) $p_i(T) \sim q_i(T)$ in $K[T]$. In particular, $p_i(T) = x_i q_i(T)$ for some $x_i \in K[T]^\times = K^\times$. Note that since $p_i(T), q_i(T) \in R[T]$, we must have $x_i \in R \backslash \{0\}$. Therefore

$$\begin{aligned} 0 &= p_1(T) \cdots p_m(T) - q_1(T) \cdots q_m(T) \\ &= p_1(T) \cdots p_m(T) - x_1 \cdots x_m p_1(T) \cdots p_m(T) \\ &= p_1(T) \cdots p_m(T)(1 - x_1 \cdots x_m) \\ &= a(T)(1 - x_1 \cdots x_m), \end{aligned}$$

and since $a(T) \neq 0$ and $R[T]$ is a domain, this implies $1 = x_1 \cdots x_n$, which implies each x_i is a unit in R. Thus $p_i(T) \sim q_i(T)$ in $R[T]$. □

5. This is false. The ring $\mathbb{Z}[\sqrt{-5}]$ provides a counterexample. In $\mathbb{Z}[\sqrt{-5}]$, we have two irreducible factorizations of 6. Namely

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{393}$$

Note that each factor in (393) is irreducible in $\mathbb{Z}[\sqrt{-5}]$. For instance, assume for a contradiction that $a + b\sqrt{-5}$ and $c + d\sqrt{-5}$ are nonunits in $\mathbb{Z}[\sqrt{-5}]$ such that

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) \tag{394}$$

Taking norms on both sides of (394) gives us

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Since both $a + b\sqrt{-5}$ and $c + d\sqrt{-5}$ are nonunits in $\mathbb{Z}[\sqrt{-5}]$, we must have

$$a^2 + 5b^2 = 2 \quad \text{and} \quad c^2 + 5d^2 = 2.$$

However no such solution exists. Similar arguments shows that each factor in (393) must be irreducible in $\mathbb{Z}[\sqrt{-5}]$.

94 Winter 2019

94.1 Linear Algebra

94.1.1 Parseval frame

Exercise 72. Let V be a finite-dimensional complex inner product space. A set of vectors $\{f_1, \dots, f_m\}$ is called a **Parseval frame** for V if for every v, we have

$$v = \sum_{i=1}^{m} \langle v, f_i \rangle f_i.$$

1. Prove that every orthonormal basis of V is a Parseval frame.
2. Prove that there exists a Parseval frame which is not an orthonormal basis.
3. Prove that every linearly independent Parseval frame is an orthonormal basis.
4. Prove that $\{f_1, \dots, f_m\}$ is a Parseval frame for V if and only if there is a complex inner product space W such that the following is true:

   (a) V is isometrically embedded in W, that is, there is an injective linear map $\phi \colon V \to W$ such that

   $$\langle v_1, v_2 \rangle_V = \langle \phi(v_1), \phi(v_2) \rangle_W$$

   for every $v_1, v_2 \in V$.

   (b) $\phi(f_i) = \mathrm{P}_{\phi(V)} e_i$ for some orthonormal basis $\{e_1, \dots, e_m\}$ of W, where $\mathrm{P}_{\phi(V)}$ is the orthogonal projection onto the subspace $\phi(V)$.

Solution 67. 1. Let $\{v_1, \dots, v_n\}$ be an orthonormal basis for V and let $v \in V$. Then we have

$$v = \sum_{i=1}^{n} a_i v_i \tag{395}$$

where $a_i \in \mathbb{C}$ are unique. Applying $\langle \cdot, v_i \rangle$ to both sides of (395) gives us $a_i = \langle v, v_i \rangle$. Thus $\{v_1, \dots, v_n\}$ is a Parseval frame for V.

2. Consider the case where V is the vector space $\mathbb{C}^2$ with its standard Euclidean inner product. Set

$$\begin{aligned}
v_1 &= \frac{\sqrt{3}}{2} e_1 - \frac{1}{2} e_2 \\
v_2 &= -\frac{\sqrt{3}}{2} e_1 - \frac{1}{2} e_2 \\
v_3 &= e_2.
\end{aligned}$$

A quick calculation shows

$$\begin{aligned}
\langle v, v_1 \rangle v_1 + \langle v, v_2 \rangle v_2 + \langle v, v_3 \rangle &= \frac{3}{2} \langle v, e_2 \rangle e_2 + \frac{3}{2} \langle v, e_1 \rangle e_1 \\
&= \frac{3}{2} \left(\langle v, e_2 \rangle e_2 + \langle v, e_1 \rangle e_1 \right) \\
&= \frac{3}{2} v.
\end{aligned}$$

so $\{v_1, v_2, v_3\}$ almost does the trick. To get a Parseval frame, we just need to rescale: set $w_i = \sqrt{2/3} v_i$ for $i = 1, 2, 3$. Then

$$\begin{aligned}
\langle v, w_1 \rangle w_1 + \langle v, w_2 \rangle w_2 + \langle v, w_3 \rangle w_3 &= \frac{2}{3} \left(\langle v, v_1 \rangle v_1 + \langle v, v_2 \rangle v_2 + \langle v, v_3 \rangle \right) \\
&= \frac{2}{3} \left(\frac{3}{2} v \right) \\
&= v.
\end{aligned}$$

Thus $\{w_1, w_2, w_3\}$ is a Parseval frame.

3. Let $\{v_1, \dots, v_m\}$ be a linearly independent Parseval frame for V. Then it is a basis for V. Indeed, if spans V since it is a Parseval frame for V: if $v \in V$, then

$$v = \sum_{i=1}^{m} \langle v, v_i \rangle v_i.$$

Also it is linearly independent by definition. Thus $\{v_1, \dots, v_m\}$ is a basis for V. To see that it is an orthonormal basis, we must check that $\langle v_j, v_i \rangle = 0$ whenever $i \neq j$ and $\langle v_j, v_j \rangle = 1$. We have this because we can express v_j as

$$v_j = \sum_{i=1}^{m} \langle v_j, v_i \rangle v_i,$$

and by uniqueness of the coefficients, it follows that $\langle v_j, v_i \rangle = 0$ whenever $i \neq j$ and $\langle v_j, v_j \rangle = 1$.

4. To be lexicographically consistent, we will assume that V is an m-dimensional vector space and that $\{f_1, \dots, f_n\}$ is a Parseval frame for V (so $m \leq n$). We may also identify V with $\mathbb{C}^m$ together with its standard Euclidean inner-product space. Let $\{e_1, \dots, e_n\}$ be the standard

Consersely, suppose conditions (a) and (b) are true. Then for every $v \in V$, we have

$$\begin{aligned}
\phi\left(\sum_{i=1}^{m} \langle v, f_i \rangle f_i\right) &= \sum_{i=1}^{m} \langle v, f_i \rangle \phi(f_i) \\
&= \sum_{i=1}^{m} \langle \phi(v), \phi(f_i) \rangle \phi(f_i) \\
&= \sum_{i=1}^{m} \langle \phi(v), \phi(f_i) \rangle \mathrm{P}_{\phi(V)}(e_i) \\
&= \mathrm{P}_{\phi(V)}\left(\sum_{i=1}^{m} \langle \phi(v), \phi(f_i) \rangle e_i\right) \\
&= \\
&=
\end{aligned}$$

94.1.2 Characteristic polynomial and minimal polynomial of matrix over $\mathbb{Q}$

Exercise 73. Let V be a finite-dimensional vector space over $\mathbb{Q}$. Suppose that $A\colon V \to V$ is an invertible linear map such that $A^{-1} = \frac{1}{2}A^2 + A$.

1. Give all possibilities for the minimal and characteristic polynomials of A.
2. Prove that $\dim V$ is a multiple of 3.
3. Give an explicit example of how part (2) can fail if $\mathbb{Q}$ is replaced by $\mathbb{C}$.
4. Still assuming that V is a $\mathbb{C}$-vector space, prove that if $\dim V = 3$, then all such linear maps are similar.
5. Does part (4) still hold over $\mathbb{Q}$? Fully justify your answer.

Solution 68. 1. Let $\chi(t)$ denote the characteristic polynomial of A, let $\pi(t)$ denote the minimal polynomial of A over $\mathbb{Q}$, and let $f(t) = t^3 + 2t^2 - 2$. From the definining equation of A, we see that $f(A) = 0$. It follows that $\pi \mid f$. In other words, we have $f = \pi g$ for some $g \in \mathbb{Q}[t]$. Furthermore, f is irreducible over $\mathbb{Q}$ since it is irreducible over $\mathbb{Z}$ by Eisenstein's criterion at 2. Since both f and π are monic, this forces $g = 1$, so $f = \pi$. Finally, since χ and π share the same irreducible factors over $\mathbb{Q}$ and since π is irreducible over $\mathbb{Q}$, it follows that $\chi = \pi^n$ for some $n \in \mathbb{N}$.

2. The dimension of V is equal to the degree of the characteristic polynomial of A, so

$$\begin{aligned}
\dim V &= \deg \chi \\
&= \deg(\pi^n) \\
&= n \det \pi \\
&= 3n.
\end{aligned}$$

This implies $\dim V$ is a multiple of 3.

3. If $\mathbb{Q}$ is replaced by $\mathbb{C}$, then we may still have $\pi = f$, but it may no longer be the case that $\chi = \pi^n$ for some $n \in \mathbb{N}$. Indeed, assume that the minimal polynomial factors over $\mathbb{C}$ as

$$\pi = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3),$$

where $\alpha_i \neq \alpha_j$ for $i \neq j$ since $\pi'(t) = t(3t + 4)$ has roots $t = 0$ and $t = -4/3$ (so $\pi'(\alpha_i) \neq 0$ for any $i = 1, 2, 3$). Then it is possible that the characteristic polynomial of A has the form

$$\chi = (t - \alpha_1)^2(t - \alpha_2)(t - \alpha_3).$$

Both χ and π share the same irreducible factors over $\mathbb{C}$, so there is no contradiction here. The Jordan canonical form for A in this case is given by the matrix

$$\begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_1 & 0 & 0 \\ 0 & 0 & \alpha_2 & 0 \\ 0 & 0 & 0 & \alpha_3 \end{pmatrix}.$$

So in this case, we see that $\dim V = 4$, which is not a multiple of 3.

4. I don't think we are given enough information here to conclude that all such linear maps are similar. Indeed, the minimal polynomial of A simply needs to divide f. Thus we could have $\pi = t - \alpha$ and $\chi = (t - \alpha)^3$. In this case, the Jordan canonical form for A is

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}.$$

It is easy to check that this matrix satisfies f. If we make the further assumption that $\pi = f$, then since $\deg \chi = \dim V = \deg \pi$, and $\pi \mid \chi$, and π and χ both being monic forces $\pi = f$. In this case, the Jordan canonical form for A is

$$\begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{pmatrix}.$$

5. By part 1, we necessarily have $f = \pi$. Also $\dim V = 3$ implies $\pi = \chi$ by the same reasoning as in part 4. So the rational canonical form of A is

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & -2 \end{pmatrix}.$$

94.2 Abstract Algebra

94.2.1 Torsion subgroup of abelian group

Exercise 74. Let G be an additive abelian group. For each positive integer n, set

$$\Gamma_n(G) = \{g \in G \mid n^m g = 0 \text{ for some positive integer } m\}.$$

Let $\alpha\colon G \to H$ and $\beta\colon H \to K$ be homomorphisms of additive abelian groups.

1. Prove that $\Gamma_n(G)$ is a subgroup of G.
2. Prove that $\alpha(\Gamma_n(G)) \subseteq \Gamma_n(H)$ and that $\Gamma_n(\alpha)\colon \Gamma_n(G) \to \Gamma_n(H)$ defined by

   $$\Gamma_n(\alpha)(g) = \alpha(g)$$

   for all $g \in \Gamma_n(G)$ is a well-defined group homomorphism.
3. Prove that if α is injective, then so is $\Gamma_n(\alpha)$.
4. Prove or disprove that if α is surjective, then so is $\Gamma_n(\alpha)$.
5. Prove that if G is finitely generated, then $\Gamma_n(G)$ is finite.

Solution 69. 1. First note that $\Gamma_n(G)$ is nonempty since $0 \in \Gamma_n(G)$. Now let $g_1, g_2 \in \Gamma_n(G)$ and choose $m_1, m_2 \in \mathbb{Z}$ such that $n^{m_1} g_1 = n^{m_2} g_2 = 0$. Then

$$\begin{aligned} n^{m_1+m_2}(g_1 - g_2) &= n^{m_1+m_2} g_1 - n^{m_1+m_2} g_2 \\ &= n^{m_2}(n^{m_1} g_1) - n^{m_1}(n^{m_2} g_2) \\ &= n^{m_2} \cdot 0 - n^{m_1} \cdot 0 \\ &= 0. \end{aligned}$$

implies $g_1 - g_2 \in \Gamma_n(G)$. It follows that $\Gamma_n(G)$ is a subgroup of G.

2. Let $g \in \Gamma_n(G)$ and choose $m \in \mathbb{Z}$ such that $n^m g = 0$. Then

$$\begin{aligned} n^m \alpha(g) &= \alpha(n^m g) \\ &= \alpha(0) \\ &= 0. \end{aligned}$$

implies $\alpha(g) \in \Gamma_n(H)$. It follows that $\alpha(\Gamma_n(G)) \subseteq \Gamma_n(H)$.

Next we show that $\Gamma_n(\alpha)$ is a well-defined group homomorphism. First note that $\Gamma_n(\alpha)$ lands in $\Gamma_n(H)$ by what we've just shown. It is also a well-defined group homomorphism since it is just the restriction of $\alpha \colon G \to H$ to $\Gamma_n(G)$.

3. This follows from the fact that the restriction of an injective map is injective.

4. This is false. Consider the case where $G = \mathbb{Z}$, $H = \mathbb{Z}/2\mathbb{Z}$, and $n = 2$. Here, we have $\Gamma_2(\mathbb{Z}) = 0$ and $\Gamma_2(\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. Then the natural quotient map $\pi \colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is surjective, but the induced map $\Gamma_n(\pi) \colon 0 \to \mathbb{Z}/2\mathbb{Z}$ clearly cannot be surjective.

5. First note that if G_1 and G_2 are two abelian groups, then we have

$$\Gamma_n(G_1 \oplus G_2) = \Gamma_n(G_1) \oplus \Gamma_n(G_2).$$

Indeed, if $(g_1, g_2) \in \Gamma_n(G_1 \oplus G_2)$, then we choose $m \in \mathbb{Z}$ such that $n^m(g_1, g_2) = 0$. This implies $n^m g_1 = 0$ and $n^m g_2 = 0$ which implies $g_1 \in \Gamma_n(G_1)$ and $g_2 \in \Gamma_n(G_2)$. Conversely, if $g_1 \in \Gamma_n(G_1)$ and $g_2 \in \Gamma_n(G_2)$, then we choose $m_1, m_2 \in \mathbb{Z}$ such that $n^{m_1} g_1 = 0$ and $n^{m_2} g_2 = 0$. This implies

$$\begin{aligned} n^{m_1+m_2}(g_1, g_2) &= (n^{m_2}(n^{m_1} g_1), n^{m_1}(n^{m_2} g_2)) \\ &= (0, 0) \end{aligned}$$

which implies $(g_1, g_2) \in \Gamma_n(G_1 \oplus G_2)$.

Now we can prove 5 easily as follows: by the fundamental theorem of finitely generated abelian groups, G is isomorphic to

$$\mathbb{Z}^r \oplus \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_s}$$

where $q_1, \dots, q_s$ are powers of (not necessarily distinct) prime numbers and $r \in \mathbb{Z}_{\geq 0}$. It follows that

$$\begin{aligned} \Gamma_n(G) &\cong \Gamma_n(\mathbb{Z}^r \oplus \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_s}) \\ &= \Gamma_n(\mathbb{Z}^r) \oplus \Gamma_n(\mathbb{Z}_{q_1}) \oplus \cdots \oplus \Gamma_n(\mathbb{Z}_{q_s}) \\ &= 0 \oplus \Gamma_n(\mathbb{Z}_{q_1}) \oplus \cdots \oplus \Gamma_n(\mathbb{Z}_{q_s}). \end{aligned}$$

In particular, we see that $|\Gamma_n(G)| \leq q_1 \cdots q_s$.

95 Winter 2018

95.0.1 Eigenvalues of a 3×3 real matrix

Exercise 75. Consider the matrix

$$A = \begin{pmatrix} 0 & a & b \\ a & 0 & c \\ b & c & 0 \end{pmatrix} \in \mathbb{R}^{3 \times 3}$$

where $a, b, c > 0$. Let λ_1, λ_2, and λ_3 denote the eigenvalues of A and suppose that $\lambda_1 \leq \lambda_2 \leq \lambda_3$.

1. Prove that $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$.

2. Prove that $\lambda_1, \lambda_2 < 0$ and $\lambda_3 > 0$.

3. Prove that if $v \in \mathbb{R}^3$, then $\langle Av, v\rangle \lambda_3 \leq \langle Av, Av\rangle$.

4. Show that
$$\lambda_3 \leq \frac{(a+b)^2 + (b+c)^2 + (a+c)^2}{2(a+b+c)}.$$

Solution 70. 1. Let λ be an eigenvalue of A and let $\mathbf{v}$ be a corresponding eigenvector. Then we have

$$\begin{aligned}
\lambda \mathbf{v}^\top \mathbf{v} &= (\lambda \mathbf{v})^\top \mathbf{v} \\
&= (A\mathbf{v})^\top \mathbf{v} \\
&= \mathbf{v}^\top A^\top \mathbf{v} \\
&= \mathbf{v}^\top A \mathbf{v} \\
&= \mathbf{v}^\top \lambda \mathbf{v} \\
&= \lambda \mathbf{v}^\top \mathbf{v}
\end{aligned}$$

Any eigenvector v of a symmetric matrix B mustObserve that if v is an eigenvector of

Here, we can appeal to the fact that A is a compact self-adjoint operator with respect to the Euclidean inner-product. Such an operator always has real eigenvalues. However let's prove that $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ in another way. A quick calculation using the Leibniz formula for computing determinants shows that the characteristic polynomial of A is given by

$$(X - \lambda_1)(X - \lambda_2)(X - \lambda_3) = \chi_A(X) = X^3 - (a^2 + b^2 + c^2)X - 2abc. \tag{396}$$

Expanding the product on the left side in (396) and equation coefficients gives us the relations

$$\begin{aligned}
\lambda_1\lambda_2\lambda_3 &= 2abc \\
\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 &= -(a^2 + b^2 + c^2) \\
\lambda_1 + \lambda_2 + \lambda_3 &= 0.
\end{aligned}$$

Since $\lambda_1\lambda_2\lambda_3 = 2abc$ and $a, b, c > 0$ we must have $\lambda_3 > 0$ and either $\lambda_1, \lambda_2 < 0$ or $\lambda_1, \lambda_2 > 0$. Since $\lambda_1 + \lambda_2 + \lambda_3 = 0$ and $\lambda_3 > 0$, we must have $\lambda_1, \lambda_2 < 0$.

95.0.2 Orthogonal projections

Exercise 76. Let V be a real finite-dimensional inner-product space with proper subspaces U and W. Let P_U and P_V be the orthogonal projections onto U and W respectively.

1. For this part of the problem suppose that $V = \mathbb{R}^n$ and $U = \operatorname{span}(u)$ for some vector $u \neq 0$. Prove that the matrix of P_U with respect to the standard basis of V is $uu^\top/(u^\top u)$.

2. Prove that $\operatorname{trace}(\mathrm{P}_U) = \dim U$.

3. Prove that $\ker(\mathrm{P}_W \mathrm{P}_U) = U^\perp \oplus (W^\perp \cap U)$

Solution 71. 1. Let $\mathbf{e} = (e_1, \ldots, e_n)$ denote the standard ordered basis of $\mathbb{R}^n$. Express u in terms of the ordered basis $\mathbf{e}$, say

$$u = \sum_{i=1}^n a_i e_i.$$

For each $1 \leq i \leq n$, we have

$$\begin{aligned}
\mathrm{P}_U(e_i) &= \frac{\langle e_i, u\rangle}{\langle u, u\rangle} u \\
&= \frac{1}{u^\top u} \sum_{j=1}^n a_i a_j e_j
\end{aligned}$$

Thus the entry in the (i, j) component of the matrix representation of P_U with respect to $\mathbf{e}$ is $a_i a_j/(u^\top u)$. This is also the same entry in the (i, j) component of the matrix $uu^\top/(u^\top u)$. Since the matrix representation of P_U

with respect to $\mathbf{e}$ and the matrix $uu^\top/(u^\top u)$ are $n \times n$ matrices with the same entries, it follows that they must be equal.

2. Let $\mathbf{u} = (u_1, \ldots, u_m)$ be an ordered basis for U and let $\mathbf{u}' = (u'_1, \ldots, u'_{m'})$ be an ordered basis for $U^\perp$. Since $V = U \oplus U^\perp$ (we have this decomposition over any inner-product space), we see that $\mathbf{u} \cup \mathbf{u}'$ is an ordered basis for V. Since

$$\mathrm{P}_U(u_i) = u_i \quad \text{and} \quad \mathrm{P}_U(u'_{i'}) = 0$$

for all $1 \leq i \leq m$ and $1 \leq i' \leq m'$, we see that the matrix representation of P_U with respect to $\mathbf{u} \cup \mathbf{u}'$ is given by

$$[\mathrm{P}_U] = \begin{pmatrix} \mathrm{I}_m & 0 \\ 0 & 0 \end{pmatrix}$$

where I_m is the $m \times m$ identity matrix. Clearly we have

$$\mathrm{trace}(\mathrm{P}_U) = m = \dim U.$$

3. Let $v \in \ker(\mathrm{P}_W \mathrm{P}_U)$. Express v in terms of its decomposition in $U^\perp \oplus U$ as

$$v = v - \mathrm{P}_U(v) + \mathrm{P}_U(v),$$

where $v - \mathrm{P}_U(v) \in U^\perp$ and $\mathrm{P}_U(v) \in U$. To show that $v \in U^\perp \oplus (W^\perp \cap U)$, we just need to show that $\mathrm{P}_U(v) \in W^\perp \cap U$ or, more simply, $\mathrm{P}_U(v) \in W^\perp$ (as we already have since $\mathrm{P}_U(v) \in U$). This is clear though since

$$\mathrm{P}_W(\mathrm{P}_U(v)) = 0$$

implies $\mathrm{P}_U(v) \in \ker \mathrm{P}_W = W^\perp$.

Conversely, let $u + v \in U^\perp \oplus (W^\perp \cap U)$, so $u \in U^\perp$ and $v \in W^\perp \cap U$. Then

$$\begin{aligned} \mathrm{P}_W \mathrm{P}_U(u+v) &= \mathrm{P}_W(\mathrm{P}_U(v)) \\ &= \mathrm{P}_W(v) \\ &= 0 \end{aligned}$$

implies $u + v \in \ker \mathrm{P}_W \mathrm{P}_U$.

95.0.3 Rings of the form $R[s]$ where R is a subring of and integral domain S and $s \in S$

Exercise 77. Let S be an integral domain and let R be a subring of S such that $1_S \in R$. Let $s \in S$ be given, and let $R[s]$ denote the intersection of the subrings of S containing R and s.

1. Prove that the set $R[s]$ is the smallest subring of S containing R and s and that $R[s]$ is an integral domain.
2. Prove that
$$R[s] = \{f(s) \in S \mid f(X) \in R[X]\},$$
that is, $R[s]$ is the set of all elements $t \in S$ such that there is a polynomial $f(X) \in R[X]$ such that $t = f(X)$.
3. Prove that there exists a surjective ring homomorphism $\varphi \colon R[X] \to R[s]$ such that $\varphi(r) = r$ for all $r \in R$.
4. Prove that $\ker \varphi$ is a prime ideal of $R[X]$.
5. Prove or give a counterexample to the following statement: $\ker \varphi$ is a maximal ideal of $R[X]$.

Solution 72. 1. We first show that $R[s]$ is a subring of S. First note that $R[s]$ shares the identity in S. Indeed, if A is any subring of S which contains R and s, then $1_S \in A$ (by definition of what it means to be a subring). As A is arbitrary, this implies $1_S \in R[s]$. Now let $a, b \in R[s]$ and let A be a subring of S which contains R and s. Then $a, b \in A$, and since A is a ring, we have $a + b \in A$ and $ab \in A$. Since A is arbitrary, this implies $a + b \in R[s]$ and $ab \in R[s]$. It follows that $R[s]$ is a subring of S which contains R and s.

It is also clearly the *smallest* subring of S which contains R and s. Indeed, $R[s]$ is, by definition, the intersection of all subrings of S which contain R and s. Thus if A is a subring of S which contains R and s, then $R[s] \subseteq A$. Finally, note that $R[s]$ is an integral domain since it inherits this property from S. Indeed, if $a, b \in R[s]$ such that $ab = 0$, then since $a, b \in S$, we see that either $a = 0$ or $b = 0$.

(2 and 3). First we solve part 3. Let $\varphi\colon R[X] \to R[s]$ be the unique R-algebra homorphism a ring homomorphism such that $\varphi(X) = s$. Thus if $f(X) \in R[x]$, then $\varphi(f) = f(s)$. Clearly we have $\varphi(r) = r$ for all $r \in R$. Let us check that this is in fact a ring homomorphism. Let $f(X), g(X) \in R[X]$, say

$$f(X) = \sum_{i=0}^{\infty} a_i X^i \quad \text{and} \quad g(X) = \sum_{j=0}^{\infty} b_j X^j$$

where $a_i, b_j \in R$ and where $a_i, b_j = 0$ for all but finitely many i, j. Then

$$\begin{aligned}
\varphi(fg) &= \varphi\left(\sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k\right) \\
&= \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) s^k \\
&= \left(\sum_{i=0}^{\infty} a_i s^i\right)\left(\sum_{j=0}^{\infty} b_j s^j\right) \\
&= \varphi(f)\varphi(g).
\end{aligned}$$

Similarly

$$\begin{aligned}
\varphi(f+g) &= \varphi\left(\sum_{k=0}^{\infty}(a_k + b_k) X^k\right) \\
&= \sum_{k=0}^{\infty}(a_k + b_k) s^k \\
&= \sum_{k=0}^{\infty} a_k s^k + \sum_{k=0}^{\infty} b_k s^k \\
&= \varphi(f) + \varphi(g).
\end{aligned}$$

Thus φ is a ring homomorphism. We want to show that φ is surjective. Clearly we have

$$\operatorname{im}\varphi = \{f(s) \in S \mid f(X) \in R[X]\},$$

thus we are trying to show $\operatorname{im}\varphi = R[s]$. Note that $\operatorname{im}\varphi$ is a subring of S by the first isomorphism theorem for rings. Furthermore, $\operatorname{im}\varphi$ contains R and s. It follows that $R[s] \subseteq \operatorname{im}\varphi$. For the reverse inclusion, let A be any subring of S which contains R and s. Let $f(X)$ be any polynomial in $R[x]$, say

$$f(X) = \sum_{i=0}^{n} a_i X^i$$

where $a_i \in R$ for all $0 \leq i \leq n$. Then since A is a ring which contains R and s, we must have

$$f(s) = \sum_{i=0}^{n} a_i s^i \in A.$$

In particular, $\operatorname{im}\varphi \subseteq A$. It follows that $\operatorname{im}\varphi \subseteq R[s]$.

4. Combining the first isomorphism theorem for rings with the fact that $\operatorname{im}\varphi = R[s]$, we see that

$$R[s] \cong R[X]/\ker\varphi.$$

Now since $R[s]$ is an integral domain, it follows that $\ker\varphi$ is a prime ideal in $R[X]$.

5. Clearly $\ker\varphi$ need not be a maximal ideal. Indeed, $\ker\varphi$ being a maximal ideal is equivalent to $\operatorname{im}\varphi$ being a field, however this may not happen. For instance, consider the case where $S, R = \mathbb{Z}$ and $s = 1$. Then $\operatorname{im}\varphi = \mathbb{Z}$ is not a field. Thus $\ker\varphi$ is not a maximal ideal.

95.0.4 Groups of order 100

Exercise 78. 1. Show that all groups of order 100 are semi-direct products of their Sylow p-subgroups. You may of course appeal to the Sylow theorems.

2. Explicitly classify the groups of order 100 which have cyclic Sylow p-subgroups as follows. Give a presentation (generators and fundamental relations) of a group from each isomorphism class and argue that your list is complete. Be sure to state any theorems to which you appeal.

3. Give an example of a group of order 100 which has at least one non-cyclic Sylow p-subgroup. Again, give the presentation for your example, and argue that it really does have order 100 and that it has a non-cyclic Sylow p-Subgroup.

Solution 73. 1. Let G be a group of order $100 = 2^2 \cdot 5^2$. Denote n_2 and n_5 to be the number of 2-Sylow subgroups of G and 5-Sylow subgroups of G respectively. The Sylow Theorems tells us that

$$n_5 \equiv 1 \bmod 5 \quad \text{and} \quad n_5 \mid 4.$$

The only possibility here is that $n_5 = 1$. Let P be a 2-Sylow subgroup of G and let Q be the 5-Sylow subgroup. Since $n_5 = 1$, it follows that Q is a normal subgroup of G (conjugating Q results in another 5-Sylow subgroup, which must be Q itself). It follows from the Second Isomorphism Theorem that PQ is a subgroup of G.

We claim that $|PQ| = |G|$ (which forces $PQ = G$). First note that since PQ is a subgroup of G, Lagranges Theorem tells us that $|PQ| \mid |G|$. Similarly since P and Q are both subgroups of PQ, we must have $4 \mid |PQ|$ and $25 \mid |PQ|$. This implies $100 \mid |PQ|$, that is, $|G| \mid |PQ|$. It follows that $|G| = |PQ|$ which implies $G = PQ$.

Finally, note that $P \cap Q = \{e\}$ since $|P|$ and $|Q|$ are relatively prime. Indeed, if $x \in P \cap Q$, then $\operatorname{ord} x$ must divide $\gcd(|P|, |Q|) = 1$. Thus $\operatorname{ord} x = 1$ which implies $x = e$. Therefore G is a semi-direct product of its Sylow p-subgroups.

2. Suppose that G has cyclic Sylow p-subgroups. Again let P be a Sylow 2-subgroup of G and let Q by the Sylow 5-subgroup of G. Suppose $P = \langle x \rangle$ and $Q = \langle y \rangle$. By part 1, G is a semidirect product of P and Q, thus every element in G can be expressed uniquely as $x^i y^j$ where $i \in \mathbb{Z}/4\mathbb{Z}$ and $j \in \mathbb{Z}/25\mathbb{Z}$. Furthermore, if $x^i y^j$ and $x^{i'} y^{j'}$ are two elements in G, then their product is

$$\begin{aligned}
(x^i y^j)(x^{i'} y^{j'}) &= x^i y^j x^{i'} y^{j'} \\
&= x^i (x^{i'} x^{-i'}) y^j x^{i'} y^{j'} \\
&= x^i x^{i'} (x^{-i'} y^j x^{i'}) y^{j'} \\
&= x^i x^{i'} (x^{-i'} y x^{i'})^j y^{j'} \\
&= x^i x^{i'} (y^{k^{i'}})^j y^{j'} \\
&= x^{i+i'} y^{jk^{i'}+j'}
\end{aligned}$$

where $x^{-1} y x = y^k$ where $k \in \mathbb{Z}/25\mathbb{Z}$. To see why the second to the last line holds, observe that

$$\begin{aligned}
x^{-2} y x^2 &= x^{-1}(x^{-1} y x) x \\
&= x^{-1} y^k x \\
&= (x^{-1} y x)^k \\
&= (y^k)^k \\
&= y^{k^2}.
\end{aligned}$$

More generally, we have

$$\begin{aligned}
x^{-1} y x &= y^k \\
x^{-2} y x^2 &= y^{k^2} \\
x^{-3} y x^3 &= y^{k^3}
\end{aligned}$$

Since $\operatorname{ord} x = 4$, we must have $y^{k^4} = y$, which implies $k^4 \equiv 1 \bmod 25$. Thus we see that

$$k \in \{1, 7, 18, 24\}.$$

Therefore we have the following isomorphism classes

$$\begin{aligned} G_1 &= \langle x, y \mid x^4 = e, y^{25} = e, x^{-1}yx = y \rangle \\ G_7 &= \langle x, y \mid x^4 = e, y^{25} = e, x^{-1}yx = y^7 \rangle \\ G_{18} &= \langle x, y \mid x^4 = e, y^{25} = e, x^{-1}yx = y^{18} \rangle \\ G_{24} &= \langle x, y \mid x^4 = e, y^{25} = e, x^{-1}yx = y^{24} \rangle \end{aligned}$$

95.0.5 On $\mathrm{GL}_2(\mathbb{F}_5)$ and $\mathrm{SL}_2(\mathbb{F}_5)$

Exercise 79. Let $G = \mathrm{GL}_2(\mathbb{F}_5)$ and let $H = \mathrm{SL}_2(\mathbb{F}_5)$.

1. Show that G acts on H by conjugation. Prove any assumptions that you make along the way. You may of course assume properties of matrix multiplication and determinants.
2. Compute the stabilizers of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ under the action described above. What is the kernel of this action?

Solution 74. 1. Let $g \in G$ and $h \in H$. Then

$$\begin{aligned} \det(ghg^{-1}) &= \det(g)\det(h)\det(g)^{-1} \\ &= \det(g)\det(g)^{-1}\det(h) \\ &= \det(h) \\ &= 1, \end{aligned}$$

where we used the fact that $\det\colon \mathrm{GL}_2(\mathbb{F}_5) \to \mathbb{F}_5^\times$ is a group homomorphism. It follows that $ghg^{-1} \in H$, and hence H is a normal subgroup of G.

Thus we can define a map $\pi\colon G \times H \to H$, denoted $\pi(g, h) = g \cdot h$, by

$$g \cdot h = ghg^{-1}. \tag{397}$$

for all $g \in G$ and $h \in H$. We claim that π is an action of G on H. To see this, first note that π lands in H since H is a normal in G. Next, let $g_1, g_2 \in G$ and let $h \in H$. Then

$$\begin{aligned} g_1 \cdot (g_2 \cdot h) &= g_1 \cdot (g_2 h g_2^{-1}) \\ &= g_1(g_2 h g_2^{-1})g_1^{-1} \\ &= (g_1 g_2)h(g_1 g_2)^{-1} \\ &= (h_1 h_2) \cdot h. \end{aligned}$$

Also if $e \in G$ is the identity, then

$$\begin{aligned} e \cdot h &= ehe^{-1} \\ &= h. \end{aligned}$$

It follows that π is a group action of G on H.

2. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{F}_5)$. We have

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\iff \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\iff \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\iff \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\iff \begin{pmatrix} a+c & b+d-a-c \\ c & d-c \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\iff c = 0 \text{ and } d = a \end{aligned}$$

Thus

$$\begin{aligned} \mathrm{Stab}_G\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) &= \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_5) \right\} \\ &= \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_5 \right\} \cup \left\{ \begin{pmatrix} 4 & b \\ 0 & 4 \end{pmatrix} \mid b \in \mathbb{F}_5 \right\}. \end{aligned}$$

Similarly, we have

$$\begin{aligned}
\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\iff \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&\iff \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&\iff \begin{pmatrix} -a & -b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&\iff \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&\iff b = -b \text{ and } c = -c \\
&\iff b = c = 0.
\end{aligned}$$

Thus

$$\begin{aligned}
\operatorname{Stab}_G\left(\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right) &= \left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_5)\right\} \\
&= \left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_5^\times\right\}.
\end{aligned}$$

The kernel of π is given by

$$\begin{aligned}
\ker_G(H) &= \left\{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\right\} \\
&= \{g \in G \mid gh = hg \text{ for all } h \in H\}.
\end{aligned}$$

Thus the kernel of π is the set of all elements in G which commute with every element in H. Clearly we have

$$\ker_G(H) \supseteq \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_5\right\}.$$

In fact, we claim that the reverse inclusion holds too. Indeed, let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ and let $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in H$. We have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

if and only if

$$\begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix} = \begin{pmatrix} \alpha a + \beta c & \alpha b + \beta d \\ \gamma a + \delta c & \gamma b + \delta d \end{pmatrix}$$

if and only if

$$\begin{aligned}
b\gamma &= \beta c \\
a\beta + b\delta &= \alpha b + \beta d \\
c\alpha + d\gamma &= \gamma a + \delta c.
\end{aligned}$$

If $\alpha = \beta = \delta = 1$ and $\gamma = 0$, then we must have $c = 0$ and $a = d$. Similarly if $\alpha = \gamma = \delta = 1$ and $\beta = 0$, then we must have $b = 0$. It follows that any element in G which commute with all elements in H must have the form $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ for some $a \in \mathbb{F}_5$. Thus

$$\ker_G(H) = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_5\right\}.$$

96 Summer 2018

96.1 Abstract Algebra

96.1.1 The symmetric group on p elements

Exercise 80. Let p be a positive prime integer. We consider S_p, the symmetric group on p elements.

1. How many elements of order p are there in S_p?

2. How many subgroups of order p are there?

3. What do the Sylow Theorems tell us about the possibilities for the number of p-Sylow subgroups of S_p?

4. For what value(s) of p is the p-Sylow subgroup of S_p a normal subgroup of S_p?

5. Wilson's Theorem implies that if p is a prime, then

$$(p-1)! \equiv -1 \mod p.$$

Use the previous results to prove this statement.

Solution 75. 1. An element σ in S_p has order p if and only if it is a cycle of length p. Thus we are counting the number of all p-cycles in S_p. Let X be the set of all p-cycles in S_p. Then S_p gives rise to an group action on X by conjugation: if $\sigma \in S_p$ and $(a_1 a_2 \cdots a_p) \in X$, then

$$\sigma(a_1 a_2 \cdots a_p)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_p)).$$

Note that the orbit of $(12\cdots p)$ under this action is all of X. Indeed, let $(a_1 a_2 \cdots a_p) \in X$ and let $\sigma = (1a_1)(2a_2)\cdots(pa_p)$. Then we have

$$\sigma(12\cdots p)\sigma^{-1} = (a_1 a_2 \cdots a_p).$$

Furthermore, we have $\sigma(12\cdots p)\sigma^{-1} = (12\cdots p)$ if and only if $\sigma = (12\cdots p)^k$ for some $1 \leq k \leq p$. Thus

$$\mathrm{Fix}_{S_p}((12\cdots p)) = \langle(12\cdots p)\rangle.$$

It follows from the orbit-stabilizer theorem that

$$\begin{aligned}
|X| &= |\mathrm{Orb}_{S_p}((12\cdots p))| \\
&= |S_p|/|\mathrm{Fix}_{S_p}((12\cdots p))| \\
&= p!/p \\
&= (p-1)!.
\end{aligned}$$

2. Let n denote the number of p-subgroups of S_p and let $H_1, \dots, H_n$ denote the p-subgroups of S_p. Any group of order p is a cyclic group. In particular, each H_i consists of the identity element together with $p-1$ different p-cycles. Furthemore, for $i \neq j$, we have $H_i \cap H_j = \{1\}$. Thus we have

$$\begin{aligned}
(p-1)! &= |(H_1 \backslash \{1\} \cup \cdots \cup H_n \backslash \{1\}| \\
&= |(H_1 \backslash \{1\}| + \cdots + |H_n \backslash \{1\}| \\
&= n(p-1).
\end{aligned}$$

Therefore $n = (p-2)!$.

3. Let n_p denote number of p-Sylow subgroups of S_p. Observe that $|S_p| = p! = p(p-1)!$. Since $p \nmid (p-1)!$, it follows that the order of any p-Sylow subgroup of S_p is p. Thus the p-Sylows subgroups of S_p are precisely the p-subgroups. By the previous problem, we have $n_p = (p-2)!$. Now the Sylow Theorems tells us that

$$n_p \equiv 1 \mod p \qquad \text{and} \qquad n_p \mid (p-1)!.$$

4. Suppose S_p has a normal p-Sylow subgroup. Then necessarily we have $n_p = 1$. Since $n_p = (p-2)!$ (as counted above), this implies $p = 2$ or $p = 3$.

5. Combining the previous results, we have

$$(p-2)! = n_p \equiv 1 \mod p. \tag{398}$$

Multiplying both sides of (398) by $p-1$ gives us the desired result.

96.1.2 Every finitely generated non-trivial subgroup of $\mathbb{Q}$ is isomorphic to $\mathbb{Z}$

Exercise 81. Consider the ordinary integers $\mathbb{Z}$.

1. Show that every subgroup of $\mathbb{Z}$ is cyclic.

2. Show that every homomorphic image of $\mathbb{Z}$ is cyclic.

3. Use the previous to show that $\mathbb{Z}$ is a principal ideal domain.

4. Show that in a principal ideal domain, any two nonzero elements a and b have a greatest common divisor that is a linear combination of a and b.

5. Use the previous to show that every finitely generated, nonidentity subgroup of $\mathbb{Q}$ is isomorphic to $\mathbb{Z}$.

Solution 76. 1. Let A be a subgroup of $\mathbb{Z}$. Choose $a \in A\backslash\{0\}$ such that $|a|$ is minimal; that is, $b \in A\backslash\{0\}$ implies $|a| \leq |b|$. We claim that $A = \langle a \rangle$. Indeed, let $b \in A$. Since $\mathbb{Z}$ is a Euclidean domain, there exists $r, n \in \mathbb{Z}$ such that

$$b = na + r$$

where either $r = 0$ or $0 < |r| < |a|$. We claim that $r = 0$ (which will imply $b \in \langle a \rangle$). To see this, assume for a contradiction that $r \neq 0$, so $r < a$. Then note that $r = b - na$ implies $r \in A$. However this contradicts our choice of $a \in A$ with $|a|$ being minimal. Thus we must have $r = 0$, which implies $b \in \langle a \rangle$.

2. Let A be an abelian group and let $\varphi \colon \mathbb{Z} \to A$ be a surjective homomorphism. We claim that $A = \langle \varphi(1) \rangle$. Indeed, let $a \in A$. Choose $n \in \mathbb{Z}$ such that $\varphi(n) = a$ (we can do this since φ is surjective). Then we have

$$a = \varphi(n) = n\varphi(1).$$

Thus $A = \langle \varphi(1) \rangle$.

3. Let I be a subgroup of $\mathbb{Z}$. By 1, we know that every subgroup of $\mathbb{Z}$ is cyclic. In particular, I is cyclic. Thus I is generated by one element, which implies $\mathbb{Z}$ is a principal ideal domain. More generally, any Euclidean domain is a principal ideal domain.

4. Let R be a principal ideal domain and let $a, b \in R\backslash\{0\}$. Since R is a principal ideal domain, there exists a $d \in R$ such that

$$\langle a, b \rangle = \langle d \rangle. \tag{399}$$

Since $d \in \langle a, b \rangle$, there exists $x, y \in R$ such that

$$ax + by = d \tag{400}$$

Since $a, b \in \langle d \rangle$, there exists $\widetilde{a}, \widetilde{b} \in R$ such that

$$d\widetilde{a} = a \quad \text{and} \quad d\widetilde{b} = b$$

In particular, $d \mid a$ and $d \mid b$. Now suppose $d' \in R$ such that $d' \mid a$ and $d' \mid b$, say

$$d'a' = a \quad \text{and} \quad d'a' = b$$

where $a', b' \in R$. Then by (400), we have

$$\begin{aligned} d &= ax + by \\ &= d'a'x + d'b'y \\ &= d'(a'x + b'y). \end{aligned}$$

In particular, $d' \mid d$. Thus d is a greatest common divisor, and (400) shows that it is a linear combination of a and b.

5. Let A be a finitely generated, nonidentity subgroup of $\mathbb{Q}$. . Choose $b \in \mathbb{Z}$ such that $bA \subseteq \mathbb{Z}$. Then bA is a subgroup of $\mathbb{Z}$, and thus in particular, is it generated by one element, say $bA = \langle a \rangle$. It follows that $A = \langle a/b \rangle$.

97 Winter 2017

97.0.1 Linear functionals on $F^{n\times n}$

Exercise 82. Let F be a field, let $F^{n\times n}$ be the vector space of $n \times n$ matrices over F and let $\{E_{ij} \mid 1 \le i, j \le n\}$ be a basis of $F^{n\times n}$ consisting of matrices with an entry 1 in row i and column j and zero otherwise.

1. Show that the trace function $\mathrm{Tr}\colon F^{n\times n} \to F$ is a linear functional such that

$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$$

   for all $A, B \in F^{n\times n}$.

2. Let $f\colon F^{n\times n} \to F$ be a linear functional such that

$$f(AB) = f(BA)$$

   for all $A, B \in F^{n\times n}$. Prove that

   (a) $f(E_{ij}) = 0$ for $1 \le i < j \le n$ and

   (b) $f(E_{ii}) = f(E_{11})$ for all $1 \le i \le n$.

3. Let $f\colon F^{n\times n} \to F$ be a linear functional. Prove that the following conditions on f are equivalent:

   (a) $f(AB) = f(BA)$ for every $A, B \in F^{n\times n}$.

   (b) There is $a \in F$ such that $f(C) = a\mathrm{Tr}(C)$ for all $C \in F^{n\times n}$.

Solution 77. 1. Let $A, B \in F^{n\times n}$ and let $a, b \in F$. Express A and B in matrix notation as

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}.$$

Then we have

$$\begin{aligned}
\mathrm{Tr}(aA + bB) &= \mathrm{Tr}\left(a \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} + b \begin{pmatrix} b_{11} & \cdots & b_{n1} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \right) \\
&= \mathrm{Tr} \begin{pmatrix} aa_{11} + bb_{11} & \cdots & aa_{1n} + bb_{1n} \\ \vdots & \ddots & \vdots \\ aa_{n1} + bb_{n1} & \cdots & aa_{nn} + bb_{nn} \end{pmatrix} \\
&= \sum_{i=1}^{n} aa_{ii} + bb_{ii} \\
&= a \sum_{i=1}^{n} a_{ii} + b \sum_{i=1}^{n} b_{ii} \\
&= a\mathrm{Tr}(A) + b\mathrm{Tr}(B).
\end{aligned}$$

It follows that Tr is a linear functional. Also, we have

$$\begin{aligned}
\operatorname{Tr}(AB) &= \operatorname{Tr}\left(\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}\right) \\
&= \operatorname{Tr}\begin{pmatrix} \sum_{i=1}^n a_{1i}b_{i1} & \cdots & \sum_{i=1}^n a_{1i}b_{in} \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n a_{ni}b_{i1} & \cdots & \sum_{i=1}^n a_{ni}b_{in} \end{pmatrix} \\
&= \sum_{j=1}^n \sum_{i=1}^n a_{ji}b_{ij} \\
&= \sum_{j=1}^n \sum_{i=1}^n b_{ij}a_{ji} \\
&= \operatorname{Tr}\begin{pmatrix} \sum_{j=1}^n b_{1j}a_{j1} & \cdots & \sum_{i=1}^n b_{1j}a_{jn} \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n b_{nj}a_{j1} & \cdots & \sum_{i=1}^n b_{nj}a_{jn} \end{pmatrix} \\
&= \operatorname{Tr}\left(\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\right) \\
&= \operatorname{Tr}(AB)
\end{aligned}$$

2. Let $1 \leq i < j \leq n$. We have

$$\begin{aligned}
f(E_{ij}) &= f(E_{ii}E_{ij}) \\
&= f(E_{ij}E_{ii}) \\
&= f(0) \\
&= 0.
\end{aligned}$$

Similarly, let $1 \leq i \leq n$. We have

$$\begin{aligned}
f(E_{ii}) &= f(E_{i1}E_{1i}) \\
&= f(E_{1i}E_{i1}) \\
&= f(E_{11}).
\end{aligned}$$

3. First suppose that $f(AB) = f(BA)$ for every $A, B \in F^{n\times n}$. Let $C = (c_{ij}) \in F^{n\times n}$. We have

$$\begin{aligned}
f(C) &= f\left(\sum_{1\leq i,j\leq n} c_{ij}E_{ij}\right) \\
&= \sum_{1\leq i,j\leq n} c_{ij}f(E_{ij}) \\
&= \sum_{1\leq i\leq n} c_{ii}f(E_{ii}) + \sum_{1\leq i<j\leq n} c_{ij}f(E_{ij}) \\
&= \sum_{1\leq i\leq n} c_{ii}f(E_{ii}) \\
&= \sum_{1\leq i\leq n} c_{ii}f(E_{11}) \\
&= f(E_{11})\operatorname{Tr}(C).
\end{aligned}$$

Thus, setting $a = f(E_{11})$, we see that $f(C) = a\operatorname{Tr}(C)$ for all $C \in F^{n\times n}$.

Conversely, suppose $f(C) = a\operatorname{Tr}(C)$ for all $C \in F^{n\times n}$ for some $a \in F$. Let $A, B \in F^{n\times n}$. Then

$$\begin{aligned}
f(AB) &= a\operatorname{Tr}(AB) \\
&= a\operatorname{Tr}(BA) \\
&= f(BA).
\end{aligned}$$

Thus $f(AB) = f(BA)$ for all $A, B \in F^{n\times n}$.

97.0.2 Sylow subgroups of group of order 72

Exercise 83. Let G be a group of order 72, let P_2 be a Sylow 2-subgroup of G, and let P_3 be a Sylow 3-subgroup of G.

1. Prove that G is not simple.
2. Describe all abelian groups of order 72 up to isomorphism.
3. Describe all possibilities for P_3 up to isomorphism.
4. Assume that P_2 and P_3 are cyclic, and describe all possibilities for G up to isomorphism in the following cases
   (a) P_2 is a normal subgroup of G;
   (b) P_3 is a normal subgroup of G.

Solution 78. 1. Let n_p denote the number of p-Sylow subgroups of G. Note that $72 = 2^3 \cdot 3^2$, so by the Sylow theorems, we have

$$n_2 \equiv 1 \bmod 2 \quad \text{and} \quad n_2 \mid 9.$$

Similarly, we have

$$n_3 \equiv 1 \bmod 3 \quad \text{and} \quad n_3 \mid 8.$$

It follows that $n_2 \in \{1, 3, 9\}$ and $n_3 \in \{1, 4\}$. If $n_3 = 1$, then P_3 is a normal subgroup of G, so assume $n_3 = 4$. Let X_3 denote the set of 3-Sylow subgroups of G and define $\pi\colon G \to \mathrm{Sym}(X_3) \cong S_4$ by $g \mapsto \pi_g$ where

$$\pi_g(P) = gPg^{-1}$$

for all $P \in X_3$. Denote $K = \ker \pi$. Then G/K embeds into S_4, which implies $[G : K] \mid 24$, which implies $3 \mid |K|$. It follows that K is a nontrivial normal subgroup of G.

2. By the fundamental theorem of finite abelian groups, every abelian group of order 72 is isomorphic to one of the groups listed below:

$$C_2^3 \times C_3^2$$
$$C_2^3 \times C_9$$

$$C_2 \times C_3^2 \times C_4$$
$$C_2 \times C_4 \times C_9$$
$$C_8 \times C_3^2$$
$$C_8 \times C_9$$

3.

97.0.3 Finite multiplicative group of 2×2 integer matrices

Exercise 84. Let G be a finite multiplicative group of 2×2 integer matrices.

1. Given $A \in G$, what can one prove about:
   (a) $\det A$ and $\operatorname{tr} A$?
   (b) the characteristic polynomial of A?
   (c) the eigenvalues of A? (Hint: don't forget to consider the non-real cases).
   (d) the Jordan canonical form of A?
   (e) the order of A?
2. Is A necessarily diagonalizable? Why or why not?
3. Find all possible groups G up to isomorphism.

Solution 79. 1. First we note that G is a finite subgroup of $\mathrm{GL}_2(\mathbb{Q})$. In particular, if $C \in \mathrm{GL}_2(\mathbb{Q})$, then

$$CGC^{-1} = \left\{ CAC^{-1} \mid A \in G \right\}$$

is a conjugate subgroup of $\mathrm{GL}_2(\mathbb{Q})$, which itself is isomorphic to G. Furthermore, the characteristic polynomial of A, the determinant of A, the eigenvalues of A, the trace of A, and the order of A are invariant under conjugation.

Now let $\pi_A(X)$ denote the minimal polynomial of A over $\mathbb{C}$ and let $\chi_A(X)$ denote the characteristic polynomial of A. Since A satisfies $A^n - I = 0$, it follows that $\pi_A \mid X^n - 1$. The irreducible factors of $X^n - 1$ are the cyclotomic polynomials $\Phi_d(X)$ where $d \mid n$. Since π_A is not a unit, it follows that the irreducible factoriation of π_A consists of Φ_d for some of the d's which divide n. In particular, since $\pi_A \mid \chi_A$, we have $\deg \pi_A \leq 2$. The cyclotomic polynomials with degree ≤ 2 are given below

$$\begin{aligned}
\Phi_1(X) &= X - 1 \\
\Phi_2(X) &= X + 1 \\
\Phi_3(X) &= X^2 + X + 1 \\
\Phi_4(X) &= X^2 + 1 \\
\Phi_6(X) &= X^2 - X + 1.
\end{aligned}$$

In the the table below, we describe all possible cases for π_A together with the relevant data such as the rational canonical form of A, denoted A_{rat}, and the Jordan canonical form of A, denoted A_{jor}. After the table, we will also describe why the remaining cases for π_A do not work.

π_A	χ_A	$\det A$	$\operatorname{tr} A$	eigenvalues	$\operatorname{ord} A$	A_{rat}	A_{jor}
$X-1$	$(X-1)^2$	1	2	1	1	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$
$X+1$	$(X+1)^2$	1	-2	-1	2	$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$	$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$
$(X-1)(X+1)$	$(X-1)(X+1)$	-1	0	$1,-1$	2	$\begin{pmatrix}1&0\\0&-1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&-1\end{pmatrix}$
X^2+X+1	X^2+X+1	1	-1	ζ_3, ζ_3^2	3	$\begin{pmatrix}0&-1\\1&-1\end{pmatrix}$	$\begin{pmatrix}\zeta_3&0\\0&\zeta_3^2\end{pmatrix}$
X^2+1	X^2+1	1	0	$i,-i$	4	$\begin{pmatrix}0&-1\\1&0\end{pmatrix}$	$\begin{pmatrix}i&0\\0&-i\end{pmatrix}$
X^2-X+1	X^2-X+1	1	1	ζ_6, ζ_6^5	6	$\begin{pmatrix}0&-1\\1&1\end{pmatrix}$	$\begin{pmatrix}\zeta_6&0\\0&\zeta_6^5\end{pmatrix}$

Note that $\pi_A \neq (X-1)^2$, since in this case

$$A_{\mathrm{jor}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

which has infinite order. Similarly, $\pi_A \neq (X+1)^2$, since in this case A has the form

$$A_{\mathrm{jor}} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$$

which again has infinite order. Finally, note that in each case in the table above, A_{rat} has integer entries. Thus there is always a multiplicative group of 2×2 entries have A_{rat} as one of its elements, namely the cyclic group generated by A_{rat}. Thus all possibilities listed in the table above are realized.

Now let N denote the kernel of the determinant map (which is a homomorphism). So we have the following short exact sequence of groups

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\det} \{\pm 1\} \longrightarrow 1 \tag{401}$$

To understand G, we first describe N. First note that N is a multiplicative subgroup of $\mathrm{SL}_2(\mathbb{Z})$. In particular, there is a natural homomorphism $\varphi \colon N \to \mathrm{SL}_2(\mathbb{F}_3)$ given by reducing matrix entries mod 3. We claim that φ is injective. Indeed, let $A \in \ker \varphi$. To show that A is identity matrix, we just need to show that $\operatorname{tr} A = 2$. Indeed, we already know that $\det A = 1$ since $A \in N$, and the identity matrix is the only matrix of with finite order in $\mathrm{GL}_2(\mathbb{Z})$ which has determinant 1 and trace 2. Now since $A \in \ker \varphi$, it must have the form

$$A = \begin{pmatrix} 1 + 3a & 3b \\ 3c & 1 + 3d \end{pmatrix}$$

where $a, b, c, d \in \mathbb{Z}$. Since $\det A = 1$, we must have

$$\begin{aligned} 1 &= (1+3a)(1+3d) - 9bc \\ &= 1 + 3d + 3a + 9ad - 9bc \\ &= 1 + 3(a+d) + 9(ad - bc), \end{aligned}$$

which implies $a + d = 3(bc - ad)$. Therefore

$$\begin{aligned} \operatorname{tr} A &= 2 + 3(a+d) \\ &= 2 + 9(bc - ad). \end{aligned}$$

In other words, $\operatorname{tr} A \equiv 2 \bmod 9$. Since the only possibilities for $\operatorname{tr} A$ are $\{-2, -1, 0, 1, 2\}$, it follows that $\operatorname{tr} A = 2$, hence φ is injective.

In particular, N is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$.

98 Winter 2016

98.0.1 Product of vector spaces

Exercise 85. Let V be a finite-dimensional real vector space. Let W_1 and W_2 be subspaces of V. We defined the following operations

$$(w_1, w_2) + (w_1', w_2') := (w_1 + w_1', w_2 + w_2') \quad \text{and} \quad \alpha(w_1, w_2) := (\alpha w_1, \alpha w_2)$$

for all $\alpha \in \mathbb{R}$, $w_1 \in W_1$, and $w_2 \in W_2$. The set $W_1 \times W_2$ is a vector space with respect to these operations.

1. Let $U = \{(u, -u) \mid u \in W_1 \cap W_2\}$. Prove that U is a subspace of $W_1 \times W_2$ isomorphic to $W_1 \cap W_2$.
2. Define the map $T\colon W_1 \times W_2 \to W_1 + W_2$ by $T(w_1, w_2) = w_1 + w_2$. Prove that T is a linear transformation.
3. Use the above to prove that
$$\dim(W_1 + W_2) + \dim(W_1 \cap W_2) = \dim W_1 + \dim W_2.$$

Solution 80. 1. We first show U is a subspace of $W_1 \times W_2$. It is nonempty since $(0,0) \in U$. Let $\alpha, \alpha' \in \mathbb{R}$ and let $(u, -u), (u', -u') \in U$. Then observe that

$$\begin{aligned} \alpha(u, -u) + \alpha'(u', -u') &= (\alpha u + \alpha' u', -\alpha u - \alpha' u') \\ &= (\alpha u + \alpha' u', -(\alpha u + \alpha' u')) \\ &\in U, \end{aligned}$$

where the last part follows from the fact that $\alpha u + \alpha' u' \in W_1 \cap W_2$ since $W_1 \cap W_2$ is a subspace of V. It follows that U is a subspace of $W_1 \times W_2$. Let us now show that it is isomorphic to $W_1 \cap W_2$. Define $\varphi\colon U \to W_1 \cap W_2$ by

$$\varphi(u, -u) = u$$

for all $(u, -u) \in U$. Clearly φ is a bijection and a linear map, hence it is an isomorphism.

2. Let $\alpha, \alpha' \in \mathbb{R}$ and let $(w_1, w_2), (w_1', w_2') \in W_1 \times W_2$. Then we have

$$\begin{aligned} T(\alpha(w_1, w_2) + \alpha'(w_1', w_2')) &= T((\alpha w_1 + \alpha' w_1', \alpha w_2 + \alpha' w_2')) \\ &= \alpha w_1 + \alpha' w_1' + \alpha w_2 + \alpha' w_2' \\ &= \alpha(w_1 + w_2) + \alpha'(w_1' + w_2') \\ &= \alpha T(w_1, w_2) + \alpha' T(w_1', w_2'). \end{aligned}$$

It follows that T is a linear map.

3. First note that $\ker T = U$. Indeed, we have

$$\begin{aligned} T(w_1, w_2) = 0 &\iff w_1 + w_2 = 0 \\ &\iff w_1 = -w_2 \\ &\iff (w_1, w_2) \in U. \end{aligned}$$

Next we note that $\operatorname{im} T = W_1 + W_2$. Thus by the rank nullity theorem, we have

$$\begin{aligned} \dim W_1 + \dim W_2 &= \dim(W_1 \times W_2) \\ &= \dim(\ker T) + \dim(\operatorname{im} T) \\ &= \dim U + \dim(W_1 + W_2) \\ &= \dim(W_1 \cap W_2) + \dim(W_1 + W_2). \end{aligned}$$

98.0.2 Two real symmetric matrices commute if and only if they are diagonalizable in common orthonormal basis

Exercise 86. Let A and B be two real symmetric matrices. Show that they commute if and only if they are diagonalizable in a common orthonormal basis using the following path:

1. If A and B are diagonalizable in a common orthonormal basis, then A and B commute.
2. If A and B commute, and if λ is an eigenvalue of A, then the eigenspace E_λ of A that is associated to the eigenvalue λ is invariant under B.
3. If A and B commute, then A and B have at least one common eigenvector.
4. If A and B commute, then A and B are diagonalizable in a common orthonormal basis.

Solution 81. 1. Suppose A and B are diagonalizable in a common orthonormal basis, say

$$PAP^\top = D_1 \quad \text{and} \quad PBP^\top = D_2$$

where P is an orthonormal matrix whose column vectors correspond to a common eigenbasis. In particular $P^\top = P^{-1}$. Then we have

$$\begin{aligned} AB &= P^\top D_1 P P^\top D_2 P \\ &= P^\top D_1 D_2 P \\ &= P^\top D_2 D_1 P \\ &= P^\top D_2 P P^\top D_1 P \\ &= BA. \end{aligned}$$

Thus A and B commute.

2. Suppose A and B commute and let λ be an eigenvalue of A with corresponding eigenspace E_λ. Then for any eigenvector $v \in E_\lambda$ corresponding to the eigenvalue λ, we have

$$\begin{aligned} ABv &= BAv \\ &= B\lambda v \\ &= \lambda Bv. \end{aligned}$$

It follows that Bv is also an eigenvector corresponding to the eigenvalue λ. Thus E_λ is invariant under B.

3. Suppose A and B commute. Since $B \neq 0$, we must have $B|_{E_\lambda} \neq 0$ for some eigenvalue λ of A. Applying the real spectral theorem to $B|_{E_\lambda}$, we see that there exists an eigenvector $v \in E_\lambda$ for $B|_{E_\lambda}$. Since $B|_{E_\lambda}$ is just the restriction of B to E_λ, we see that v is an eigenvector for B, and since $v \in E_\lambda$, we see that v is an eigenvector for A too. Thus v is a common eigenvector of A and B.

4. It is easier to prove this in the setting where A and B are linear transformations from a finite dimensional Hilbert-space $(V, \langle \cdot, \cdot \rangle)$ to itself. In this case, A and B being symmetric in the old settting translates to A and B being self-adjoint in the new setting: that is

$$\langle Av, w \rangle = \langle v, Aw \rangle \quad \text{and} \quad \langle Bv, w \rangle = \langle v, Bw \rangle$$

for all $v, w \in V$. So assuming A and B commute, let us show that they are diagonalizable and have a common orthonormal basis. We will do this by induction on the dimension of V. The base case $n = 1$ is trivial. Assume that we have shown the proposition to be true for all self-adjoint commuting linear maps $A, B \colon V \to V$ for all finite-dimensional Hilbert spaces V where $\dim V < n$ for some $n > 1$. Now suppose $A, B \colon V \to V$ are self-adjoint linear maps and suppose $\dim V = n$. By part 3, A and B both have a common eigenvector, say v (necessarily $v \neq 0$). By rescaling if necessary, we choose v such that $\|v\| = 1$. Consider the subspace W of V defined by

$$W = \{w \in V \mid \langle w, v \rangle = 0\}.$$

Since the inner-product is positive-definite, we have $\langle v, v \rangle \neq 0$. Thus the map $\langle \cdot, v \rangle \colon V \to \mathbb{R}$ is onto, and since $\ker(\langle \cdot, v \rangle) = W$, we see that $\dim W = n - 1$. Now observe that $A|_W$ and $B|_W$ are self-adjoint commuting linear maps which act on a finite-dimensional Hilbert space of dimension $< n$. By induction, $A|_W$ and $B|_W$ share a common orthonormal eigenbasis, say $w_1, \dots, w_{n-1} \in W$. We claim that $\{v, w_1, \dots, w_{n-1}\}$ is a common orthonormal eigenbasis for both A and B. Indeed, it suffices to show that they form an orthonormal eigenbasis since v and w_i were chosen to be eigenvectors for both A and B. This follows immediately from the fact that $\langle v, w_i \rangle = 0$ for all $1 \leq i \leq n-1$ since each $w_i \in W$. Also $\|v\| = \|w_i\| = 1$ for all $1 \leq i \leq n-1$ by construction. Thus $\{v, w_1, \dots, w_{n-1}\}$ is a common orthonormal eigenbasis for both A and B.

98.0.3 Finite groups of order $2n$, p, and p^2

Exercise 87. Let G be a finite group.

1. Show that if $|G| = 2n$ with $n \geq 3$ then there is a nonabelian group of order $2n$.
2. Show that if $|G| = p$ with $p > 0$ a prime integer, then G is abelian.
3. Show that if $|G| = p^2$ with $p > 0$ a prime integer, then G is abelian.
4. Find the smallest odd integer n such that there is a nonabelian group of order n. Give generators and relations for such a group.

Solution 82. 1. Consider the Dihedral group D_n, given in terms of generators and relations by

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle.$$

Every element in D_n can be expressed in the form $r^i s^j$ for unique $0 \leq i \leq n-1$ and $0 \leq j \leq 1$. In particular, $\#D_n = 2n$ (one can also see this from the isomorphism $D_n \cong C_2 \rtimes C_n$). Finally, we observe that D_n is nonabelian since in D_n we have $rs = r^{-1}s \neq sr$. Thus r and s do not commute (if $rs = sr$, then we'd have $r = r^{-1}$ which is impossible since r has order > 2).

2. Suppose $\#G = p$. Choose any nonidentity element $g \in G$. Then by Lagrange's Theorem, we must have $\operatorname{ord} g \mid p$. This implies $\operatorname{ord} g = p$ since g is not the identity element and since p is prime. In particular, we see that G is a cyclic group (which is certainly abelian!).

3. To prove this, we use the following lemma:

Lemma 98.1. *Any p-group has nontrivial center.*

Proof. Suppose G is a p-group, say $|G| = p^n$, and assume for a contradiction that $|\mathrm{Z}(G)| = 1$. Let $x_1, \dots, x_k$ represent the nontrivial conjugacy classes of G: so $|\mathrm{K}_{x_i}| > 1$ and $\mathrm{K}_{x_i} \cap \mathrm{K}_{x_j} = \emptyset$ for each $1 \leq i < j \leq k$ and

$$G = \{1\} \cup \mathrm{K}_{x_1} \cup \cdots \cup \mathrm{K}_{x_k}.$$

Then the class equation gives us

$$|G| = 1 + \sum_{i=1}^{k} [G : \mathrm{Z}(x_i)]. \tag{402}$$

Note that $p \mid [G : \mathrm{Z}(x_i)]$ for each $1 \leq i \leq k$. Indeed, $\mathrm{Z}(x_i)$ is a proper subgroup (otherwise x_i would not represent a nontrivial conjugacy class). Its order must divide the order of G by Lagrange's Theorem, thus $|\mathrm{Z}(x_i)| = p^{m_i}$ for some $m_i < n$. It follows that $[G : \mathrm{Z}(x_i)] = p^{n-m_i}$. With this understood, we now reduce (402) modulo p to get

$$0 \equiv 1 \bmod p,$$

which is a contradiction. □

Now we proceed with the problem at hand. Suppose $\#G = p^2$ and assume for a contradiction that $G \neq \mathrm{Z}(G)$. Since G is a p-group, $\mathrm{Z}(G)$ must be a nontrivial subgroup of G by Lemma (98.1). In particular, we must have $|\mathrm{Z}(G)| = p$. But then $|G/\mathrm{Z}(G)| = p$, which implies $G/\mathrm{Z}(G)$ is cyclic. It follows that G is abelian, which implies $G = \mathrm{Z}(G)$, a contradiction. So our assumption that $G \neq \mathrm{Z}(G)$ leads to a contradiction, which means we must in fact have $G = \mathrm{Z}(G)$.

98.0.4 Valuation domain equivalent characterizations

Proposition 98.1. *Let A be a domain and let K be its quotient field. The following conditions are equivalent*

1. *For all nonzero $a, b \in A$, either $a \mid b$ or $b \mid a$;*
2. *For all nonzero $x \in K$, either x or x^{-1} is in A;*
3. *There is a valuation v on K such that $A = \{x \in K \mid v(x) \geq 0\} \cup \{0\}$.*

Proof. ($1 \implies 2$): Let $x \in K^\times$. Write $x = a/b$ where $a, b \in A \backslash \{0\}$. Then either $a \mid b$ or $b \mid a$. If $b \mid a$, then we can write $a = bc$ for some nonzero $c \in A$. In this case, we have

$$\begin{aligned} x &= a/b \\ &= bc/b \\ &= c, \end{aligned}$$

and hence $x \in A$. On the other hand, if $a \mid b$, then we can write $b = ad$ for some nonzero $d \in A$. In this case, we have

$$\begin{aligned} x^{-1} &= b/a \\ &= ad/a \\ &= d, \end{aligned}$$

and hence $x^{-1} \in A$.

($2 \implies 3$): Let $\Gamma = K^\times / A^\times$. We define a total ordering on Γ as follows: Let $\overline{x}, \overline{y} \in \Gamma$. We say

$$\overline{x} \geq \overline{y} \text{ if and only if } xy^{-1} \in A. \tag{403}$$

Let us check that (81) is well-defined. Suppose xa and yb are two different representatives of the cosets $\overline{x}$ and $\overline{y}$ respectively, where $a, b \in A^\times$. Then

$$\begin{aligned} (xa)(yb)^{-1} &= (xa)(b^{-1}y^{-1}) \\ &= (xy^{-1})(ab^{-1}) \\ &\in A \end{aligned}$$

implies $\overline{xa} \geq \overline{yb}$. Thus (81) is well-defined. Next, observe that the relation given in (81) is antisymmetric: if $\overline{x} \geq \overline{y}$ and $\overline{y} \geq \overline{x}$, then $xy^{-1} \in A$ and $yx^{-1} \in A$, which implies $xy^{-1} \in A^\times$, and hence

$$\begin{aligned} \overline{x} &= \overline{x(yy^{-1})} \\ &= \overline{(xy^{-1})y} \\ &= \overline{y}. \end{aligned}$$

It is also transitive: if $\overline{x} \geq \overline{y}$ and $\overline{y} \geq \overline{z}$, then

$$\begin{aligned} xz^{-1} &= x(y^{-1}y)z^{-1} \\ &= (xy^{-1})(yz^{-1}) \\ &\in A, \end{aligned}$$

which implies $\overline{x} \geq \overline{z}$. It is also a total relation since either $\overline{x} \geq \overline{y}$ or $\overline{y} \geq \overline{x}$ (since either $xy^{-1} \in A$ or $yx^{-1} \in A$ by our assumption). Thus (81) gives us a total ordering on Γ.

Now we define $v \colon K^\times \to \Gamma$ to be the natural quotient map. Clearly v is a surjective homomorphism. We also have

$$v(x+y) \geq \min\{v(x), v(y)\} \text{ with equality if } v(x) \neq v(y).$$

Indeed, assume without loss of generality that $v(y) \geq v(x)$, so $v(x) = \min\{v(x), v(y)\}$. Then $(x+y)x^{-1} = 1 + yx^{-1} \in A$ implies $v(x+y) \geq v(x)$. Now assume $v(x) \neq v(y)$, so $yx^{-1} \notin A$. Then $x^{-1}(x+y) = 1 + yx^{-1} \notin A$. This implies $x(x+y)^{-1} \in A$ (by our assumption). Thus $v(x) \geq v(x+y)$, which implies $v(x) = v(x+y)$ by antisymmetry of $\geq$. Finally, we observe that

$$A^\times = \{x \in K \mid v(x) = 0\}$$

by construction. Moreover, we have

$$A = \{x \in K \mid v(x) \geq 0\} \cup \{0\},$$

since $v(x) \geq 0$ if and only if $v(x) \geq v(1)$ if and only if $x \in A$.

($3 \implies 1$): Let $(\Gamma, \geq)$ be a totally ordered abelian group and let $v \colon K^\times \to \Gamma$ be such a valuation. Suppose $a, b \in A \backslash \{0\}$, and without loss of generality, assume that $v(b) \geq v(a)$. Then

$$\begin{aligned} v(ba^{-1}) &= v(b) - v(a) \\ &\geq 0 \end{aligned}$$

implies $ba^{-1} \in A$. In particular, this implies $a \mid b$. □

99 Winter 2014

99.1 Abstract Algebra

99.1.1 $\mathrm{GL}_n(\mathbb{F}_p)$ counting

Exercise 88. Let p be a prime and $\mathbb{F}_p$ the finite field with p elements. Recall $\mathrm{GL}_n(\mathbb{F}_p)$ is the group of $n \times n$ intvertible matrices with entries in $\mathbb{F}_p$.

1. Prove that the size of $\mathrm{GL}_n(\mathbb{F}_p)$ is given by $\#\mathrm{GL}_n(\mathbb{F}_p) = \prod_{j=0}^{n-1}(p^n - p^j)$.

We now consider the case where $n = 2$. Set $G = \mathrm{GL}_2(\mathbb{F}_p)$, $U = \left\{ \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in G \right\}$, and $B = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G \right\}$.

1. Prove that U is a p-Sylow subgroup of G. Give another p-Sylow subgroup of G.

2. Prove that $B \subseteq \mathrm{N}_G(U)$ where $\mathrm{N}_G(U)$ denotes the normalizer of U in G.

3. Let n_p be the number of p-Sylow subgroups of G. Calculate n_p and prove your answer is correct.

Solution 83. 1. Let A be a random matrix in $\mathrm{GL}_n(\mathbb{F}_p)$ and let $v_1, \dots, v_n$ denote the column vectors of A. Note that counting the number of matrices A in $\mathrm{GL}_n(\mathbb{F}_p)$ is equivalent to counting the number of ordered tuples of linearly independent vectors $(v_1, \dots, v_n)$. So it suffices to count the latter.

There are $p^n - 1$ different possible vectors in $\mathbb{F}_p^n$ for which v_1 can be. The only vector which is not allowed is the zero vector. This is because the vectors $(v_1, \dots, v_n)$ must be linearly independent, so no zero vectors allowed. Now we fix v_1. Then there are $p^n - p$ different possible vectors in $\mathbb{F}_p^n$ for which v_2 can be. Indeed, v_1 and v_2 must be linearly independent, so v_2 cannot equal to any vectors of the form av_1 where $a \in \mathbb{F}_p$. If we had fixed v_1 to be a different vector, then the same counting argument would apply, so altogether, the number of pairs of linearly independent vectors (v_1, v_2) is $(p^n - 1)(p^n - p)$.

More generally, for $1 \leq j \leq n$, if the vectors $v_1, \dots, v_{j-1}$ are fixed, then there are $p^n - p^{j-1}$ different possible vectors in $\mathbb{F}_p^n$ for which v_j can be. Again, varying the vectors $v_1, \dots, v_{j-1}$ to a new set of fixed vectors results in the same counting argument, so altogether the number of j-tuples of linearly independent vectors $(v_1, v_2, \dots, v_j)$ is $(p^n - 1)(p^n - p) \cdots (p^n - p^{j-1})$. In particular, taking $j = n$ gives us

$$\#\mathrm{GL}_n(\mathbb{F}_p) = \prod_{j=1}^{n}(p^n - p^{j-1}) = \prod_{j=0}^{n-1}(p^n - p^j).$$

2. First note that $\#G = (p^2 - p)(p^2 - 1) = p(p-1)^2(p+1)$. In particular, the largest power of p in $\#G$ is simply p. Thus every p-Sylow subgroup of $\#G$ has size p. The set U certainly has size p since every element in U has the form $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ for some $x \in \mathbb{F}_p$. To see that it is a p-Sylow subgroup then, we just need to show that it is a subgroup. It is clearly nonempty. Also, if $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)$ are two matrices in U, then

$$\begin{aligned}
\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & x-y \\ 0 & 1 \end{pmatrix} \\
&\in U.
\end{aligned}$$

It follows that U is a subgroup, and hence a p-Sylow subgroup of G. In fact, it is a cyclic, generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Another p-Sylow subgroup of G is obtained by simply taking the transpose of all matrices in U. Namely we set $U^\top = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) \in G \right\}$. Again, $U^\top$ has a size p and is a subgroup of G, so it is a p-Sylow subgroup of G. It is different from U becuase, $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in U^\top$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \notin U$.

3. Let $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in B$ and $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in U$. Then

$$\begin{aligned}
\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} &= \frac{1}{ad}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \\
&= \frac{1}{ad}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} d & ax-b \\ 0 & a \end{pmatrix} \\
&= \frac{1}{ad}\begin{pmatrix} ad & a^2x \\ 0 & ad \end{pmatrix} \\
&= \begin{pmatrix} 1 & (a/d)x \\ 0 & 1 \end{pmatrix} \\
&\in U.
\end{aligned}$$

It follows that $B \subseteq \mathrm{N}_G(U)$.

4. By the Sylow Theorems, we have $n_p = [\mathrm{N}_G(U) : U]$. Also the size of B is given by $\#B = (p-1)^2 p$. Thus

$$\begin{aligned} n_p &= [\mathrm{N}_G(U) : U] \\ &= [\mathrm{N}_G(U) : B][B : U] \\ &= [\mathrm{N}_G(U) : B](p-1)^2 \end{aligned}$$

$$n_p = [\mathrm{N}_G(U) : U]$$

We claim that $\mathrm{N}_G(U) = B$. Indeed, we've already shown that $B \subseteq \mathrm{N}_G(U)$. Conversely, let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ and $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in U$. Then

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} &= \frac{1}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \frac{1}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d-cx & -b+ax \\ -c & a \end{pmatrix} \\ &= \frac{1}{\Delta} \begin{pmatrix} \Delta - acx & a^2 x \\ c^2 x & \Delta + acx \end{pmatrix} \end{aligned}$$

where $\Delta = ad - bc$. Thus $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ conjugates $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ to another element of U if and only if $c = 0$, that is, if and only if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in B$. It follows that $\mathrm{N}_G(U) \subseteq B$. Therefore $\mathrm{N}_G(U) = B$. Finally, the number of matrices in B is given by $\#B = (p-1)^2 p$ since for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in B$, there $p-1$ different choices for a and d and there are p different choices b. It follows from the Sylow Theorems that

$$\begin{aligned} n_p &= [G : \mathrm{N}_G(U)] \\ &= [G : B] \\ &= \frac{p(p-1)^2(p+1)}{p(p-1)^2} \\ &= p+1. \end{aligned}$$

99.1.2 Symmetric group is generated by transpositions

Exercise 89. As usual, let S_n denote the set of bijections from the set $[n] = \{1, \dots, n\}$ to itself.

1. Show that as a group S_n is generated by transpositions. Be sure to prove *all* your assertions.
2. Cayley's Theorem states that any group is isomorphic to a permutation group. Prove from first principles that any group of order n is isomorphic to a subgroup of S_n.
3. Considering what you know about $n \times n$ elementary matrices action on GL_n, show that any group of order n can be realized as a subgroup of $\mathrm{GL}_n(\mathbb{F}_2)$.

Solution 84. 1. We shall prove this in two steps.

Step 1: First we show that any element in S_n can be expressed as a product of disjoint cycles. Let $\sigma \in S_n$. We shall describe an algorithm which expresses σ as a product of disjoint cycles. In the first step of the algorithm, choose any $a_{1,1} \in [n]$. Let k_1 be the least nonnegative integer such that $\sigma^{k_1}(a_{1,1}) = a_{1,1}$. We denote $a_{1,i_1} = \sigma^{i_1 - 1}(a_{1,1})$ for each $1 \leq i_1 \leq k_1$. Observe that $1 \leq k_1 \leq n$ by the pigeonhole principle. Also observe that $a_{1,i_1} \neq a_{1,i'_1}$ whenever $i_1 \neq i'_1$. Indeed, if $a_{1,i_1} = a_{1,i'_1}$ for some $1 \leq i_1 < i'_1 \leq k_1$, then

$$\begin{aligned} \sigma^{i'_1 - i_1}(a_{1,1}) &= \sigma^{i'_1} \sigma^{-i_1}(a_{1,1}) \\ &= \sigma^{-i_1} \sigma^{i'_1}(a_{1,1}) \\ &= \sigma^{-i_1}(a_{1,i'_1}) \\ &= \sigma^{-i_1}(a_{1,i_1}) \\ &= a_{1,1}, \end{aligned}$$

which would contradict the minimality of k_1 since $i_1' - i_1 < k_1$. So if we denote $\tau_1 = (a_{1,1} \cdots a_{1,k_1})$ and $\sigma_1 = \tau_1^{-1}\sigma$, then we can express σ as

$$\sigma = \tau_1\sigma_1.$$

where τ_1 is a cycle of length k_1 and where σ_1 fixes $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\}$. Indeed, we have

$$\begin{aligned} \sigma_1(a_{1,i}) &= \tau_1^{-1}\sigma(a_{1,i_1}) \\ &= \tau_1^{-1}(a_{1,i_1+1}) \\ &= a_{1,i_1}, \end{aligned}$$

where a_{1,i_1+1} is understood to be $a_{1,1}$ if $i_1 = k_1$.

Now we proceed to the second step of the algorithm. If $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\} = [n]$, then the algorithm terminates and we are done. Indeed, in this case, σ_1 is the identity element since it fixes all of $[n]$. Then $\sigma = \tau_1$ shows that σ is a cycle itself. If $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\} \subset n$, where the inclusion is proper, then we choose any $a_{2,1} \in [n] \backslash \{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\}$. Let k_2 be the least nonnegative integer such that $\sigma^{k_2}(a_{2,1}) = a_{2,1}$. We denote $a_{2,i_2} = \sigma^{i_2-1}(a_{2,1})$ for each $1 \leq i_2 \leq k_2$. As in the case of the first step of the algorithm, we observe that $1 \leq k_2 \leq n - k_1$ and we also observe that $a_{2,i_2} \neq a_{2,i_2'}$ whenever $i_2 \neq i_2'$. The proof for these two observations is nearly identical to the ones we did above. We denote $\tau_2 = (a_{2,1} \cdots a_{2,k_2})$ and $\sigma_2 = \tau_2^{-1}\sigma_1$. Then we can express σ_1 as

$$\sigma_1 = \tau_2\sigma_2,$$

where τ_2 is a cycle of length k_2 and where σ_2 fixes $\{a_{1,i_1}, a_{1,i_2} \mid 1 \leq i_1 \leq k_1 \text{ and } 1 \leq i_2 \leq k_2\}$. Indeed, the proof that σ_2 fixes a_{1,i_2} is nearly identical to the proof that σ_1 fixes a_{1,i_1}, and the reason that σ_2 fixes a_{1,i_1} is because both τ_2 and σ_1 fix a_{1,i_1}.

Now we describe the algorithm at the sth step where $s \geq 2$. If $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\} = [n]$, then the algorithm terminates and we are done. Indeed, in this case, σ_{s-1} is the identity element since it fixes all of $[n]$. Then

$$\begin{aligned} \sigma &= \tau_1\sigma_1 \\ &= \tau_1\tau_2\sigma_2 \\ &\vdots \\ &= \tau_1\tau_2\cdots\tau_{s-1}\sigma_{s-1} \\ &= \tau_1\tau_2\cdots\tau_{s-1} \end{aligned}$$

shows that σ is a product of distinct cycles. If $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\} \subset [n]$, where the inclusion is proper, then we choose any $a_{s,1} \in [n] \backslash \{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\}$. Let k_s be the least nonnegative integer such that $\sigma^{k_s}(a_{s,1}) = a_{s,1}$. We denote $a_{s,i_s} = \sigma^{i_s-1}(a_{s,1})$ for each $1 \leq i_s \leq k_s$. As in the case of the first and second step of the algorithm, we observe that $1 \leq k_s \leq n - k_1 - \cdots - k_{s-1}$ and we also observe that that $a_{s,i_s} \neq a_{s,i_s'}$ whenever $i_s \neq i_s'$. We denote $\tau_s = (a_{s,1} \cdots a_{s,k_s})$ and $\sigma_s = \tau_s^{-1}\sigma_{s-1}$. Then we can express σ_{s-1} as

$$\sigma_{s-1} = \tau_s\sigma_s,$$

where τ_s is a cycle of length k_s and where σ_s fixes $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\}$.

This algorithm must terminate since $[n]$ is finite and since after the sth step, we produce a strictly increasing sequence of sets

$$(\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\})$$

each of which is contianed in $[n]$.

Step 2: Now we show that any cycle in S_n can be expressed as a product of transposition. Let $(a_1a_2\cdots a_k)$ be any in S_n. We claim that

$$(a_1a_2\cdots a_k) = \prod_{i=1}^{k-1}(a_ia_{i+1}). \tag{404}$$

Indeed, let $a \in [n]$. If $a \neq a_j$ for any $1 \leq j \leq k$, then applying a to both $(a_1a_2\cdots a_k)$ and $\prod_{i=1}^{k-1}(a_ia_{i+1})$ results in a again. In other words, both $(a_1a_2\cdots a_k)$ and $\prod_{i=1}^{k-1}(a_ia_{i+1})$ fix a. If $a = a_j$ for some $1 \leq j \leq k$, then applying a_j to $(a_1a_2\cdots a_k)$ results in a_{j+1}, where a_{j+1} is understood to be a_1 if $j = k$. Applying a_j to $\prod_{i=1}^{k-1}(a_ia_{i+1})$ also results in

a_{j+1}, where a_{j+1} is understood to be a_1 if $j = k$. Indeed,

$$\begin{aligned}\prod_{i=1}^{k-1}(a_i a_{i+1})(a_j) &= (a_1 a_2)\cdots(a_{j-1}a_j)(a_j a_{j+1})\cdots(a_k a_{k-1})(a_j)\\ &= (a_1 a_2)\cdots(a_{j-1}a_j)(a_j a_{j+1})(a_j)\\ &= (a_1 a_2)\cdots(a_{j-1}a_j)(a_{j+1})\\ &= a_{j+1}.\end{aligned}$$

Combining step 1 with step 2 shows that any permutation can be expressed as a product of transpositions.

2. We state and prove Cayley's Theorem:

Theorem 99.1. *(Cayley's Theorem) Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.*

Proof. We write S_G for the group of all permutations of G as a set. We have $S_G \cong S_n$, so we just need to show that G is isomorphic to a subgroup of S_G. Define a map $\pi\colon G \to S_G$, denoted $\pi \mapsto \pi_g$, where $\pi_g\colon G \to G$ is given by

$$\pi_g(x) = gx$$

for all $x \in G$. We claim that π is an injective group homomorphism. Indeed, first let us show that it is a group homomorphism. Let $g_1, g_2 \in G$. Then observe that

$$\begin{aligned}\pi_{g_1 g_2}(x) &= g_1 g_2 x\\ &= \pi_{g_1}(g_2 x)\\ &= \pi_{g_1}\pi_{g_2}(x)\end{aligned}$$

for all $x \in G$. It follows that $\pi_{g_1 g_2} = \pi_{g_1}\pi_{g_2}$, and hence π is a group homomorphism. Now let us show that it is injective. Suppose $g \in \ker \pi$. Thus $gx = x$ for all $x \in G$. In particular, $g^2 = g$. Multiplying both sides by g^{-1} implies $g = 1$. Thus $\ker \pi = \{1\}$, which implies π is injective. Finally, by the first isomorphism theorem for groups, we find that $\operatorname{im} \pi$ is a subgroup of S_G, and moreover,

$$\operatorname{im} \pi \cong G/\ker \pi \cong G.$$

It follows that G is isomorphic to a subgroup of S_G which implies G is isomorphic to a subgroup of S_n.

□

3. It suffices to show that S_n can be realized as a subgroup of $\mathrm{GL}_n(\mathbb{F}_2)$ since G can be realized as a subgroup of S_n. Since S_n is generated by transpositions, we can define a group homomorphism out of S_n by describing how it acts on transpositions, however we need to be sure that this map respects any relations involving these transpositions. For each $1 \leq i < j \leq n$, let s_{ij} be the matrix in $\mathrm{GL}_n(\mathbb{F}_2)$ obtained by swapping the ith row with the jth row in the identity matrix. For any matrix A, multiplying s_{ij} to left of A results in the same matrix obtained by swapping the ith and jth row of A. Thus we can view s_{ij} as a transposition of the rows of A. Thus we have the relations

$$s_{ij}s_{kl} = \begin{cases} s_{kl}s_{ij} & \text{if } i \neq k \text{ and } j \neq l\\ s_{kl}s_{il} & \text{if } j = k\\ s_{kl}s_{jl} & \text{if } i = k \text{ and } j \neq l\\ 1 & \text{if } i = k \text{ and } j = l\end{cases}$$

In particular, we can define an injective group homomorphism $\varphi\colon S_n \to \mathrm{GL}_n(\mathbb{F}_2)$ as follows: let $\sigma \in S_n$ and express it as a product of transpositions, say $\sigma = (i_1 j_1)\cdots(i_k j_k)$. Then we set

$$\varphi(\sigma) = s_{i_1 j_1}\cdots s_{i_k j_k}.$$

Note that φ is a well-defined group homomorphism since the s_{ij} satisfy the relations described above.

99.1.3 Non-commutative polynomial ring over characteristic p

Exercise 90. Suppose that p is a prime and that R is a characteristic p ring which identity. Let

$$R\{X\} = \left\{ \sum_{i=0}^{n} a_i X^{p^i} \mid a_i \in R \right\} \tag{405}$$

Note that the polynomials in $R\{X\}$ have no constant term.

1. Show that $R\{X\}$ is a ring under the operations of polynomial addition and composition of functions.
2. Suppose that F is a characteristic p field. Then we can consider the ring $F\{X\}$ defined as in (405). It is a fact (which you do not need to prove) that $F\{X\}$ is not commutative. Show that $F\{X\}$ has a right division algorithm, that is, show that for $a(X), b(X) \in R\{X\}$ with $b(X) \neq 0$, there exists $q(X), r(X) \in F\{X\}$ with $r(X) = 0$ or $\deg(r(X)) < \deg(b(X))$ and $a(X) = q(X)b(X) + r(X)$.
3. Again suppose that F is a characteristic p field and consider the ring $F\{X\}$ defined as in (405). Show that every left ideal of $F\{X\}$ is principal. You may use the result from part (3b).

Solution 85. 1. Let $f, g, h \in R\{X\}$ and express them as

$$f(X) = \sum_{i \geq 0} a_i X^{p^i}, \quad g(X) = \sum_{i \geq 0} b_i X^{p^i}, \quad \text{and} \quad \sum_{i \geq 0} c_i X^{p^i}$$

where $a_i, b_i, c_i \in R$ such that $a_i = b_i = c_i = 0$ for $i \gg 0$. We have

$$\begin{aligned} f \circ g &= \sum_{i \geq 0} a_i \left(\sum_{j \geq 0} b_j X^{p^j} \right)^{p^i} \\ &= \sum_{i \geq 0} a_i \sum_{j \geq 0} b_j^{p^i} X^{p^{i+j}} \\ &= \end{aligned}$$

$$\begin{aligned} (f+g) \circ h &= \left(\sum_{i \geq 0} a_i X^{p^i} + \sum_{i \geq 0} b_i X^{p^i} \right) \sum_{i \geq 0} c_i X^{p^i} \\ &= \sum_{i \geq 0} (a_i + b_i) X^{p^i} \sum_{i \geq 0} c_i X^{p^i} \end{aligned}$$

99.2 Linear Algebra

99.2.1 Rank, transpose, and difference of two squares

Exercise 91. Let A be a real $n \times n$ matrix.

1. Prove that $\operatorname{rank}(A^{n+1}) = \operatorname{rank}(A^n)$.
2. Prove that $\operatorname{rank}(A^\top A) = \operatorname{rank}(A)$.
3. We say A is a **difference of two squares** if there exists real $n \times n$ matrices B and C such that $BC = CB = 0$ and $A = B^2 - C^2$. Prove that if A is symmetric, then A is a difference of two squares.
4. Let $A = B^2 - C^2$ be a difference of two squares as defined in part 3. Prove that if B has a nonzero real eigenvalue, then A has a positive real eigenvalue.

Solution 86. 1. First note that for any $i \in \mathbb{N}$, if $\dim(\operatorname{im} A^i) = \dim(\operatorname{im} A^{i+1})$, then $\operatorname{im} A^i = \operatorname{im} A^{i+1}$. Indeed, this is because $\operatorname{im} A^{i+1}$ is already a subspace of $\operatorname{im} A^i$, and so having equal dimensions forces equality. Now observe that

$$n \geq \dim(\operatorname{im} A) \geq \dim(\operatorname{im} A^2) \geq \cdots \geq \dim(\operatorname{im} A^i) \geq \cdots \geq 0.$$

By the pigeonhole principle, there must be some $1 \leq i \leq n$ such that $\dim(\operatorname{im} A^i) = \dim(\operatorname{im} A^{i+1})$. In this case, it follows that

$$\operatorname{im} A^i = \operatorname{im} A^{i+1} = \cdots = \operatorname{im} A^{n+1}.$$

In particular, we have $\operatorname{rank}(A^{n+1}) = \operatorname{rank}(A^n)$.

2. We claim that $A^\top|_{\operatorname{im} A} \colon \operatorname{im} A \to \operatorname{im} A^\top A$ is injective. Indeed, let $Av \in \ker A^\top$. Then observe that

$$\begin{aligned}
\|Av\|^2 &= (Av)^\top (Av) \\
&= v^\top A^\top A v \\
&= v^\top 0 \\
&= 0,
\end{aligned}$$

where $\|\cdot\|$ denotes the Euclidean norm on $\mathbb{R}^n$. Since $\|\cdot\|$ is positive definite, it follows that $Av = 0$. This implies $A^\top|_{\operatorname{im} A}$ is injective. Therefore

$$\begin{aligned}
\operatorname{rank}(A^\top A) &= \dim(\operatorname{im}(A^\top A)) \\
&= \dim(\operatorname{im} A) \\
&= \operatorname{rank}(A).
\end{aligned}$$

3. Assume that A is symmetric. By the real spectral theorem, A can be diagonalized by an orthogonal matrix. That is, there is an orthogonal matrix P and a diagonal matrix D such that $PAP^\top = D$. The diagonal matrix D has the form

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_k & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_{k+1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_n \end{pmatrix}$$

ordered in such a way that first k entries along the main diagonal are nonnegative and the remaining entries negative. Note that we can express D as $D = D_+^2 - D_-^2$ where

$$D_+ = \begin{pmatrix} \sqrt{\lambda_1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\lambda_k} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad D_- = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{-\lambda_{k+1}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{-\lambda_n} \end{pmatrix}.$$

Furthermore it's easy to see that $D_+D_- = 0 = D_-D_+$. Then setting $B = P^\top D_+ P$ and $C = P^\top D_- P$, we find that

$$\begin{aligned}
A &= P^\top D P \\
&= P^\top (D_+^2 - D_-^2) P \\
&= P^\top D_+^2 P - P^\top D_-^2 P \\
&= (P^\top D_+ P)^2 - (P^\top D_- P)^2 \\
&= B^2 - C^2.
\end{aligned}$$

Furthemore we have

$$\begin{aligned}
BC &= P^\top D_+ P P^\top D_- P \\
&= P^\top D_+ D_- P \\
&= P^\top 0 P \\
&= 0.
\end{aligned}$$

A similar calculation gives us $CB = 0$.

4. Let λ be a nonzero eigenvalue for B and choose an eigenvector v corresponding to λ. Observe that

$$\begin{aligned}
0 &= CBv \\
&= \lambda C v
\end{aligned}$$

implies $Cv = 0$ since $\lambda \neq 0$. Therefore

$$\begin{aligned} Av &= (B^2 - C^2)v \\ &= B^2 v - C^2 v \\ &= B^2 v \\ &= \lambda^2 v. \end{aligned}$$

It follows that v is an eigenvector for A corresponding to the positive eigenvalue λ^2.

Part X
Miscellaneous

100 Ring Extensions

Let A be a noetherian domain which is integrally closed in its field of fractions K. Let L/K be a finite field extension with $n = [L : K]$ and let B be the integral closure of A in L. We want to know under what conditions is B a finitely generated A-module. The following proposition gives one such condition:

Proposition 100.1. *If L/K is separable, then B is a finitely generated A-module.*

Proof. We first define a symmetric non-denerate K-bilinear form $\langle \cdot, \cdot \rangle \colon L \times L \to K$ as follows: given $y, y' \in L$, we set

$$\langle y, y' \rangle := \mathrm{Tr}_{L/K}(yy').$$

Indeed, it is clearly symmetric and bilinear since the usual multiplication map on L is symmetric and K-bilinear and since the trace map is K-linear. Recall that $\mathrm{Tr}_{L/K} = 0$ if and only if L/K is inseparable. Equivalently, $\mathrm{Tr}_{L/K}$ is onto if and only if L/K is separable. Since L/K is separable, there exists a $\widetilde{y} \in L$ such that $\mathrm{Tr}_{L/K}(\widetilde{y}) \neq 0$. In particular, if $y \neq 0$ is in L, then $\langle y, y^{-1}\widetilde{y} \rangle \neq 0$, hence $\langle \cdot, \cdot \rangle$ is non-degenerate as well. We claim that the trace map restricted to B lands in A. To see this, we first choose a finite extension L'/L such that L'/K is Galois. Then for each $b \in B$ we have

$$\mathrm{Tr}_{L/K}(b) = \sum_{\sigma \colon L \hookrightarrow L'} \sigma(b) \tag{406}$$

where the sum in L' is taken over all K-embeddings $\sigma \colon L \hookrightarrow L'$. Each $\sigma(b)$ is integral over A since b is integral over A, and thus the sum (406) is also integral over A. Since $\mathrm{Tr}_{L/K}(b) \in K$ and is integral over A, it follows that $\mathrm{Tr}_{L/K}(b) \in A$. Now for each $y \in L$, we obtain a K-linear map $\ell_y \colon L \to K$ where $\ell_y(y') = \langle y, y' \rangle$ for all $y' \in L$. Given an A-submodule M of L, we set

$$M^\vee = \{y \in L \mid \ell_y(M) \subseteq A\} = \{y \in L \mid \langle y, u \rangle \in A \text{ for all } u \in M\}.$$

Suppose that $e_1, \dots, e_n$ is a K-basis of L, and by rescaling the e_i if necessary, we may also assume that each e_i is in B. For each i, we let $e_i^\vee$ be the unique element in L such that

$$\langle e_i^\vee, e_j \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases}$$

Indeed, $e_i^\vee$ is unique precisely because $\langle \cdot, \cdot \rangle$ is non-degenerate. If we set $F = \sum_i Ae_i$ to be the free A-module spanned by the e_i, then clearly we have $F^\vee = \sum_i Ae_i^\vee$. Furthermore we have inclusions:

$$F \subseteq B \subseteq B^\vee \subseteq F^\vee.$$

In particular, B is contained in a finitely generated A-module, and since A is noetherian, it follows that B is a finitely generated A-module. □

Remark 136. The condition stated in the proposition above is not the only condition that implies B is a finitely generated A-module. One can show that if A is a finitely generated $\Bbbk$-algebra where $\Bbbk$ is a field, then B is a finitely generated A-module. Similarly one can show that if A is a complete discrete valuation ring, then B is a finitely generated A-module.

Keep the same notation as above and assume B is finitely generated as an A-module. We also assume that $\dim A = 1$, hence A is a Dedekind domain. This implies $\dim B = 1$ since B is integral over A, and thus B is a

Dedekind domain too. In this case, if we are given a nonzero prime $\mathfrak{p}$ of A, then $\Bbbk = A/\mathfrak{p}$ is a field and $\overline{B} = B/\mathfrak{p}$ is a finite $\Bbbk$-algebra. In particular, then we have a decomposition

$$\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_{\mathfrak{p}}}$$

where the $e_{\mathfrak{q}} \in \mathbb{Z}_{\geq 0}$ are uniquely determined. Since there are only

Proposition 100.2.

100.1 Conductor

Let B/A be an extension of commutative rings. The **conductor** of B/A is the ideal $\mathfrak{f} = \mathfrak{f}(B/A)$ of A given by

$$\mathfrak{f} := \operatorname{Ann}_A(B/A) = \{x \in A \mid xB \subseteq A\}.$$

101 Discriminants

Let K be a field and let R be a finite K-algebra. There is a canonical symmetric K-bilinear map $\langle \cdot, \cdot \rangle \colon R \times R \to K$ given by

$$\langle r, r' \rangle = \operatorname{Tr}_{R/K}(rr')$$

for all $r, r' \in R$. We call $\langle \cdot, \cdot \rangle$ the **trace product** of R/K. The the reason why the trace product of R/K is useful is because it can help us determine the structure of R as a K-algebra. Indeed, in general R will be isomorphic as a K-algebra to a direct product of fields

$$R \simeq L_1 \times L_2 \times \cdots \times L_m,$$

where L_i/K is a finite extension. Then in this case, the trace product will decompose as

$$\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_1 + \langle \cdot, \cdot \rangle_2 + \cdots + \langle \cdot, \cdot \rangle_m,$$

where $\langle \cdot, \cdot \rangle_i$ corresponds to the trace product of the field extension L_i/K. More specifically, if $r, r' \in R$, then we set

$$\langle r, r' \rangle_i = \begin{cases} \langle r, r' \rangle & \text{if } r, r' \in L_i \\ 0 & \text{else} \end{cases}$$

Moreover, if L_i/K is not separble, then $\langle \cdot, \cdot \rangle_i = 0$, and if L_i/K is separable, then $\langle \cdot, \cdot \rangle_i|_{L_i \times L_i}$ is non-degenerate and agrees with the trace product of L_i/K.

Now suppose K is the field of fractions of a dedekind domain A, and that A is integrally closed in K. Let L/K be a finite extension of fields and let B be the integral closure of A in L. Then the trace product of L/K has the following nice property:

1. When we restrict to entries in B, we land in A (you prove this by using the description of the trace function as a sum of embeddings formula). Thus the trace product of L/K restricts to the trace product of B/A.

2. Suppose $\mathfrak{q}$ is a prime ideal of B which lies over a prime ideal $\mathfrak{p}$ of A. Also set $\Bbbk_{\mathfrak{q}} = B/\mathfrak{q}$ and $\Bbbk = A/\mathfrak{p}$, so we have an extension $\Bbbk_{\mathfrak{q}}/\Bbbk_{\mathfrak{p}}$ of finite fields. When we restrict to entries in $\mathfrak{q}$, we land in $\mathfrak{q}$. Furthermore, if we restrict one entry in $\mathfrak{p}$ and the other entry in $\mathfrak{q}$, then we land in $\mathfrak{p}$. Thus the trace product of trace product of B/A and this is a lift of the trace product of $\Bbbk_{\mathfrak{q}}/\Bbbk_{\mathfrak{p}}$.

In particular, let $\boldsymbol{e} = e_1, \dots, e_n$ be a K-basis of L such that each e_i is in B, and let $\boldsymbol{e}^\vee = e_1^\vee, \dots, e_n^\vee$ be the dual basis of $\boldsymbol{e}$ with respect to $\langle \cdot, \cdot \rangle$, that is

$$\langle e_i, e_j^\vee \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases}$$

101.1 Discriminant Ideal

Let A be a noetherian domain and let B be finitely-generated A-algebra which is finitely generated and torsion-free as an A-module. We further assume that B is "locally free" as an A-module in the sense that for every maximal ideal $\mathfrak{m}$ of A, the finitely generated $A_{\mathfrak{m}}$-module $B_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$. Since A is noetherian,

102 Bass Numbers

Let $(R, \mathfrak{m}, \Bbbk)$ be a local noetherian ring and let M be a finitely generated R-module. The i**th Bass number** of M is given by

$$\mu^i = \mu^i_R(M) := \dim_{\Bbbk}(\mathrm{Ext}^i_R(\Bbbk, R)).$$

We are interested in the sequence (μ^i) and how it grows. For instance, it is known that R is Gorenstein if and only if its Bass numbers are eventually 0. The following question however is open:

Question: If R is Cohen-Macaulay and (μ^i) is bounded, then is R Gorenstein?

Now note that if $x \in \mathfrak{m}$ is R-regular and M-regular, then $\mu^i_{R/x}(M/x) = \mu^i_R(M)$. In particular, by modding out by a regular sequence if necessary, we can reduce this question to the case where $\dim R = 0$. In the $\dim R = 0$ case, we want to show

$$\begin{aligned} (\mu^i) \text{ is bounded } &\iff 0 : \mathfrak{m} \text{ is simple} \\ &\iff \omega_R \text{ generated by one element.} \end{aligned}$$

It is useful to capture the sequence (μ^i) in the form of a generating function. Thus we define the **Bass series** of M to be the formal power series

$$\mathrm{I}(t) := \mathrm{I}^M_R(t) = \sum_{i \in \mathbb{Z}} \mu^i_R(M) t^i \in \mathbb{Z}[\![t]\!].$$

Now in order to compute the Bass series, we first need to know how to compute $\mathrm{Ext}_R(\Bbbk, R)$. There are a couple ways of doing this:

1. Choose an injective resolution $E = (E, \delta)$ of R over itself and choose a free resolution $F = (F, \mathrm{d})$ over $\Bbbk$ over R. Then
$$\mathrm{H}(F^\vee) = \mathrm{Ext}_R(\Bbbk, R) = \mathrm{H}(0 :_E \mathfrak{m}),$$
where $F^\vee$ is the graded dual of F and where $0 :_E \mathfrak{m} = \{e \in E \mid \mathfrak{m}e = 0\}$ is the annihilator of $\mathfrak{m}$ in E.

2. Suppose we have a short exact sequence of the form
$$0 \longrightarrow R \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{407}$$
Then for each i we get an exact sequence which could potentially be used in an induction argument:
$$\mathrm{Ext}^i_R(\Bbbk, M_2) \longrightarrow \mathrm{Ext}^i_R(\Bbbk, M_3) \longrightarrow \mathrm{Ext}^{i+1}_R(\Bbbk, R) \longrightarrow \mathrm{Ext}^{i+1}_R(\Bbbk, M_2) \tag{408}$$
Similarly, suppose we have a short exact sequence of the form
$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow \Bbbk \longrightarrow 0 \tag{409}$$
Then for each i we get another exact sequence which could potentially be used in an induction argument:
$$\mathrm{Ext}^i_R(N_2, R) \longrightarrow \mathrm{Ext}^i_R(N_1, R) \longrightarrow \mathrm{Ext}^{i+1}_R(\Bbbk, R) \longrightarrow \mathrm{Ext}^{i+1}_R(N_2, R) \tag{410}$$

102.1 Cohen Structure Theorem

Let $(R, \mathfrak{m}, \Bbbk)$ be a local noetherian ring. Let $\delta = \operatorname{depth} R$, let $e = \operatorname{edim} R = \beta_1(\mathfrak{m})$, and let $c = e - \delta$ be the **ecodepth** of R. The Cohen Structure Theorem states that there exists a complete regular local ring $(P, \mathfrak{p}, \Bbbk)$ and an ideal $I \subseteq \mathfrak{p}^2$ such that $\widehat{R} = P/I$ and such that $\rho = \mathrm{pd}_P(\widehat{R}) = c$. Avramvo showed that if $c \leq 3$ and R is not Gorenstein, then there exists $\gamma > 1$ such that

$$\mu^{d+i} \geq \gamma \mu^{d+i-1} \tag{411}$$

for all $i \geq 1$ with two exceptions for $i = 2$: namely if $I = \langle xw, yw \rangle$ or $I = \langle xw, yw, z \rangle$ where $x, y \in \mathfrak{p}$ is P-regular, where $w \in P$, and where $z \in \mathfrak{p}^2$ is $P/\langle xw, yw \rangle$-regular. In this case,

$$\mu^{d+2} = \mu^{d+1} = 2.$$

If R is Cohen Macaulay, then (411) holds for all i.

103 Fibers

Definition 103.1. Let S be an R-algebra and let $\mathfrak{p}$ be a prime ideal of R. We define the **fiber of** S **over** $\mathfrak{p}$ to be the $\kappa(\mathfrak{p})$-algebra $\kappa(\mathfrak{p}) \otimes_R S = S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ where $\kappa(\mathfrak{p}) = K(R/\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$ denotes the quotient field of $R/\mathfrak{p}$. In particular, if $\mathfrak{m}$ is a maximal ideal of R, then the fiber of S over $\mathfrak{m}$ is the $R/\mathfrak{m}$-algebra $S/\mathfrak{m}S$. If R is an integral domain with fraction field K, then **generic fiber of** S is the K-algebra $K \otimes_R S$.

Remark 137. Let $\iota\colon A \to B$ be an inclusion of $\mathbb{k}$-algebras where $\mathbb{k}$ is a field. Geometrically speaking, the inclusion map $\iota\colon A \to B$ of $\mathbb{k}$-algebras corresponds to the morphism $\pi\colon Y \to X$ of affine $\mathbb{k}$-schemes, where $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, and where π is defined by

$$\pi(\mathfrak{q}) = A \cap \mathfrak{q}$$

for all primes $\mathfrak{q}$ of B. If $\iota\colon A \to B$ is an integral extension, then π is surjective (this is referred to as the **lying over** property for integral extensions). Note that π is continuous with respect to the Zariski topology, for if $U := \mathrm{D}(a)$ is an open subset of X where $a \in A$, then

$$\pi^{-1}(U) = \pi^{-1}(\mathrm{D}(a)) = \mathrm{D}(\iota(a)) := V.$$

In other words, we have $a \notin A \cap \mathfrak{q}$ if and only if $a \notin \mathfrak{q}$ for all primes $\mathfrak{q}$ of B. Now, given a prime $\mathfrak{p}$ of A, the fiber of $\pi\colon Y \to X$ over $\mathfrak{p}$, denoted $Y_{\mathfrak{p}}$, is the pullback of $\pi\colon Y \to X$ with respect to the morphism $\varepsilon_{\mathfrak{p}}\colon \operatorname{Spec}(\kappa(\mathfrak{p})) \to X$ where $\varepsilon_{\mathfrak{p}}$ is the morphism which corresponds to the $\mathbb{k}$-algebra homomorphism $A \to \kappa(\mathfrak{p})$. In particular, $Y_{\mathfrak{p}}$ is an affine $\mathbb{k}$-scheme and the $\mathbb{k}$-algebra which corresponds to $Y_{\mathfrak{p}}$ is $\kappa(\mathfrak{p}) \otimes_A B$, which is precisely how we defined the fiber of B over $\mathfrak{p}$ in the first place.

Example 103.1. Let $R = \mathbb{k}[\boldsymbol{a}] = \mathbb{k}[a_1, a_2, a_3]$ and let $S = R[\boldsymbol{x}]/f = R[x_1, x_2]/f$ where $f = a_1x_1^2 + a_2x_1x_2 + a_3x_2^2$. Also for $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{k}^3$, we set

$$\mathfrak{m}_{\boldsymbol{\alpha}} = \langle a_1 - \alpha_1, a_2 - \alpha_2, a_3 - \alpha_3 \rangle \quad \text{and} \quad f_{\boldsymbol{\alpha}} = \alpha_1x_1^2 + \alpha_2x_1x_2 + \alpha_3x_2^2.$$

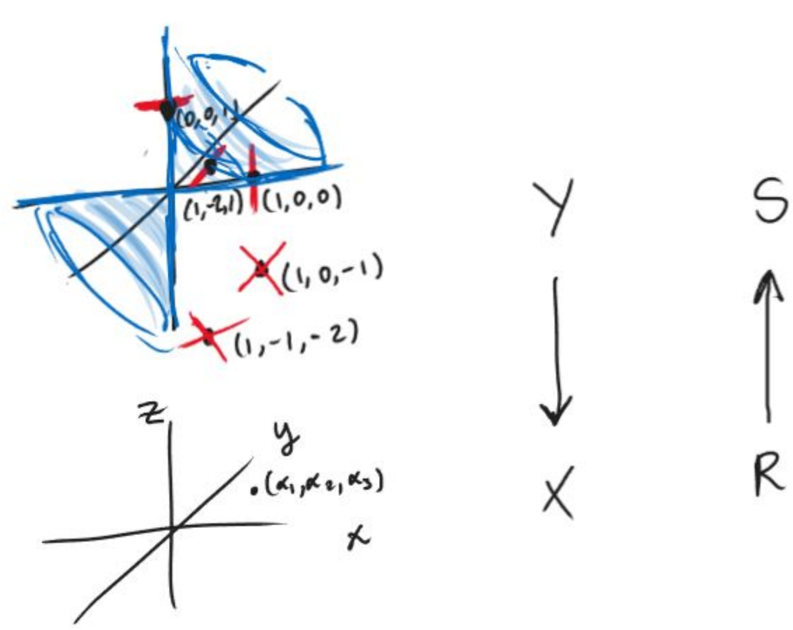
Then the fiber of S over $\mathfrak{m}_{\boldsymbol{\alpha}}$ is the $\mathbb{k}$-algebra $S_{\boldsymbol{\alpha}} := \mathbb{k}[\boldsymbol{x}]/f_{\boldsymbol{\alpha}}$. Geometrically speaking, the inclusion map $\iota\colon R \to S$ of $\mathbb{k}$-algebras corresponds to the projection $\pi\colon Y \to X$ of affine $\mathbb{k}$-schemes, where $X = \operatorname{Spec} R$ and $Y = \operatorname{Spec} S$. Then the fiber of π over $\mathfrak{m}_{\boldsymbol{\alpha}}$ is given by

$$\pi^{-1}(\{\mathfrak{m}_{\boldsymbol{\alpha}}\}) = \mathrm{V}(f_{\boldsymbol{\alpha}}) = \operatorname{Spec}(S_{\boldsymbol{\alpha}}).$$

Notice that $f_{\boldsymbol{\alpha}}$ will always factor in a splitting field as

$$f_{\boldsymbol{\alpha}} = (x_1 + (\alpha_2 + \beta)x_2)(x_1 + (\alpha_2 - \beta)x_2),$$

where we set $\beta = \frac{1}{2\alpha_1}\sqrt{\alpha_2^2 - 4\alpha_1\alpha_3}$. In particular, if $\mathbb{k}$ is algebraically closed, then the fiber is either a union of two lines or a double line. It is a double line exactly when $\alpha_2^2 = 4\alpha_1\alpha_3$. In other words, the fiber over $\mathfrak{m}_{\boldsymbol{\alpha}}$ is a double line if and only if $\boldsymbol{\alpha}$ belongs to the double cone $Z = \mathrm{V}(a_1^2 - 4a_1a_3) \subseteq X$. In the image below, we attempted to draw how the situation looks geometrically:



The blue shape is the double cone given by

Example 103.2. Let $R = \Bbbk[t]$, let $S = R[x]/\langle x^2 - t\rangle$, and let $\mathfrak{p}_\tau = \langle t - \tau\rangle$ where $\tau \in \Bbbk$. Then for $\tau \neq 0$, the fiber of S over $\mathfrak{p}_\tau$ is $\Bbbk[x]/\langle x^2 - \tau\rangle \cong \Bbbk \times \Bbbk$. The fiber over $\mathfrak{p}_0$ is $S_0 := \Bbbk[x]/\langle x^2\rangle$. Finally, the fiber over the zero ideal $\langle 0\rangle$ is $\Bbbk(t)[x]/\langle x^2 - t\rangle$, a field of degree 2 over the residue field $\kappa(\langle 0\rangle) = \Bbbk(t)$. We see that for each prime $\mathfrak{p}$, the fiber over $\mathfrak{p}$ is a vector space of dimension 2 over its residue field $\kappa(\mathfrak{p})$. In fact, S is a free R-module on the generators $(1, x)$. Thus $S \otimes_R N = N \oplus N$ for any R-module N, and it follows that S is flat.

Proposition 103.1. *Let $\varphi\colon A \to B$ be a ring homomorphism and let $\mathfrak{p}$ be a prime ideal of A. Let $f\colon Y \to X$ be the corresponding map of affine schemes where $Y = \operatorname{Spec} A$ and $X = \operatorname{Spec} B$. Then $\mathfrak{p}$ is in the image of f if and only if the fiber of B over $\mathfrak{p}$ is nonzero.*

Proof. First note that if $\mathfrak{q}$ is a prime of B that lies over $\mathfrak{p}$, then $\mathfrak{q}_\mathfrak{q}$ is a prime of $B_\mathfrak{q}$ that lies over $\mathfrak{p}_\mathfrak{p}$. Conversely, if $\mathfrak{r}$ is a prime of $B_\mathfrak{q}$ that lies over $\mathfrak{p}_\mathfrak{p}$, then it must have the form $\mathfrak{r} = \mathfrak{q}_\mathfrak{p}$ for some prime $\mathfrak{q}$ of B. Thus, by localizing at $\mathfrak{p}$ if necessary, we may assume that $A = (A, \mathfrak{p}, \Bbbk)$ is a local ring. Now if $\mathfrak{q}$ if a prime of B that lies over $\mathfrak{p}$, then $\overline{\mathfrak{q}} := \mathfrak{q}/\mathfrak{p}B$ is a prime of $\overline{B} := B/\mathfrak{p}B$ which implies $\overline{B}$ is nonzero. Conversely, if $\overline{B} \neq 0$, then there exists a prime $\mathfrak{r}$ of $\overline{B}$, which must have the form $\mathfrak{r} = \overline{\mathfrak{q}} := \mathfrak{q}/\mathfrak{p}B$ for some prime $\mathfrak{q}$ of B which necessarily lies over $\mathfrak{p}$. □

Proposition 103.2. *Let $\varphi\colon A \to B$ be a flat ring homomorphism and let $f\colon Y \to X$ be the corresponding map of affine schemes where $Y = \operatorname{Spec} B$ and $X = \operatorname{Spec} A$. Then φ is faithfully flat if and only if f is surjective.*

Proof. Suppose M is a nonzero A-module. Let $\mathfrak{p} \in \operatorname{Supp} M$, so $M_\mathfrak{p} \neq 0$. □

104 Hochschild Homology

Let A be a $\Bbbk$-algebra and let M be an A-bimodule. We set $A^{\mathrm{e}} = A \otimes_\Bbbk A^{\mathrm{o}}$ to be the **enveloping algebra** of A over $\Bbbk$ where A^{o} is the opposite algebra of A. In particular, we have

$$(a_1 \otimes a_2)(a_1' \otimes a_2') = a_1 a_1' \otimes a_2' a_2$$

for all $a_1, a_2 \in A$. In this case, note that the action

$$(a_1 \otimes a_2)m = a_1 m a_2 = m(a_1 \otimes a_2)$$

gives M and A^{e}-module structure. Indeed, we have

$$\begin{aligned}(a_1 \otimes a_2)((a_1' \otimes a_2')m) &= a_1 \otimes a_2(a_1' m a_2') \\ &= a_1 a_1' m a_2' a_2 \\ &= (a_1 a_1' \otimes a_2' a_2)m \\ &= ((a_1 \otimes a_2)(a_1' \otimes a_2'))m.\end{aligned}$$

Thus A-bimodules are essentially the same as A^{e}-modules. In particular, it makes sense to consider the following definitions:

Definition 104.1. The ith **Hochschild homology** of A with coefficients in M is

$$\mathrm{HH}_i(A, M) := \mathrm{Tor}_i^{A^{\mathrm{e}}}(A, M),$$

and the ith **Hochschild cohomology** of A with coefficients in M is

$$\mathrm{HH}^i(A, M) = \mathrm{Ext}^i_{A^{\mathrm{e}}}(A, M).$$

Now suppose that $\Bbbk$ is a ring and that A is an associative $\Bbbk$-algebra which is projective as a $\Bbbk$-module. We define the **Hochschild complex** $C = \mathrm{C}(A, M)$ of A with coefficients in M to be the A^{e}-complex whose component in homological degree n is $C_n = M \otimes_\Bbbk A^{\otimes_\Bbbk n}$ and whose differential is defined by

$$\partial(m \otimes a_1 \otimes \cdots \otimes a_n) = ma_1 \otimes \cdots \otimes a_n + \sum_{i=1}^{n-1} (-1)^i m \otimes a_1 \otimes \cdots \otimes a_i a_{i+1} \otimes \cdots \otimes a_n + (-1)^n a_n m \otimes \cdots \otimes a_{n-1}.$$

One has $\mathrm{HH}(A, M) = \mathrm{H}(\mathrm{C}(A, M))$.

Example 104.1. In homological degree $n = 1$, we have $\partial_1(a_1 \otimes a_2) = a_1 a_2 - a_2 a_1 = [a_1, a_2]$. Thus

$$\mathrm{HH}_0(A/\Bbbk) = A \otimes_{A^{\mathrm{e}}} A = A/[A, A].$$

In particular, if A is commutative, then $\mathrm{HH}_0(A/\Bbbk) = A$. Furthermore, if A is commutative, then

$$\mathrm{HH}_1(A/\Bbbk) = (A \otimes_\Bbbk A)/\langle\{a_1 a_2 \otimes a_3 - a_1 \otimes a_2 a_3 + a_3 a_1 \otimes a_2 \mid a_1, a_2, a_3 \in A\}\rangle.$$

Note that we are quotienting out by the Leibniz law, so we have an isomorphism of A-modules

$$\mathrm{HH}_1(A/\Bbbk) \xrightarrow{\simeq} \Omega^1_{A/\Bbbk}$$

given by $a_1 \otimes a_2 \mapsto a_1 \mathrm{d} a_2$.

Example 104.2. If $A = \Bbbk$, then the boundary maps in the Hochschild complex are alternately zero and the identity, hence

$$\mathrm{HH}_i(\Bbbk/\Bbbk) = \begin{cases} \Bbbk & \text{if } i = 0 \\ 0 & \text{if } i > 0 \end{cases}$$

The higher Hochschild homology groups vanish more generally whenever A is a commutative étale $\Bbbk$-algebra.

104.1 The Bar Complex

We construct a projective resolution of A over A^{e}. The component in homological degree n is given by $B_n = A^{\otimes_{\Bbbk}(n+2)}$ and the differential is defined by

$$\partial(a_1 \otimes \cdots \otimes a_m) = \sum_{i=2}^{m} (-1)^i a_1 \otimes \cdots \otimes a_{i-1} a_i \otimes \cdots \otimes a_m.$$

The map $\varepsilon \colon B \to A$ given by $\varepsilon(a_1 \otimes a_2) = a_1 a_2$ and $\varepsilon_i = 0$ for all $i \geq 0$ is a quasi-isomorphism. Indeed, the map $h \colon B \to B$ given by

$$h(a_1 \otimes \cdots \otimes a_m) = 1 \otimes a_1 \otimes \cdots \otimes a_m$$

is easily seen to be a null-homotopy of the identity map. Note that B is an A^{e}-module via the rule

$$(a_1 \otimes a_2)(a_1' \otimes a_2' \otimes \cdots \otimes a_{m-1}' \otimes a_m') = a_1 a_1' \otimes a_2' \otimes \cdots \otimes a_{m-1}' \otimes a_m' a_2.$$

Furthermore B is flat since A is flat over $\Bbbk$. We have an isomorphism of complexes

$$A \otimes_{A^{\mathrm{e}}} B \simeq C$$

105 Koszul Homology

Let R be a ring and let $\boldsymbol{r} = r_1, \ldots, r_m$ be a sequence of elements in R.

1. The Koszul algebra $\mathbb{K} = \mathcal{K}(\boldsymbol{r})$ is defined to be the R-complex whose underlying graded R-module is given by

$$\mathbb{K} = \bigoplus_{\sigma \subseteq \{1 \ldots, m\}} e_\sigma R,$$

where we use the notation $e_\sigma = \prod_{i \in \sigma} e_i$ and where e_σ is homogeneous with $|e_\sigma| = \#\sigma$. The differential d of E is defined on the homogeneous basis by $\mathrm{d} e_i = r_i$ and extended everywhere else using the Leibniz law. In particular, we have

$$\mathrm{d} e_\sigma = \sum_{i \in \sigma} (-1)^{\mathrm{pos}(i,\sigma)} r_i e_{\sigma \setminus i}.$$

For example, we haveFor example, if $m = 3$ then we have

$$\begin{array}{llll} & \mathrm{d}e_1 = r_1 & \mathrm{d}e_{23} = e_3 r_2 - e_2 r_3 & \\ \mathrm{d}(1) = 0 & \mathrm{d}e_2 = r_2 & \mathrm{d}e_{13} = e_3 r_1 - e_1 r_3 & \mathrm{d}e_{123} = e_{23} r_1 - e_{13} r_2 + e_{12} r_3 \\ & \mathrm{d}e_3 = r_3 & \mathrm{d}e_{12} = e_2 r_1 - e_1 r_2 & \end{array}$$

An alternative description of $\mathbb{K}$ is the the iterated tensor product of complexes:

$$\mathbb{K}(\boldsymbol{r}) \simeq \mathbb{K}(r_1) \otimes_R \mathbb{K}(r_2) \otimes_R \cdots \otimes_R \mathbb{K}(r_m).$$

If M is an R-module, then we set $\mathbb{K}(\boldsymbol{r}, M) := \mathbb{K} \otimes_R M$ and we denote its homology by $\mathrm{H}(\boldsymbol{x}, M)$.

2. Another Koszul complex we are interested in is called the **dual Koszul complex**: it is given by $\mathbb{K}^\star := \mathrm{Hom}^\star_R(\mathbb{K}, R)$. The underlying graded R-module is given by

$$\mathbb{K}^\star = \bigoplus_{\sigma \subseteq \{1,\dots,m\}} Re^\star_\sigma.$$

Here $e^\star_\sigma \colon E \to R$ is an R-linear map, graded of degree $-(\#\sigma)$, which is defined by

$$e^\star_\sigma(e_\tau) = \begin{cases} 1 & \text{if } \sigma = \tau \\ 0 & \text{else} \end{cases}$$

The differential $\mathrm{d}^\star$ of $E^\star$ is defined by $\mathrm{d}^\star e^\star_\sigma = e^\star_\sigma \mathrm{d}$. In particular, we have

$$\mathrm{d}^\star e^\star_\sigma = (-1)^{\#\sigma+1} \sum_{i \in \sigma^\star} (-1)^{\mathrm{pos}(i,\sigma^\star)} r_i e^\star_{\sigma \cup i},$$

where $\sigma^\star := \{1,\dots,m\} \backslash \sigma$. For example, if $m = 3$ then we have

$$\begin{array}{llll} & \mathrm{d}^\star e^\star_1 = r_3 e^\star_{13} + r_2 e^\star_{12} & \mathrm{d}^\star e^\star_{23} = r_1 e^\star_{123} & \\ \mathrm{d}^\star(1) = -r_1 e^\star_1 - r_2 e^\star_2 - r_3 e^\star_3 & \mathrm{d}^\star e^\star_2 = r_3 e^\star_{23} - r_1 e^\star_{12} & \mathrm{d}^\star e^\star_{13} = -r_2 e^\star_{123} & \mathrm{d}^\star e^\star_{123} = 0 \\ & \mathrm{d}^\star e^\star_3 = -r_2 e^\star_{23} - r_1 e^\star_{13} & \mathrm{d}^\star e^\star_{12} = r_3 e^\star_{123} & \end{array}$$

Note that the nonzero components of $E^\star$ live in negative homological degree, that is, if $0 < k < m$, then $E^\star_k = 0$ and $E^\star_{-k} \neq 0$. We often think of $E^\star$ as a cochain complex using the upper sign convention $E^\star_{-k} = E^{\star,k}$ and $\mathrm{d}^\star_{-k} = \mathrm{d}^{\star,k}$. Note that the map $\varphi \colon \Sigma^n \mathbb{K}^\star \to \mathbb{K}$ defined by

$$\varphi(e^\star_\sigma) = \mathrm{sign}(\sigma^\star, \sigma) e_{\sigma^\star}$$

is an isomorphism of R-complexes. In particular we obtain $\mathrm{H}_i(\mathbb{K}) \simeq \mathrm{H}_{i-m}(\mathbb{K}^\star)$.

3. The **stable Koszul complex** $\widetilde{\mathbb{K}}$ is complex whose underlying graded R-module is given by

$$\widetilde{\mathbb{K}} = \bigoplus_{\sigma \subseteq \{1,\dots,m\}} \widetilde{e}_\sigma R_{r_\sigma}$$

For example, if $m = 3$ then we have

$$\begin{array}{llll} & \widetilde{\mathrm{d}}\widetilde{e}_1 = \widetilde{e}_{13} - \widetilde{e}_{12} & \widetilde{\mathrm{d}}\widetilde{e}_{23} = \widetilde{e}_{123} & \\ \widetilde{\mathrm{d}}(1) = \widetilde{e}_1 + \widetilde{e}_2 + \widetilde{e}_3 & \widetilde{\mathrm{d}}\widetilde{e}_2 = \widetilde{e}_{23} - \widetilde{e}_{12} & \widetilde{\mathrm{d}}e_{13} = -\widetilde{e}_{123} & \widetilde{\mathrm{d}}\widetilde{e}_{123} = 0 \\ & \widetilde{\mathrm{d}}\widetilde{e}_3 = \widetilde{e}_{23} - \widetilde{e}_{13} & \widetilde{\mathrm{d}}\widetilde{e}_{12} = \widetilde{e}_{123} & \end{array}$$

Observe that

$$\widetilde{\mathbb{K}} = \varinjlim \mathbb{K}^\star(\boldsymbol{r}^n),$$

where $\boldsymbol{r}^n = r_1^n, \dots, r_m^n$. In particular, it follows that

$$\mathrm{H}(\boldsymbol{r}^\infty, M) = \bigcup_{n \geq 0} \mathrm{H}(\boldsymbol{r}^n, M) = \varinjlim \mathrm{H}(\boldsymbol{r}^n, M).$$

106 Massey Triple Products

Definition 106.1. Let A be a DG algebra and let $H = \mathrm{H}(A)$ be its homology. The **Massey triple product** of $\overline{a}_1, \overline{a}_2, \overline{a}_3 \in H$ is defined by

$$\langle \overline{a}_1, \overline{a}_2, \overline{a}_3 \rangle = \{\overline{a_{1,2}a_3 - a_1 a_{2,3}} \mid \mathrm{d}a_{1,2} = a_1 a_2 \text{ and } \mathrm{d}a_{2,3} = (-1)^{|a_1|} a_2 a_3\}.$$

Note that $a_{1,2}a_3 - a_1 a_{2,3}$ represents an element in H since

$$\mathrm{d}(a_{1,2}a_3 - a_1 a_{2,3}) = [a_1, a_2, a_3] = 0.$$

Note also that if either $\overline{a}_1\overline{a}_2 \neq 0$ or $\overline{a}_2\overline{a}_3 \neq 0$, then $\langle \overline{a}_1, \overline{a}_2, \overline{a}_3 \rangle = \emptyset$. If $\overline{a}_1\overline{a}_2 = 0 = \overline{a}_2\overline{a}_3$ then every element in $\langle \overline{a}_1, \overline{a}_2, \overline{a}_3 \rangle$ represents the same element in the quotient group

$$H / \langle H\overline{a}_3 + \overline{a}_1 H \rangle.$$

So the Massey product can be regarded as a function defined on triples of classes such that the product of the first or last two is zero, taking values in the above quotient group.

Indeed, suppose $b_1 = a_1 + \mathrm{d}x_1$ and $b_2 = a_2 + \mathrm{d}x_2$, and suppose that $\mathrm{d}b_{1,2} = b_1 b_2$. Then we have

$$\begin{aligned} b_{1,2}b_3 - a_{1,2}a_3 &= b_{1,2}a_3 + b_{1,2}\mathrm{d}x_3 - a_{1,2}a_3 \\ &= (b_{1,2} - a_{1,2})a_3 + b_{1,2}\mathrm{d}x_3 \\ &\equiv (b_{1,2} - a_{1,2})a_3 \text{ in } H, \end{aligned}$$

and note that

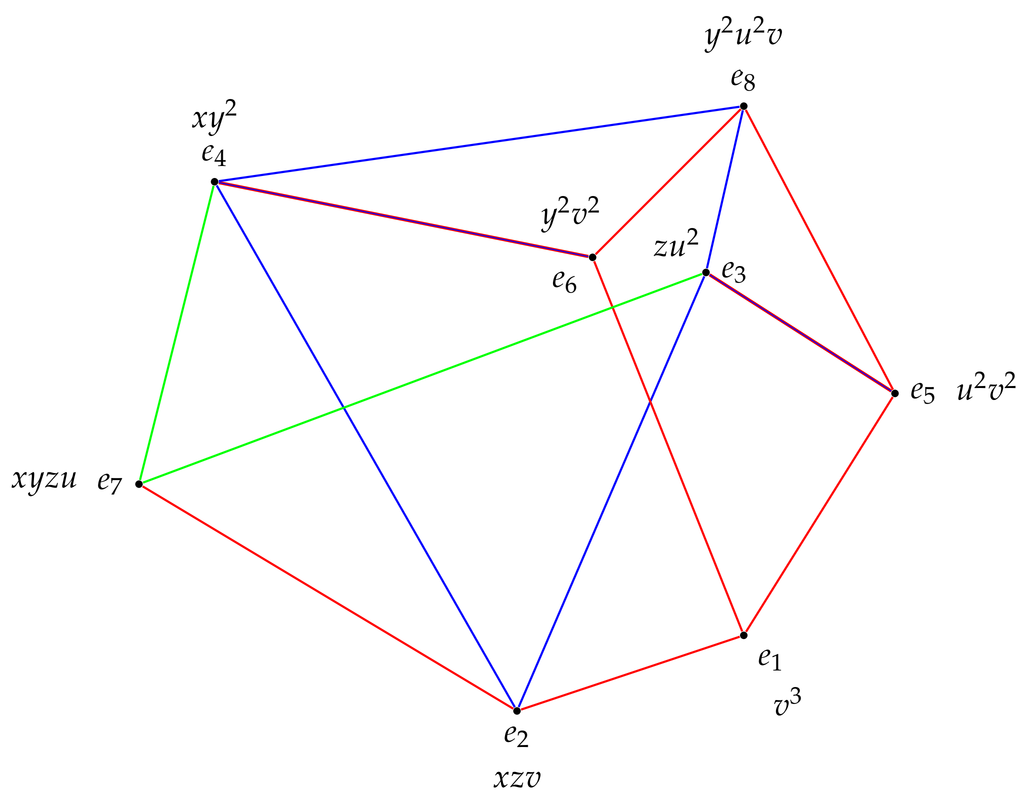
$$\begin{aligned} \mathrm{d}(b_{1,2} - a_{1,2}) &= b_1 b_2 - a_1 a_2 \\ &= a_1(\mathrm{d}x_2) + (\mathrm{d}x_1)a_2 + (\mathrm{d}x_1)(\mathrm{d}x_2) \\ &= \mathrm{d}(a_1 x_2 + x_1 a_2 + x_1(\mathrm{d}x_2)) \end{aligned}$$

Therefore we have

$$\begin{aligned} b_{1,2}b_3 - b_1 b_{2,3} - a_{1,2}a_3 + a_1 a_{2,3} &= b_{1,2}(a_3 + \mathrm{d}x_3) - (a_1 + \mathrm{d}x_1)b_{2,3} - a_{1,2}a_3 + a_1 a_{2,3} \\ &= (b_{1,2} - a_{1,2})a_3 + a_1(a_{2,3} - b_{2,3}) + b_{1,2}\mathrm{d}x_3 - \mathrm{d}x_1 b_{2,3} \\ &\equiv \end{aligned}$$

Assume $|a|$ is odd. ThenThen

Example 106.1. (Katthän) Let $R = \Bbbk[x, y, z, u, v]$, let $\boldsymbol{m} = v^3, xzv, zu^2, xy^2, u^2v^2, y^2v^2, xyzu, y^2u^2v$, and let F be the minimal free resolution of $R/\boldsymbol{m}$ over R. One can visualize F as being supported on the $\boldsymbol{m}$-labeled cellular complex below:



Let T be the Taylor algebra resolution of $R/\boldsymbol{m}$ over R and let $A = T \otimes_R \Bbbk$. We compute Massey triple products in $\mathrm{H}(T_{\Bbbk}) \simeq F_{\Bbbk}$. We claim that $\langle \bar{e}_1, \bar{e}_3, \bar{e}_4 \rangle$ contains a nonzero element. Indeed, let $e_{1,3} = e_{135}$ and $e_{3,4} = e_{347}$. Note that $\mathrm{d}e_{135} = e_1 e_3$ and $\mathrm{d}e_{347} = e_3 e_4$ so $\overline{e_{1,3}e_4 - e_1 e_{3,4}}$ is an element in $\langle \bar{e}_1, \bar{e}_3, \bar{e}_4 \rangle$. We claim that $\overline{e_{1,3}e_4 - e_1 e_{3,4}} \neq 0$. First we observe that

$$\begin{aligned} e_{1,3}e_4 - e_1 e_{3,4} &= e_{135}e_4 - e_1 e_{347} \\ &= e_{1345} - e_{1347} \\ &= \mathrm{d}e_{13457} + e_{3457}. \end{aligned}$$

Now observe that in F we have

$$\begin{aligned} [e_1, e_3, e_4]_\mu &= (e_1 \star e_3) \star e_4 - e_1 \star (e_3 \star e_4) \\ &= \mathrm{d}(e_{1234567}). \end{aligned}$$

Example 106.2. (Avromov) Let $R = \Bbbk[x, y, z, w]$, let $\boldsymbol{m}' = x^2, w^2$, and let $\boldsymbol{m} = x^2, w^2, zw, xy, yz$. Let E be the Koszul algebra resolution of $R/\boldsymbol{m}'$ over R and let T be the Taylor algebra resolution of $R/\boldsymbol{m}$ over R. The homogeneous basis of T as a graded R-module is denoted $\{\varepsilon_\sigma\}$. We may view E as the R-subalgebra of T given by

$$E = R \oplus R\varepsilon_1 \oplus R\varepsilon_2 \oplus R\varepsilon_{12}.$$

We set $E_\Bbbk = E \otimes_R \Bbbk$ and $T_\Bbbk = T \otimes_R \Bbbk$ and we remark that $\mathrm{H}E_\Bbbk = \mathrm{Tor}^R(R/\boldsymbol{m}', \Bbbk)$ and $\mathrm{H}T_\Bbbk = \mathrm{Tor}^R(R/\boldsymbol{m}, \Bbbk)$. Define $h\colon T_\Bbbk \otimes_\Bbbk T_\Bbbk \to T_\Bbbk$ by $h(x\varepsilon_1 \otimes z\varepsilon_3) = x\varepsilon_{123}$ and zero on all other $\Bbbk$-basis elements. Then we have

$$[x\varepsilon_1, z\varepsilon_3, w\varepsilon_4]_{\mu,h} = xw\varepsilon_{1234}.$$

In particular, $\langle \overline{x\varepsilon_1}, \overline{z\varepsilon_3}, \overline{w\varepsilon_4} \rangle$ contains the element $\overline{xw\varepsilon_{1234}}$.

107 Multiplicity and Koszul Homology

Lemma 107.1. *Let M be a finitely generated R-module and let I be an ideal of R. Then*

$$\sqrt{\mathrm{Ann}(M/IM)} = \sqrt{\langle I, \mathrm{Ann}\, M \rangle}.$$

Proof. To prove the equality on radicals, it suffices to show that a prime $\mathfrak{p}$ of R contains $\mathrm{Ann}(M/IM)$ if and only if it contains $\langle I, \mathrm{Ann}\, M\rangle$. Recall that for any finitely generated R-module N, we have $\mathrm{V}(\mathrm{Ann}\, N) = \mathrm{Supp}\, N$, or equivalently, $\mathfrak{p} \supseteq \mathrm{Ann}\, N$ if and only if $N_\mathfrak{p} \neq 0$. Thus since M is finitely generated (and hence M/IM is finitely generated too), we have

$$\begin{aligned} \mathfrak{p} \supseteq \mathrm{Ann}(M/IM) &\iff M_\mathfrak{p}/I_\mathfrak{p} M_\mathfrak{p} \neq 0 \\ &\iff M_\mathfrak{p} \neq 0 \text{ and } I_\mathfrak{p} \subseteq \mathfrak{p}_\mathfrak{p} \\ &\iff \mathfrak{p} \supseteq \mathrm{Ann}\, M \text{ and } I \subseteq \mathfrak{p} \\ &\iff \mathfrak{p} \supseteq \langle \mathrm{Ann}\, M, I \rangle \end{aligned}$$

□

Let $A = (A, \mathfrak{m}, \Bbbk)$ be a noetherian local ring, let $\boldsymbol{x} = x_1, \dots, x_r$ be a sequence contained in $\mathfrak{m}$, and let M be a finitely generated A-module such that $\ell(M/\boldsymbol{x}M) < \infty$ (equivalently, we have $\mathfrak{m} = \sqrt{\mathrm{Ann}(M/\boldsymbol{x}M)}$). We set $K = K(\boldsymbol{x}, M)$ to be koszul complex with respect to $\boldsymbol{x}$ and M and we denote its homology by $\mathrm{H}(\boldsymbol{x}, M)$. Recall that the A-module $\mathrm{H}_i(\boldsymbol{x}, M)$ is finitely generated and annihilated by $\langle \boldsymbol{x}, \mathrm{Ann}\, M\rangle$, hence they have finite length (indeed, we have $\mathfrak{m} = \sqrt{\mathrm{Ann}(M/\boldsymbol{x}M)} = \sqrt{\langle \boldsymbol{x}, \mathrm{Ann}\, M\rangle}$). We may therefore define the **Euler-Poincare characteristic**

$$\chi(\boldsymbol{x}, M) = \sum_{i=0}^{r} (-1)^i \ell(\mathrm{H}_i(\boldsymbol{x}, M)).$$

On the other hand, we the Hilbert-Samuel polynomial $P_{\boldsymbol{x}}(M)$ has degree $\leq r$, and we have

$$P_{\boldsymbol{x}}(M, n) = \mathrm{e}_{\boldsymbol{x}}(M, r)\frac{n^r}{r!} + Q(n)$$

with $\deg Q < r$ and where $\mathrm{e}_{\boldsymbol{x}}(M, r) = \Delta^r P_{\boldsymbol{x}}(M)$ is the Hilbert-Samuel multiplicity.

Theorem 107.2. *We have $\chi(\boldsymbol{x}, M) = \mathrm{e}_{\boldsymbol{x}}(M, r)$.*

Proof. We prove this in several steps:

Step 1: To ease notation in what follows, we set $Q = \langle \boldsymbol{x} \rangle$. We first equip A with the standard Q-filtration $A = (Q^n)$ and view it as a filtered ring. Similarly, we equip M with the Q-filtration $M = (Q^n M)$ and view it as a filtered A-module. We now equip K with a Q-filtration as follows: for each $n \in \mathbb{N}$, let K^n be the R-subcomplex of K whose component in homological degree i

$$K_i^n = \begin{cases} Q^{n-i}K_i. & \text{if } 0 \leq i < n \\ K_i & \text{else} \end{cases}$$

Thus for example, we have

$$\begin{aligned} K^0 &= M + \sum Me_i + \sum Me_{i,j} + \cdots \\ K^1 &= QM + \sum Me_i + \sum Me_{i,j} + \cdots \\ K^2 &= Q^2M + \sum QMe_i + \sum Me_{i,j} + \cdots \\ &\vdots \end{aligned}$$

Notice that

$$\begin{aligned}
K^0/K^1 &= M/QM \\
K^1/K^2 &= QM/Q^2M + \sum (M/QM)e_i \\
K^2/K^3 &= Q^2M/Q^3M + \sum (QM/Q^2M)e_i + \sum (M/QM)e_{i,j} \\
&\vdots
\end{aligned}$$

In particular, we clearly have

$$\begin{aligned}
\mathrm{gr}(K) &= \bigoplus_{n=0}^{\infty} K^n/K^{n+1} \\
&= \mathrm{gr}(M) + \sum \mathrm{gr}(M)e_i + \sum \mathrm{gr}(M)e_{i,j} \\
&= K(\boldsymbol{x}, \mathrm{gr}(M)).
\end{aligned}$$

Finally, we have

$$\begin{aligned}
\chi(\boldsymbol{x}, M) &= \sum_{i=0}^{r} (-1)^i \ell(\mathrm{H}_i(\boldsymbol{x}, M)) \\
&= \sum_{i=0}^{r} (-1)^i \ell(\mathrm{H}_i(K/K^n)) \\
&= \sum (-1)^i \ell(K_i/K_i^n) \\
&= \sum (-1)^i \ell\left(\bigoplus_{\binom{r}{i}} M/\boldsymbol{x}^{n-i}M \right) \\
&= \sum (-1)^i \binom{r}{i} \ell(M/\boldsymbol{x}^{n-i}M) \\
&= \mathrm{e}_{\boldsymbol{x}}(M, r).
\end{aligned}$$

□

107.1 Extra

Let $(R, \mathfrak{m}, \Bbbk)$ be a local noetherian ring, let M be a nonzero finitely generated R-module of dimension d, and let $\boldsymbol{x} = x_1, \dots, x_d$ be a system of parameters for M. By definition, this means $\boldsymbol{x}$ is a sequence contained in $\mathfrak{m}$ such that $M/\boldsymbol{x}M$ has finite length, or equivalently, such that

$$\mathfrak{m} = \sqrt{\langle \mathrm{Ann}(M/\boldsymbol{x}M) \rangle} = \sqrt{Q},$$

where $Q = \langle \boldsymbol{x}, \mathrm{Ann}\, M \rangle$. There's a beautiful formula due to Auslander and Buchsbaum which expresses the Hilbert multiplicity of M with respect to $\boldsymbol{x}$ as an Euler characteristic of the Koszul homology $\mathrm{H}(\boldsymbol{x}, M)$. To explain this, first let's recall how the Hilbert multiplicity of M with respect to $\boldsymbol{x}$ is defined: let (M_n) be any stable Q-filtration of M (for example, we can pick $M_n = \langle \boldsymbol{x} \rangle^n M = Q^n M$). Then the Hilbert-Samuel function with respect (M_n) is the function $f_{(M_n)} = f \colon \mathbb{N} \to \mathbb{N}$ defined by

$$f(n) = \ell_R(M/M_n) = \sum_{i=0}^{n-1} \ell_{R/Q}(M_i/M_{i+1}).$$

For n sufficiently large, we have $f(n) = P(n)$ where $P = P_{\boldsymbol{x},M}$ is a polynomial whose lead term is $(e/d!)n^d$. Here, $e = e(\boldsymbol{x}, M)$ is called the **Hilbert multiplicity** of M with respect to $\boldsymbol{x}$. It depends on the choice of Q (which itself depends on the choice of $\boldsymbol{x}$ assuming M is fixed), however it doesn't depend on the choice of stable Q-filtration (M_n).

On the other hand, the Euler-Poincare characteristic with respect to $\boldsymbol{x}$ and M is the alternating sum:

$$\chi(\boldsymbol{x}, M) = \sum_{i=0}^{\infty} (-1)^i \ell_{R/Q}(\mathrm{H}_i(\boldsymbol{x}, M)) = \sum_{i=0}^{d} (-1)^i \ell_{R/Q}(\mathrm{H}_i(\boldsymbol{x}, M)), \tag{412}$$

where $\mathrm{H}(\boldsymbol{x}, M)$ is the homology of the Koszul complex $E := \mathcal{K}(\boldsymbol{x}, M) = \mathcal{K}(\boldsymbol{x}) \otimes_R M$. Note that if $\boldsymbol{x}$ is an R-sequence, then we have

$$\mathrm{H}(\boldsymbol{x}, M) = \mathrm{Tor}_R(R/\boldsymbol{x}, M)$$

since $\mathcal{K}(\boldsymbol{x})$ is an free resolution of $R/\boldsymbol{x}$ over R in this case. So if $\boldsymbol{x}$ is an R-sequence, then we can re-express (412) as

$$\chi(\boldsymbol{x}, M) = \sum_{i=0}^{\infty}(-1)^i \ell_{R/Q}(\mathrm{Tor}_i^R(R/\boldsymbol{x}, M)).$$

More generally, let $\mathfrak{p}$ and $\mathfrak{q}$ be prime ideals of R and set $I = \mathfrak{p} + \mathfrak{q}$. We define the **intersection multiplicity** of $R/\mathfrak{p}$ and $R/\mathfrak{q}$ to be the quantity:

$$\chi(R/\mathfrak{p}, R/\mathfrak{q}) := \sum_{i=0}^{\infty}(-1)^i \ell_{R/I}(\mathrm{Tor}_i^R(R/\mathfrak{p}, R/\mathfrak{q})).$$

Note that this only makes sense when I is $\mathfrak{m}$-primary. If $\dim(R/\mathfrak{p}) + \dim(R/\mathfrak{q}) = \dim R$, then it is an open conjecture that $\chi(R/I, R/J) > 0$.

In order to see the connection between Hilbert multiplicity and the Euler characteristic, we first extend the Q-stable filtration (M_n) of M to a Q-stable filtration (E^n) of E as follows: for each $n \in \mathbb{N}$ let E^n be the R-subcomplex of E whose component in homological degree i is

$$E_i^n = \begin{cases} M_{n-i}E_i. & \text{if } 0 \leq i < n \\ E_i & \text{else} \end{cases}$$

Thus for example, we have

$$\begin{aligned} E^0 &= M + \sum Me_i + \sum Me_{i,j} + \cdots \\ E^1 &= QM + \sum Me_i + \sum Me_{i,j} + \cdots \\ E^2 &= Q^2M + \sum QMe_i + \sum Me_{i,j} + \cdots \\ &\vdots \end{aligned}$$

and so on. In particular, note that

$$\begin{aligned} \operatorname{gr} E &= \bigoplus_{n=0}^{\infty} E^n/E^{n+1} \\ &= \operatorname{gr} M + \sum(\operatorname{gr} M)e_i + \sum(\operatorname{gr} M)e_{i,j} + \cdots \\ &= \mathcal{K}(\boldsymbol{x}, \operatorname{gr} M). \end{aligned}$$

108 Vanishing Homology in Commutative Algebra

Unless otherwise specified, let $(R, \mathfrak{m}, \Bbbk)$ be a local noetherian ring. Ext and Tor show up all over the place in commutative algebra.
one is often presented with an R-complex A which is homologically bounded above and homologically bounded below, and would like to know *when* does $\mathrm{H}_i(A)$ vanish? In particular, we want to find an $\varepsilon, \delta \in \mathbb{Z}$ such that $\varepsilon \leq \delta$ and

$$\begin{aligned} &\mathrm{H}_\delta(A) \neq 0 \\ &\mathrm{H}_\varepsilon(A) \neq 0 \\ &\mathrm{H}_i(A) = 0 \text{ for all } i < \varepsilon \text{ and } i > \delta. \end{aligned}$$

Vanishing in Ext

109 Shifting and Antishifting

In order to get a better understanding of Ext and Tor, the first step is to understand their shifting/antishifting properties. The lesson that we shall learn is that covariant left exact functors typically satisfy the shift property whereas everything else usually satisfies the antishift property.

109.1 Shifting and Antishifting Depth

109.1.1 Antishift Property of Koszul Homology and Depth

Let R be a noetherian ring, let I be an ideal of R such that $I = \sqrt{\langle x_1, \dots, x_n \rangle} = \sqrt{\langle \boldsymbol{x} \rangle}$ where $x_1, \dots, x_n \in I$, and let N a finitely-generated R-module such that $N \neq IN$. Set $\delta = \sup\{i \in \mathbb{Z} \mid \mathrm{H}_i(\boldsymbol{x}, N) \neq 0\}$ and let y be an N-regular sequence contained in $\langle \boldsymbol{x} \rangle$. Then we have an isomorphism

$$\mathrm{H}_\delta(\boldsymbol{x}, N) \simeq \mathrm{H}_{\delta+1}(\boldsymbol{x}, N/yN) \tag{413}$$

We think of (413) as an **antishift property** of Koszul homology with respect to depth in the sense that δ increases by one when we replace it by $\delta + 1$ whereas the $\langle \boldsymbol{x} \rangle$-depth (and hence I-depth) of N decreases by one when we replace N by N/yN (slogan: homological degree goes up, depth goes down). This antishift property is derived by considering the short exact sequence of R-modules

$$0 \to N \xrightarrow{y} N \to N/yN \to 0.$$

Then applying the right exact Koszul functor $\mathrm{H}(\mathcal{K}(\boldsymbol{x}, -))$ to this short exact sequence and using the fact that y kills $\mathrm{H}(\boldsymbol{x}, N)$, we obtain the short exact sequence of Koszul homologies

$$0 \to \mathrm{H}_i(\boldsymbol{x}, N) \to \mathrm{H}_i(\boldsymbol{x}, N/yN) \to \mathrm{H}_{i-1}(\boldsymbol{x}, N) \to 0$$

for all $i \in \mathbb{Z}$.

109.1.2 Shift Property of Ext and Depth

Let R be a noetherian local ring, let I be an ideal of R, let N be a finitely-generated R-module such that $IN \neq N$, and let M be a finitely generated R-module such that $\mathrm{V}(\mathrm{Ann}\, M) = \mathrm{V}(I)$ (for instance one may take $M = R/I$ or $M = R/\sqrt{I}$). Set $\delta = \inf\{i \in \mathbb{Z} \mid \mathrm{Ext}^i_R(M, N) \neq 0\}$ and let y be an N-regular element contained in $\mathrm{Ann}\, M$. Then we have an isomorphism

$$\mathrm{Ext}^\delta_R(M, N) \simeq \mathrm{Ext}^{\delta-1}_R(M, N/yN). \tag{414}$$

We think of (414) as a **shift property** of Ext with respect to depth in the sense that δ decreases by one when we replace it by $\delta - 1$ whereas the I-depth of the second component also decreases by one when replace N by N/yN. This shift property is derived by considering the short exact sequence of R-modules

$$0 \to N \xrightarrow{y} N \to N/yN \to 0$$

Then applying the left exact covariant functor $\mathrm{Ext}_R(M, -)$ to this short exact sequence and using the fact that y kills $\mathrm{Ext}_R(M, N)$, we obtain the short exact sequence of Ext modules

$$0 \to \mathrm{Ext}^i_R(M, N) \to \mathrm{Ext}^i_R(M, N/yN) \to \mathrm{Ext}^{i+1}_R(M, N) \to 0$$

for all $i \in \mathbb{Z}$.

109.2 Shifting and Antishifting Syzygies

Let us explain what we mean: let M be a finitely generated R-module and let F be the minimal R-free resolution of M. Thus we have an exact sequence:

$$\cdots \longrightarrow F_2 \xrightarrow{\mathrm{d}_2} F_1 \xrightarrow{\mathrm{d}_1} F_0 \xrightarrow{\tau} M \longrightarrow 0 \tag{415}$$

For $i \geq 0$, we define the ith **syzygy** of M, denoted M_i, to be the image of $\mathrm{d}_i \colon F_i \to F_{i-1}$. If R is Gorenstein and M is a maximal Cohen-Macaulay R-module, then we can extend this definition to all $i \in \mathbb{Z}$. Indeed, let F' be the minimal R-free resolution of $M^\star := \mathrm{Hom}_R(M, \omega_R)$. Thus we have an exact sequence:

$$\cdots \longrightarrow F'_2 \xrightarrow{\mathrm{d}'_2} F'_1 \xrightarrow{\mathrm{d}'_1} F'_0 \xrightarrow{\tau'} M^\star \longrightarrow 0 \tag{416}$$

Since $M^\star$ is maximal Cohen-Macaulay, the dual sequence is exact:

$$0 \longrightarrow M^{\star\star} \xrightarrow{(\tau')^\star} F_{-1} \xrightarrow{\mathrm{d}_{-1}} F_{-2} \xrightarrow{\mathrm{d}_{-2}} F_{-3} \longrightarrow \cdots \tag{417}$$

where we set $F_{-i} := (F'_{i-1})^\star$ and $\mathrm{d}_{-i} := (\mathrm{d}'_i)^\star$. Using the fact that M is reflexive, we can splice together (415) and (417) to get the doubly long infinite long exact sequence:

$$\begin{tikzcd} \cdots \arrow[r] & F_2 \arrow[rr, "d_2"] \arrow[dr] & & F_1 \arrow[rr, "d_1"] \arrow[dr] & & F_0 \arrow[rr, "d_0"] \arrow[dr] & & F_{-1} \arrow[rr, "d_{-1}"] \arrow[dr] & & F_{-2} \arrow[r] & \cdots \\ & & M_2 \arrow[ur] & & M_1 \arrow[ur] & & M \arrow[ur] & & M_{-1} \arrow[ur] & & \end{tikzcd}$$

where we set $d_0 = (\tau')^\star \tau$. We call this the **completed** R-free resolution of M, and we abuse notation slighly and call this F again. With this understood, we define the **ith syzygy** of M, denoted M_i, to be the image of $d_i \colon F_i \to F_{i-1}$ for all $i \in \mathbb{Z}$.

Proposition 109.1. *Let M and N finitely generated R-modules, and for $i \geq 0$, let M_i and N_i denote their respective syzygies. For $n \geq 1$, we have*

$$\begin{aligned} \mathrm{Ext}_R^{n+1}(M_i, N) &\cong \mathrm{Ext}_R^n(M_{i+1}, N) \\ \mathrm{Tor}^R_{n+1}(M_i, N) &\cong \mathrm{Tor}^R_n(M_{i+1}, N) \\ \mathrm{Tor}^R_{n+1}(M, N_i) &\cong \mathrm{Tor}^R_n(M, N_{i+1}) \end{aligned}$$

Moreover, assume R is Gorenstein and M and N are maximal Cohen-Macaulay. Then the isomorphisms above continue to make sense for all $i \in \mathbb{Z}$ and we also get

$$\mathrm{Ext}_R^n(M, N_i) \cong \mathrm{Ext}_R^{n+1}(M, N_{i+1}).$$

Proof. For each i we have a short exact sequence of R-modules:

$$0 \longrightarrow M_{i+1} \longrightarrow F_i \longrightarrow M_i \longrightarrow 0 \tag{418}$$

After applying $\mathrm{Hom}_R(-, N)$ to this short exact sequence, we obtain a long exact sequence in homology:

$$\cdots \longrightarrow \mathrm{Ext}_R^{n-1}(M_{i+1}, N) \longrightarrow \mathrm{Ext}_R^n(M_i, N) \longrightarrow \mathrm{Ext}_R^n(F_i, N) \longrightarrow \mathrm{Ext}_R^n(M_{i+1}, N) \longrightarrow \mathrm{Ext}_R^{n+1}(M_i, N) \longrightarrow \cdots$$

Since $\mathrm{Ext}_R^n(F_i, N) = 0$ for all $n \geq 1$, we obtain isomorphisms

$$\mathrm{Ext}_R^{n+1}(M_i, N) \cong \mathrm{Ext}_R^n(M_{i+1}, N)$$

for all $n \geq 1$. The proof of the other isomorphisms follows a similar line of logic. □

110 Tangent Space of a Local Ring

Let $(R, \mathfrak{m}, \Bbbk)$ be a local noetherain ring. Recall the tangent space of R is defined to be the $\Bbbk$-vector space:

$$T_{\mathfrak{m}}(R) = \mathrm{Hom}_{\Bbbk}(\mathfrak{m}/\mathfrak{m}^2, \Bbbk).$$

Recall that a **point-derivation** $\partial \colon R \to \Bbbk$ is a $\Bbbk$-linear map which satisfies Leibniz law, meaning

$$\partial(r_1 r_2) = \partial(r_1)\overline{r}_2 + \overline{r}_1 \partial(r_2)$$

for all $r_1, r_2 \in R$ where $\overline{r} \in \Bbbk$ denotes the image of $r \in R$ under the canonical quotient map $R \twoheadrightarrow \Bbbk$. The set of all point-derivations $\partial \colon R \to \Bbbk$ forms an R-module and is given by

$$\mathrm{Der}_{\Bbbk}(R, \Bbbk) = \mathrm{Hom}_R(\Omega_{R/\Bbbk}, \Bbbk),$$

where $\Omega_{R/\Bbbk}$ is the module of Kahler differentials of R over $\Bbbk$.

Definition 110.1. A map $\theta\colon R \to R$ is called a **derivation** if θ satisfies Leibniz law, meaning

$$\theta(r_1 r_2) = \theta(r_1)r_2 + r_1\theta(r_2)$$

for all $r_1, r_2 \in R$, and if the map $\vartheta\colon \mathfrak{m}^2 \to R$ defined by

$$\vartheta(x_1, x_2) := \theta(x_1 + x_2) - \theta(x_1) - \theta(x_2),$$

lands in $\mathfrak{m}$.

Remark 138. If θ is a derivation, then observe that

1. $\theta(\mathfrak{m}^2) \subseteq \mathfrak{m}$
2. $[r, x]_\theta := \theta(rx) - r\theta(x) = \theta(r)x \in \mathfrak{m}$.

In particular, we get a well-defined $\Bbbk$-linear map $\overline{\theta}\colon \mathfrak{m}/\mathfrak{m}^2 \to \Bbbk$. Conversely, suppose $\tau\colon \mathfrak{m}/\mathfrak{m}^2 \to \Bbbk$ is any $\Bbbk$-linear map. Let $\overline{x}_1, \ldots, \overline{x}_m$ be a basis for $\mathfrak{m}/\mathfrak{m}^2$ as a $\Bbbk$-vector space, so $x_1, \ldots, x_m$ is a minimal generating set for $\mathfrak{m}$. Furthermore, set $\tau(\overline{x}_i) = c_i$ for each i and let

$$\partial := c_1\partial_{x_1} + \cdots + c_m\partial_{x_m}.$$

References

[Eis95] D. Eisenbud. (1995) *Commutative Algebra: With a View Toward Algebraic Geometry.* New York: Springer-Verlag

[Hoc1] Melvin Hochster, *The structure theory of complete local rings*, https://dept.math.lsa.umich.edu/~hochster/615W17/supStructure.pdf.

[Hoc2] Melvin Hochster, *Noether normalization and Hilbert's nullstellensatz*, https://dept.math.lsa.umich.edu/~hochster/615W17/supNoeth.pdf.

[Hoc3] Melvin Hochster, *Dimension theory and system of parameters*, https://dept.math.lsa.umich.edu/~hochster/615W10/supDim.pdf.