COMMUTATIVE ALGEBRA

TAUGHT BY

PROF. FRANCESC CASTELLA

WRITTEN BY

BAZINGA

COURSE NOTES ON MODERN ALGEBRA

MATH 220B

Contents

CHAPTER 0

Preface

This short text is a collection of notes I made for a commutative algebra course I am currently taking (Math 220B, winter 2022). This is a first-year graduate course on (commutative) rings and module theory. Topics to be covered include: rings and ring homomorphisms; ideals and quotient rings; zero divisors, nilpotent elements; prime ideals and maximal ideals; nilradical and Jacobson radical; fields of fractions; localization; modules over commutative rings; submodules and quotient modules; isomorphism theorems; direct sums; free modules; tensor products; flatness; Noetherian rings and their finitely generated modules; Hilbert's Basis Theorem. Additional topics will be covered if time permits.

The main references for this course are Atiyah and Macdonald [1], Lang [2], Dummit and Foote [3]. The first book is the main textbook. Some of the problems will come from D/F.

CHAPTER 1

Rings and Ideals

1.1 Rings and Ring Homomorphisms

Definition 1.1. A **ring** R is an abelian group $(R, +)$ under addition, together with a multiplication $\times : R \times R \to R$, sometimes denoted by $r \cdot s$ or simply rs for elements $r, s \in R$, such that

1. Multiplication is associative: $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$.
2. Multiplication distributes over addition: $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$, and similarly $(r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$.
3. There exists element $1 \in R$ such that $r \cdot 1 = 1 \cdot r = r$ for all $r \in R$.

If multiplication is commutative, then we call R a **commutative ring**.

Example 1.2. Here are some examples of rings:

1. Integer $\mathbb{Z}$ with the usual addition and multiplication.
2. $\mathbb{Z}/n\mathbb{Z}$ with the usual addition and multiplication under modular arithmetic.
3. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with usual addition and multiplication.
4. Let R be a ring, the $n \times n$ matrices with entires in R, denoted by $M_{n\times n}(R)$, is a ring under matrix addition and multiplication.
5. The polynomials $R[x]$ with coefficients in a ring R is a ring under polynomial addition and multiplication.
6. Let G be an abelian group, let $R = \mathrm{Hom}(G)$ be the set of all group homomorphisms $G \to G$. Then define, for $\phi, \psi \in R$, the addition $(\phi + \psi)(g) = \phi(g) + \psi(g)$, and the multiplication $(\phi\psi)(g) = \phi \circ \psi(g)$. Then $1 = \mathrm{id}_G$. This gives R a ring structure.
7. Let X be any set, let $R = 2^X$ be its power set. Then define for $E, F \in R$, $E + F := (E \cup F) \backslash (E \cap F)$, and $E \cdot F = E \cap F$. Then $1 = X \in R$. This gives R a ring structure.

Definition 1.3. Let R, S be rings. A **ring homomorphism** is a map $f : R \to S$ such that $f(r + s) = f(r) + f(s)$, $f(rs) = f(r)f(s)$, and $f(1_R) = 1_S$.

For example, let $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the projection map, $\pi(a) = \overline{a} = a + n\mathbb{Z}$. This is a homomorphism between rings.

Definition 1.4. A **subring** S of a ring R is a subset that is closed under addition and multiplication inherited from R, and $1 \in S$.

Definition 1.5. Let R be a ring.

(I) A subset $I \subseteq R$ is called a **left ideal** of R if I is closed under addition, and $R \cdot I \subseteq R$, i.e. $rs \in I$ for all $r \in R, s \in I$.

(II) Similarly for **right ideals** $I \cdot R \subseteq R$.

(III) An **ideal** $I \subseteq R$ is simultaneously a left idea and right ideal.

(IV) Suppose $I \subseteq R$ and ideal, the quotient

$$R/I = \{r + I : r \in R\}$$

inherits addition and multiplication from R:

$$(r + I) + (s + I) = (r + s) + I \qquad (r + I)(s + I) = rs + I.$$

Then R/I with this addition and multiplication is a ring with $1 = 1 + I$. Note that R/I make sense since R is abelian, and I is normal. This is called the **quotient ring**. The **quotient map** $\pi : R \to R/I, r \mapsto r + I$ is a ring homomorphism.

1.2 Ideals and Quotient Rings

Before we present more definitions, there are two exercises that we present. In fact they are two very important results in undergraduate algebra class. Here we simply leave the proof to the reader.

Theorem 1.6 (Correspondence Theorem)**.** *Let R be a ring, $I \subset R$ be an ideal, and $\phi : R \to R/I$ with $\phi(r) = \overline{r} = r + I$ be the quotient map. Then there is a bijective and order preserving correspondence between ideals $J \subseteq R$ that contains I and ideals in R/I, where the correspondence is given by*

$$J \mapsto \phi(J)$$

with inverse

$$\phi^{-1}(A) \hookleftarrow A.$$

Theorem 1.7 (First Isomorphism Theorem)**.** *Let $\phi : R \to S$ be a ring homomorphism. Then we have the following claims:*

(I) $\ker\phi = \phi^{-1}(0)$ *is an ideal of R.*

(II) $\mathrm{im}(\phi) = \phi(R)$ *is a subring of S.*

(III) ϕ induces a ring isomorphism $R/\ker\phi \approx \mathrm{im}\,\phi$ via the map $r + \ker\phi \mapsto \phi(r)$.

Definition 1.8. Let R be a ring.

(1) A **zero divisor** in R is an element $x \in R$ such that there exists $y \neq 0$ in R with $xy = 0 = yx$.

(2) A nonzero commutative ring R without nonzero zero divisors is called an **integral domain**.

(3) An element $r \in R$ is **nilpotent** if $r^n = 0$ for some $n > 0$.

(4) An element $r \in R$ is a **unit** if there exists $s \in R$ such that $rs = 1 = sr$.

(5) Let $x \in R$. Then the multiples rx form a left ideal, denoted by Rx. If R is commutative. Similarly, xR form a right ideal. And if R is commutative, denote $(x) = Rx = xR$. We call (x) the **principal ideal** generated by $x \in R$.

(6) A **field** is a nonzero commutative ring R in which every nonzero element is a unit: $R^\times = R - \{0\}$.

Remark 1.9. Here are some respective remarks for the definitions above:

(1) 0 is a zero divisor unless $R = \{0\}$. Another example: $\overline{2} \in \mathbb{Z}/6\mathbb{Z}$ is a zero divisor.

(2) Examples of integral domains: $\mathbb{Z}, k[x_1, ..., x_n]$ where k is a field.

(3) Note that r is nilpotent implies r is a zero divisor: let $n > 0$ be the minimal integer such that such that $x^n = 0$ but $x^{n-1} \neq 0$. Then $x^{n-1} \cdot x = 0$. The converse is not true. For example, $\overline{2} \in \mathbb{Z}/6\mathbb{Z}$ is not nilpotent. Note that $0 = 0^1$ is nilpotent.

(4) Example of units: $\overline{5} \in \mathbb{Z}_6$, for $\overline{5 \cdot 5} = \overline{1} \in \mathbb{Z}_6$.

(5) Note that $(x) = R$ if and only if $x \in R^\times$ (x is a unit of R).

(6) Note that if x is a unit, then x is not a zero divisor. Say x is a unit and a zero divisor, so let $xy = yx = 0$ with $y \neq 0$, and let $xs = sx = 1$. Then $(sx)y = 1y = y \neq 0$ but $(sx)y = s(xy) = s0 = 0$. Contradiction. Then it follows that if R is a field, then R is automatically an integral domain.

Proposition 1.10. Let R be a nonzero commutative ring, then the following are equivalent (TFAE):

(1) R is a field.

(2) The only ideals in R are (0) and (1).

(3) Every ring homomorphism $\phi : R \to S$ is with $S \neq (0)$ injective.

Proof. (1) $\Rightarrow$ (2) : Let I be a nonzero ideal in field R. Then there exists $x \neq 0$ such that $x \in I$. So x is a unit. Then $R = (x) \subseteq I \subseteq R$ implies $I = R$.

(2) $\Rightarrow$ (3) : Let $\phi : R \to S$ be a ring homomorphism with $S \neq (0)$. Then $\ker \phi$ is an ideal. Since $S \neq (0)$, we have $\ker \phi \neq (1)$. Thus $\ker \phi = (0)$.

(3) $\Rightarrow$ (1) : Let $x \in R$ such that x is not a unit. We want to show that $x = 0$. Since x is not a unit, $(x) \neq R$. So $R/(x) \neq (0)$. Let $\phi : R \to R/(x)$ be the quotient map, then (3) implies ϕ is injective. So $\ker \phi = (0) = (x)$. Thus $x = 0$. □

Definition 1.11. Let R be a commutative ring.

(1) A **prime ideal** $I \subsetneq R$ is a proper ideal such that for all $r, s \in R$, we have $rs \in I$ implies either $r \in I$ or $s \in I$.

(2) A **maximal ideal** $I \subsetneq R$ is a proper ideal such that for all ideals $J \subseteq R$, we have $I \subseteq J \subseteq R$ implies either $J = I$ or $J = R$.

Proposition 1.12. Let R be a commutative ring and $I \subsetneq R$ be a proper ideal. Then R/I is an integral domain if and only if I is a prime ideal.

Proof. Suppose R/I is an integral domain. Then let $r, s \in R$ such that $rs \in I$. Then in R/I, we have $(r + I)(s + I) = rs + I = I = 0 \in R/I$. Since R/I is an integral domain, either $r + I = 0$ or $s + I = 0$, so either $r \in I$ or $s \in I$.

Conversely, let I be a prime ideal, assume $r + I \in R/I \neq (0)$ is a zero divisor. We want to show that $r + I = 0 \in R/I$. By assumption there exists $s + I \neq 0$ in R/I such that $(r + I)(s + I) = rs + I = 0$, so $rs \in I$. By assumption $s \neq I$ and I is prime, we have $r \in I$, so $r + I = 0 \in R/I$. □

Proposition 1.13. Let R be a commutative ring and $I \subsetneq R$ be a proper ideal. Then R/I is a field if and only if I is a maximal ideal.

Proof. Let R/I be a field. Let $J \subseteq R$ be an ideal such that $I \subsetneq J$. We want to show $J = R$. Take $x \in J \backslash I$. So $x + I \neq 0 \in R/I$. Thus there exists $y + I$ such that $(x + I)(y + I) = xy + I = 1 + I$ since R/I is a field. Then $1 - xy \in I \subseteq J$. But $x \in J$, so $xy \in J$. Thus

$$1 = (1 - xy) + (xy) \in J$$

implies $J = R$. Conversely, let I be a maximal ideal and $x + I \neq 0 \in R/I$. We want to show this is a unit. Since $x + I \neq 0$ we have $x \notin I$. Thus we consider

$$J = \{a + rx : a \in I, r \in R\}.$$

We can check that J is an ideal in R containing I, and $I \subsetneq J$ for $x \in J \backslash I$. Thus $J = R$ by the maximality of I. In particular, since $1 \in J$, we have $1 = a + rx$ for some $a \in I, r \in R$. Then $(r + I)(x + I) = rx + I = (1 - a) + I = 1 + I$. □

Corollary 1.14. *In a commutative ring, every maximal ideal is prime.*

The converse is not true. Example: Let $R = \mathbb{Z}[x]$. Let I be all polynomial with zero constant terms in $\mathbb{Z}[x]$, that is, $I = (x)$. Then I is prime since $\mathbb{Z}[x]/(x) \approx \mathbb{Z}$ via the isomorphism $\varphi(p(x)) = p(0) \in \mathbb{Z}$. But I is not maximal. In particular, let K denote all polynomials with even constant term. Then we can check that K is an ideal, and $I \subsetneq K \subsetneq \mathbb{Z}[x]$.

1.3 Existence of Maximal Ideals

Definition 1.15. A **partial ordering** on a set A is a relation $\leq$ such that:

(i) $x \leq x$ for all $x \in A$.

(ii) If $x \leq y$ and $y \leq x$, then $x = y$.

(iii) If $x \leq y$ and $y \leq z$, then $x \leq z$.

Note that we do not require any pair in A be comparable by $\leq$. Otherwise we would call $\leq$ a **total ordering**. A tuple $(A, \leq)$ is called a **partially ordered set**.

Definition 1.16. Let A be a partially ordersed set (or simply a poset).

- Let $B \subseteq A$. We say $x \in A$ is an **upper bound** for B if $y \leq x$, for all $y \in B$. Note that we require x be comparable to all elements in B.
- A subset $B \subseteq A$ is called a **chain** if $\leq$ is a total ordering in B, i.e. for all $x, y \in B$, either $x \leq y$ or $y \leq x$.

Lemma 1.17 (Zorn's Lemma)**.** *Let A be a nonempty poset in which every chain has an upper bound. Then A has a maximal element. That is, there exists $x \in A$ such that for all $y \in A$, either $y \leq x$, or x, y are not related.*

Zorn's theorem cannot be proven, since it is equivalent to the axiom of choice.

Theorem 1.18. *Let R be a nonzero commutative ring. and $I \subsetneq R$. Then there exists a maximal ideal J containing I.*

Proof. Consider the set

$$A = \{\text{all proper ideals of } R \text{ containing } I\}$$

with partial ordering $\leq$ being the inclusion $\subseteq$. Then since $I \in A$, so $A \neq \emptyset$. Let $\mathcal{C} = \{a_\lambda\}_{\lambda \in \Lambda} \subseteq A$ be a chain. We have the following observation: The element

$$a = \bigcup_{\lambda \in \Lambda} a_\lambda$$

is an upper bound for $\mathcal{C}$. We only need to check the following:

- a is an ideal of R. Let $x, y \in a$, say $x \in a_\lambda, y \in a_\mu$. Since $\mathcal{C}$ is a chain, WLOG say $a_\lambda \subseteq a_\mu$. Then $x, y \in a_\mu$. So $x + y \in a_\mu \subseteq a$. Let $x \in a$, assume $x \in a_\lambda$, then $rx \in a_\lambda \subseteq a$ for all $r \in R$, since a_λ is an ideal.
- a is proper. If $1 \in a_\lambda$ for some λ, then $a_\lambda = R$, contradicting our hypothesis.
- a contains I, for each ideal contains I.

Applying Zorn's lemma, we see A has a maximal element, as desired. □

Corollary 1.19. *Let R be a nonzero commutative ring. Then R contains some maximal ideal.*

Proof. Apply the theorem above to the ideal $I = (0)$. □

1.4 Operation on Ideals

From now on, unless otherwise noted, all rings with be commutative with identity.

Definition 1.20. Let R be a ring. Then:

(1) If $a_1, ..., a_t \subseteq R$ are ideals, then define their **sum** to be the ideal

$$a_1 + \cdots + a_t = \{\alpha_1 + \cdots + \alpha_t : \alpha_i \in a_i\}.$$

(2) If $x_1, ..., x_t \in R$, the ideal generated by them is the ideal

$$(x_1, ..., x_t) = \{r_1x_1 + \cdots + r_tx_t : r_i \in R\} = (x_1) + \cdots + (x_n).$$

Definition 1.21. A ring R with exactly one maximal ideal m is called a **local ring**. Often we denote this by (R, m).

Example 1.22. Fields are local rings with $m = (0)$: recall that maximal ideal is proper. For any prime $p \in \mathbb{N}$, the ring

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, p \not| b\right\} \subset \mathbb{Q}$$

is a local ring with $m = (p)$.

Lemma 1.23. *Let R be a ring with $m \subsetneq R$ be a proper ideal such that every element $x \in R\backslash m$ is a unit in R, then R is local and m is the unique maximal ideal in R.*

Proof. Let $I \subsetneq R$ be a proper ideal, then I must not contain any unit (otherwise $I = R$). But by assumption $I \cap (R\backslash m) = \emptyset$, so $I \subseteq m$. This means any proper ideal that contains m with be equal to m. Hence m is the unique maximal ideal. □

We can use this lemma to check the previous example.

Proposition 1.24. Let R be a ring, $m \subsetneq R$ be a maximal ideal. Then (R, m) is a local ring if and only if every element $x \in 1 + m = \{1 + t : t \in m\}$ is a unit in R.

Proof. Let (R, m) be local, but $x \in 1 + t$ with $t \in m$, and suppose x is not a unit in R. Then $(1 + t) \subsetneq R$ is a proper ideal. But (R, m) is local, and any proper ideal is contained in a maximal ideal by the theorem in the last section, we have $(1 + t) \subseteq m$, so $1 + t \in m$. But $t \in m$ implies $1 \in m$, which contradicts the assumption.

Conversely, let $x \in R\backslash m$. Since m is maximal, we have $m + (x) = R$. Then $t + xy = 1$ for some $t \in m, y \in R$. Thus $xy = 1 - t \in 1 + m$ is a unit. So xy is a unit, which means x is a unit (Let z be the inverse of xy. We claim that $yz = x^{-1}$. Clearly $x(yz) = 1$. Now, $(yz)x = y(xy)^{-1}x = yy^{-1}x^{-1}x = 1$. This proves the claim.). Then we are done by the previous lemma. □

Proposition 1.25. The set $\mathcal{N} = \{\text{all nilpotent element in } R\}$, i.e. all elements x such that $x^n = 0$ for some $n > 0$, is an ideal of R. Furthermore, $R/\mathcal{N}$ has no nonzero nilpotent element.

Proof. Let $x \in \mathcal{N}$. Then $ax \in \mathcal{N}$ for all $a \in R$. Suppose $x, y \in \mathcal{N}$, say $x^n = y^m = 0$. Then by Binomial expansion, we have

$$(x-y)^r = \sum_{i+j=r} \binom{r}{i} x^i (-y)^j.$$

Let $r = n + m - 1$. Then $(x-y)^{n+m-1} = 0$. So $\mathcal{N}$ is an ideal. Now suppose $\overline{x} \in R/\mathcal{N}$ is represented by $x \in R$. Then $\overline{x}^n = 0$ implies $x^n \in \mathcal{N}$, so $(x^n)^m = 0$ for some $m > 0$. Then $x \in \mathcal{N}$. This proves the last claim. □

Definition 1.26. The ideal $\mathcal{N}$ is called the **nilradical** of R.

Proposition 1.27. The nilradical of R is the same as the intersection of all prime ideals of R. That is,

$$\mathcal{N} = \bigcap_{\wp \subsetneq R \text{ prime}} \wp.$$

Proof. Let $\mathcal{N}'$ be the intersection of all prime ideals $\wp$ in R. Pick $x \in \mathcal{N}$ and $\wp \subsetneq R$ a prime ideal. Then $x^n = 0$ for some $n > 0$. So $x^n \in \wp$. Thus $x \in \wp$ by induction. Thus $x \in \mathcal{N}'$ since $\wp$ is arbitrary.

Conversely, suppose $f \notin \mathcal{N}$, we want to show $f \notin \mathcal{N}'$. Let

$$\Sigma = \{\text{ideals } I \subseteq R \text{ such that } f^n \notin I \text{ for all } n\}$$

and let Σ be ordered by inclusion. Then $(0) \in \Sigma \neq$ by definition. We can show that every chain in Σ has an upper bound (exercise). Then by Zorn's lemma, there exists a maximal element $\wp \in \Sigma$.

We claim that $\wp$ is a prime ideal. Let $x, y \notin \wp$, then

$$\wp \subsetneq \wp + (x) \qquad \wp \subsetneq \wp + (y).$$

Since $\wp \in \Sigma$ is maximal, we have that $\wp + (x), \wp + (y) \notin \Sigma$. Then $f^n \in \wp + (x)$ for some n and $f^m \in \wp + (y)$ for some m. Then we see that

$$f^{n+m} \in (\wp + (x))(\wp + (y)) \subseteq \wp + (xy).$$

Therefore, by definition of Σ, we have $p + (xy) \notin \Sigma$. Thus $xy \notin \wp$. Therefore, $\wp$ is a prime ideal with $f^n \notin \wp$ for all $n > 0$. So $f \notin \mathcal{N}'$. □

1.5 Chinese Remainder Theorem

Definition 1.28. Let $R_1, ..., R_n$ be rings. Their **direct product**

$$R_1 \times \cdots \times R_n = \{(x_1, ..., x_n) : x_i \in R_i\}$$

is a ring with componentwise addition and multiplication.

Definition 1.29. Let $\{a_i\}_{i \in I}$ be a collection of ideals in a ring R.

- The **sum** of $\{a_i\}_{i\in I}$ is the set $\sum_{i\in I} a_i = \left\{\sum_{i\in I} x_i : x_i \in a_i, x_i = 0 \text{ for all but finitely many } i\right\}$.
- The **intersection** $\bigcap_{i\in I} a_i$ is again an ideal.
- The **product** $a_1 \cdots a_n = \left\{\sum_{\text{finite}} x_1 \cdots x_n : x_i \in a_i\right\}$ is an ideal.

Note that the unions of ideals need not be ideals. In fact, $a + b$ is the smallet ideal containing the union $a \cup b$ of ideals a, b.

Example 1.30. Let $R = \mathbb{Z}$. Let $a = (m)$ and $b = (n)$. Then one can show that $a + b = (\gcd(m, n))$ and $a \cap b = (\text{lcm}(m, n))$. This motivates the following definition:

Definition 1.31. We say two ideals a, b are **coprime** if $a + b = R$.

Proposition 1.32 (Chinese Remainder Theorem)**.** Let R be a ring, $a_1, ..., a_n$ be ideals in R that are pairwise coprime. Then we have

$$a_1 \cdots a_n = \bigcap_{i=1}^{n} a_i$$

and the natural map

$$\begin{aligned} \phi : R &\to R/a_1 \times \cdots \times R/a_n \\ x &\mapsto (x \mod a_1, ..., x \mod a_n) \end{aligned}$$

induces a ring isomorphism

$$R/a_1 \cdots a_n \approx R/a_1 \times \cdots R/a_n.$$

Proof. We show that $a_1 \cdots a_n = \bigcap_{i=1}^{n} a_i$ by induction on n. When $n = 2$, clearly $a_1 a_2 \subseteq a_1 \cap a_2$. Conversely, one can check that

$$a_a \cap a_2 = (1) \cdot (a_1 \cap a_2) = (a_1 + a_2)(a_1 \cap a_2) = a_1(a_1 \cap a_2) + a_2(a_1 \cap a_2) \subseteq a_1 a_2.$$

Now suppose $n > 2$ and the equality is true for $a_1 \cdots a_{n-1}$. Let $b = a_1 \cdots a_{n-1}$. For $i = 1, ..., n-1$, we have $a_i + a_n = R$, so $1 = x_i + y_i$ for some $x_i \in a_i, y_i \in a_n$. Thus

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{n} (1 - y_1) \equiv 1 \mod a_n.$$

Note that LHS is in b. This means $b + a_n = R$, for 1 can be written as some elements in b plus some elements in a_n shown above. Thus $ba_n = b \cap a_n$ by the base case of induction. This proves the equality.

For the second claim, ϕ is clearly a ring homomorphism, since every component of ϕ is and the multiplication is defined componentwise. We claim that ϕ is surjective. We will show that there exists $x \in R$ such that $\phi(x) = (1, 0, ..., 0)$. Similar argument will show that there exists $x_j \in R$ for each j such that $\phi(x_j) = (0, ..., 1, 0, ..., 0)$ where the 1 is in the jth position. Then for any $r = (r_1, ..., r_n) \in R/a_1 \times \cdots \times R/a_n$, let $\eta_i \in R$ such that $\phi(\eta_i) = r_i$, then $y = \sum_{i=1}^{n} \eta_i x_i \in R$ is the desired element such that $\phi(y) = r$.

Now, for $i = 2, ..., n$, we have $a_1 + a_i = R$. So $u_i + v_i = 1$ for some $u_i \in a_1, v_i \in a_i$. Then

$$x = \prod_{i=2}^{n} v_i = \prod_{i=2}^{n} (1 - u_i) \equiv \begin{cases} 1 & \mod a_1 \\ 0 & \mod a_i, i \geq 2. \end{cases}$$

Thus x is the desired element such that $\phi(x) = (1, 0, ..., 0)$. This shows that ϕ is surjective. Now, note that $\ker \phi = \bigcap_{i=1}^{n} a_i = a_1 \cdot a_n$. Apply the first isomorphism theorem concludes the proof. □

Corollary 1.33. *If $m = \prod_{i=1}^{n} p_i^{r_i}$ is the prime factorization of $m \in \mathbb{N}$, then*

$$\mathbb{Z}/m\mathbb{Z} \approx \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{r_n}\mathbb{Z}.$$

Definition 1.34. If a is an ideal of R, the radical of a is defined to be

$$\mathrm{rad}(a) = \{x \in R : x^n \in a \text{ for some } n > 0\}.$$

Note: clearly we have the nilradical $\mathcal{N} = \mathrm{rad}((0))$. Also, if $\phi : R \to R/a$ is the quotient map, then $\mathrm{rad}(a) = \phi^{-1}(\mathcal{N}_{R/a})$.

Proposition 1.35. The radical of $a \subset R$ is the intersection of all prime ideals $\wp \subsetneq R$ containing a.

Proof. Let $\phi : R \to R/a$ be the quotient map. Then

$$\mathrm{rad}(a) = \phi^{-1}(\mathcal{N}_{R/a}) = \phi^{-1}\left(\bigcap_{\overline{\wp} \subset R/a \text{ prime}} \overline{\wp}\right) = \bigcap_{\overline{\wp} \subset R/a \text{ prime}} \phi^{-1}(\overline{\wp}) = \bigcap_{a \subset \wp \subset R \text{ prime}} \wp.$$

The last step follows from the correspondence theorem. □

Example 1.36. Let $R = \mathbb{Z}$ and $a = (m)$. Let $m = \prod_{i=1}^{n} p_i^{r_i}$ be the prime factorization. Then

$$\mathrm{rad}(a) = (p_1) \cdots (p_n) = (p_1 \cdots p_n).$$

CHAPTER 2

Localization

2.1 Extension and Contraction

Definition 2.1. Let $f : R \to S$ be ring homomorphism, let $a \subseteq R, b \subseteq S$ be ideals.

- The **contraction** b^c of b is the ideal $b^c := f^{-1}(b) \subseteq R$.
- The **extension** a^e of a is the ideal of S generated by the image $f(a)$. That is,

$$a^e = \left\{ \sum_i y_i f(x_i) : y_i \in S, x_i \in a \right\}.$$

You can check that contraction of an ideal is an ideal. However, in general, the image $f(a)$ of an ideal a need not be an ideal. Consider the inclusion map $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$. Let $a = 2\mathbb{Z}$. Then a is an ideal in $\mathbb{Z}$, but not in $\mathbb{Q}$. We make a few more remarks:

Remark 2.2.

(I) If $b \subset S$ is a prime ideal, then $b^c \subset R$ is also a prime ideal. To see this, notice that the composition

$$R \xrightarrow{f} S \xrightarrow{\pi} S/b$$

induces an injection

$$R/b^c \hookrightarrow S/b$$

by the first isomorphism theorem. Now since S/b is an inyegral domain, so is R/b^c. Thus b^c is prime.

(II) If $a \subset R$ is a prime ideal, then a^e may not be prime. For example, $a = 2\mathbb{Z}$ extends to $a^e = \mathbb{Q}$ under the inclusion map $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$.

(III) Any ring homomorphism $f : R \to S$ can be factored as

$$\begin{array}{ccccc} R & \xrightarrow{\pi} & f(R) & \xhookrightarrow{\iota} & S \\ & \searrow & \wr & & \\ & & R/\ker f & & \end{array}$$

For π, we know prime ideals for R containing $\ker f$ is in 1-1 correspondence with prime ideals of $f(R)$. But for ι, the situation is much more complicated and require analysis case by case.

Proposition 2.3. Let $f : R \to S$ be a ring homomorphism. Let $a \subset R, b \subset S$ be ideals. Then

(1) $a \subset a^{ec}$ and $b \supset b^{ce}$.

(2) $b^c = b^{cec}$ and $a^e = a^{ece}$.

(3) Let C be the set of contracted ideals in R and E be the set of extended ideals in R. Then we have

$$C = \{a \subset R : a = a^{ec}\}$$
$$E = \{b \subset S : b^{ce} = b\}.$$

More over, C and E are in bijective correspondence via the maps $\eta : C \to E$, $\xi : E \to C$, $\eta(a) = a^e$, $\xi(b) = b^c$.

Proof.

(1) If $x \in a$, then $f(x) \in a^e$. Then $x \in f^{-1}(f(x)) \in a^{ec}$. Similarly, if $x \in b^{ce}$, then $x = \sum_i y_i f(x_i)$ for some $y_i \in S, x_i \in b^c = f^{-1}(b)$. Then $f(x_i) \subset f(f^{-1}(b)) \subseteq b$. Thus $x \in b$. This proves (1).

(2) The previous two results implies the two sided inculsion $a^e \subseteq a^{ece}$ and $a^e \supseteq b^{ece}$. Thus the claim follows. The second claim also follows from (1) immediately.

(3) We first prove the equalities. Let $a \in C$. Then $a = b^c$ for some $b \in S$. Then $a^{ec} = b^{cec} = b^c = a$ by (2). Conversely, if $a = a^{ec}$, then clearly a is the contraction of $a^e \subseteq S$. A similar arguments shows the equality involving E. Now it is straightforward to check that η, ξ are indeed inverses of each other.

This concludes the proof. □

2.2 Ring of Fractions and Localization

What motivates the construction of ring of fractions is how one construct $\mathbf{Q}$ from $\mathbf{Z}$. We take all ordered pairs (a, s) with $a, s \in \mathbb{Z}$, and we set up the equivalence relation $(a, s) \sim (b, t)$ if and only if $at - bs = 0$. Then we define $\mathbb{Q}$ to be the set of all equivalent classes of such pairs. This motivates the following definition:

Definition 2.4. Let R be a commutative ring with 1. Then a **multiplicative subset** S of the ring R is a subset such that $1 \in S$, and $s, t \in S$ implies $st \in S$.

Example 2.5. Here are some examples of a multiplicative sets:

(1) If $\wp$ is prime, then $S = R \backslash \wp$ is multiplicative. Note that $\wp$ is proper by definition, so it cannot contain 1, thus $1 \in S$. Moreover, if $ab \in \wp$, then either $a \in \wp$ or $b \in wp$. Taking contrapositive, this means if $a \in S$ and $b \in S$, then $ab \in S$.

(2) If R is an integral domain, then $S = R \backslash \{0\}$ is multiplicative.

(3) For any $f \in R$, the subset $S = \{f^n : n \geq 0\}$ is multiplicative with $f^0 = 1$.

Next, we let $S \subseteq R$ be a multiplicative subset, define the following relation on $R \times S$:

$$(a, s) \sim (b, t) \Leftrightarrow (at - bs)u = 0 \text{ for some } u \in S.$$

You can check that this is indeed and equivalence relation. Then we define

$$\frac{a}{s} = \{\text{all equivalence classes of } (a, s) \in R \times S\}$$

and

$$S^{-1}R = \left\{\text{all equivalence classes } \frac{a}{s}\right\}$$

with ring structure given by

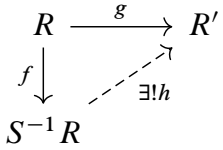
$$\frac{a}{s} + \frac{b}{t} = \frac{at + sb}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

You should check that the addition and multiplication is well-defined. We say $S^{-1}R$ is the **ring of fractions** of R with respect to S, or the **localization** of R at S. Notice that the map

$$f : R \to S^{-1}R \qquad r \mapsto r/1$$

is a ring homomorphism such that $f(s)$ is invertible for all $s \in S$, with inverse $1/s$.

Proposition 2.6 (Universal Property)**.** Let $g : R \to R'$ be a ring homomorphism such that $g(s)$ is invertible for all $s \in S$. Then there exists a unique ring homomorphism $h : S^{-1}R \to R'$ such that the following diagram commutes:



Proof. We first suppose h exists. Then for all $r \in R$, we have that $h(r/1) = h(f(r)) = g(r)$. Therefore, if $s \in S$, then we have $h(1/s) = h((s/1)^{-1}) = h(s/1)^{-1} = g(s)^{-1}$. This deduction already tells us how to define h. Let

$$h\left(\frac{r}{s}\right) = h\left(\frac{r}{1} \cdot \frac{1}{s}\right) = h\left(\frac{r}{1}\right) \cdot h\left(\frac{1}{s}\right) = g(r)g(s)^{-1}.$$

According to this definition, h is uniquely determined by g. Now it remains to show that h is well defined to prove the existence, since definition $h(r/s) = g(r)g(s)^{-1}$ is a ring homomorphism such that $g = h \circ f$. Now, suppose $r/s = r'/s'$. Then $(rs' - sr')u = 0$ for some $u \in S$. Thus by applying g we have

$$(g(r)g(s') - g(s)g(r'))g(u) = 0.$$

This is an equation in R'. But since $u \in S$, so $g(s)$ is invertible, hence a unit. Therefore, we can multiply both sides of the equation above by $g(u)^{-1}$ and get

$$g(r)g(s') - g(s)g(r') = 0 \Leftrightarrow g(r)g(s') = g(s)g(r') \Leftrightarrow g(r)g(s)^{-1} = g(r')g(s')^{-1}.$$

Thus $h(r/s) = h(r'/s')$. This proves the claim. □

Corollary 2.7. *Let $S \subset R$ be a multiplicative subset and $g : R \to R'$ a ring homomorphism such that*

(1) $s \in S$ implies $g(s)$ is invertible in R'.

(2) $g(r) = 0$ implies $rs = 0$ for some $s \in S$.

(3) Every element in R' is of the form $g(r)g(s)^{-1}$ for some $r \in R, s \in S$.

Then there exists a unique ring isomorphism $h : S^{-1}R \to R'$ such that $g = h \circ f$.

Proof. By (1) and the previous proposition we see that $g = h \circ f$. We need to show h is injective and surjective. We know $h : S^{-1}R \to R'$ defined by $h(r/s) = g(r)g(s)^{-1}$ is the only possible candidate, and it is well-defined by the proof of the proposition above. surjectivity is clear from (3). Now suppose $h(r/s) = 0$. Then $g(r)g(s)^{-1} = 0$. But $g(s)$ is a unit hence can be canceled from both sides of the equation, leaving $g(r) = 0$. By (2), we have $rt = 0$ for some $t \in S$. Now

$$rt = 0 \Rightarrow (r \cdot 1 - s \cdot 0)t = 0 \Rightarrow (r, s) \sim (0, 1) \Rightarrow r/s = 0 \in S^{-1}R.$$

Hence h is also injective. This completes the proof. □

Example 2.8. Let $\wp \subset R$ be a prime ideal. Let $S = R \backslash \wp$. We write $R_\wp = S^{-1}R$. Note

$$m = \left\{ \frac{a}{s} : a \in \wp, s \in S \right\} \subset R_\wp$$

is an ideal. If $a/s \notin m$, then $a \notin \wp$, hence $a \in S$. Then $(a/s)^{-1} = s/a \in R_\wp$. Thus a/s is invertible. By Lemma 1.23, we see that $R_\wp$ is a local ring with m being its unique maximal ideal.

A special case of the example above is when we take $R = \mathbb{Z}$ and $\wp = (p)$ with p a prime number. Then

$$m = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, a = kp, p \not| b \right\}.$$

Passing from R to $R_\wp$ is called **localization at $\wp$.**

Example 2.9. Let $S = \{f^n\}_{n \geq 0}, f \in R$. Then write R_f for $S^{-1}R$. This is another example of localization.

Proposition 2.10. Let $S \subset R$ be a multiplicative set. Consider the ring homomorphism $f : R \to S^{-1}R$ by $r \mapsto r/1$. Then we have that

(i) Every ideal of $S^{-1}R$ is an extended ideal.

(ii) If $a \subset R$ is an ideal, then $a^e = S^{-1}R$ if and only if $a \cap S \neq \emptyset$.

(iii) If $a \subset R$ is an ideal, then a is contracted if and only if S does not intersect zero divisors in R/a.

(iv) There exists a bijection

$$\{\text{prime ideals } \wp \subset R \text{ with } P \cap S = \emptyset\} \xleftrightarrow{1:1} \{\text{prime ideals in } S^{-1}R\}$$

where the correspondence is given by

$$\wp \longleftrightarrow S^{-1}\wp = \{\tfrac{r}{s} : r \in \wp, s \in S\}.$$

Proof.

(i) Let $b \subset S^{-1}R$ be an ideal. We know $b \supset b^{ce}$, with equality if and only if b is an extended ideal from Proposition 2.3. Thus we want to show $b \subset b^{ce}$. Let $x/s \in b$. Then since b is an ideal of $S^{-1}R$, we have

$$\frac{s}{1}\cdot\frac{x}{s} \in b \Longrightarrow \frac{x}{1} = f(x) \in b \Longrightarrow x \in f^{-1}(b) = b^c \Longrightarrow \frac{x}{s} = \frac{1}{s}\cdot\frac{x}{1} = \frac{1}{s}f(x) \in b^{ce}$$

where the last inclusion is by the definition of extension. This proves that $b \subset b^{ce}$, hence the equality. Thus every ideal in $S^{-1}R$ is extended.

(ii) We note that

$$a^e = \left\{\sum_i \frac{r_i}{s_i} f(x_i) : r_i \in R, s_i \in S, x_i \in a\right\} = S^{-1}a := \left\{\frac{x}{s} : x \in a, s \in S\right\}.$$

Why is it true? It is clear that $S^{-1}a \subset a^e$. For the other inclusion, note that we can always write

$$\sum_i \frac{r_i}{s_i} f(x_i) = \sum_i \frac{r_i x_i}{s} = \frac{\sum_i L_i}{\prod_i s_i}$$

where each $L_i \in a$ for a is an ideal. Now suppose $a^e = S^{-1}R$. Then there exists some $x \in a, s \in S$ such that $1 = x/s$. Then $(s - x)u = 0$ for some $u \in S$ since $(x, s) \sim (1, 1)$. This is equivalent to $su = xu \in S \cap a$, which holds since $su \in S$ and $xu \in a$. Thus $S \cap a \neq \emptyset$. Conversely, suppose $S \cap a \neq \emptyset$. Then there exists $t \in S \cap a$ such that $t/1 \in S^{-1}a$, which implies

$$1 = \underbrace{\frac{1}{t}}_{\in S^{-1}R} \cdot \underbrace{\frac{t}{1}}_{\in S^{-1}a \text{ ideal}} \in S^{-1}a = a^e.$$

(iii) Again from Proposition 2.3, we know that a is contracted if and only if $a^{ec} \subset a$. Now suppose S has no zero divisors in R/a. Let $x \in a^{ec} = f^{-1}(a^e)$. So $f(x) \in a^e = S^{-1}a$. Then this is equivalent to the statement that $x/1 = y/s$ for some $y \in a, s \in S$. Thus $(xs - y)u = 0$ for some $u \in S$. Then $x(su) = yu \in a$ and $(su) \in S$. Thus $\overline{x(su)} = 0 \in R/a$. If S has no zero divisors in R/a, then we must have $\overline{x} \in R/a$ so $x \in a$. Thus $a^{ec} \subset a$ and a is contracted.

Conversely, suppose S has a zero divisor in R/a. We want to show $a^{ec} \not\subset a$. By assumption there exists $x \notin a$ such that $xs = y \in a$ for some $s \in S$. Then $x/1 = y/s$, so $x = y/s$ with $y \in a$ and $s \in S$. Thus $x \in S^{-1}a = a^{ec}$. Thus $a^{ec} \not\subset a$ for $x \in a^{ec} \backslash a$.

(iv) If $q \subset S^{-1}R$ is a prime ideal, then it is safe to say $q = S^{-1}\wp$ for some prime ideal $\wp \subset R$, since by (i) every ideal of $S^{-1}R$ is extended, and the expression follows from the beginning of proof of (ii). Then $q^c = \wp$. Since q is prime, so is its contraction $\wp$. By (ii), we must have $\wp \cap S = \emptyset$. Otherwise $\wp^e$ will not be a prime ideal (since it is not proper). Thus we have an injection

$$\{\text{prime ideals } \wp \subset R \text{ with } P \cap S = \emptyset\} \longleftarrow \{\text{prime ideals in } S^{-1}R\}$$

given by $\wp \leftarrowtail S^{-1}\wp$.

Conversely, let $\wp \subset R$ be a prime ideal with $\wp \cap S = \emptyset$. Then we want to show $S^{-1}\wp \subset S^{-1}R$ is prime. Let $\overline{S}$ be the image of S under the quotient map $\pi : R \to R/\wp$. Then we want to show $S^{-1}R/S^{-1}\wp$ is an integral domain. The ring homomorphism

$$S^{-1}R \to \overline{S^{-1}}(R/\wp) \qquad \frac{r}{s} \mapsto \frac{\pi(r)}{\pi(s)}$$

has kernel $S^{-1}\wp$. So by the first isomorphism theorem, we have

$$S^{-1}R/S^{-1}\wp \approx \overline{S^{-1}}(R/\wp).$$

By (ii), since $\wp \cap S = \emptyset$, we have $S^{-1}\wp = \wp^e$ is proper. Thus $\overline{S^{-1}}(R/\wp)$ is an integral domain since it is contained in the **field of fractions** of the integral domain $R/\wp$. Thus $S^{-1}\wp \subset S^{-1}R$ is prime.

□

We should add some remark on the proof of (iv). Let R be an integral domain. Then $S = R\backslash\{0\}$ is multiplicative. Write $\mathrm{Frac}(R)$ for $S^{-1}R$. Then this is called the **field of fractions** of R. The reason is that every nonzero element in $S^{-1}R$ is invertible, making $\mathrm{Frac}(R) = S^{-1}R$ a field.

Remark 2.11. In the proof above, $R/\wp$ is an integral domain, and since $R/\wp - \{0\}$ is the set of all elements of the form $\pi(r)$, where $r \notin \wp$, we have that $\mathrm{Frac}(R/\wp)$ is the set of all elements of the form $\pi(r)/\pi(r')$ with $r' \notin \wp$. Since $S \cap \wp = \emptyset$ as we argued above, we see that

$$R/\wp \subset \overline{S^{-1}}(R/\wp) \subset \mathrm{Frac}(R/\wp).$$

So $\overline{S^{-1}}(R/\wp)$ is "squeezed" between two integral domains, hence must be an integral domain.

We end this section with one more observation. Let $\wp$ be a prime ideal in R. Then let $R_\wp$ be the localization $S^{-1}R$ and $S = R\backslash\wp$. Then this is a local ring with maximal ideal $S^{-1}\wp$. Then I claim that we have the following commutative diagram:

$$\begin{array}{ccccc} R & \xrightarrow{f} & R_\wp & & \\ \downarrow{\scriptstyle \pi_\wp} & & & \searrow^{\pi_{\wp R_\wp}} & \\ R/\wp & \hookrightarrow & \mathrm{Frac}(R/\wp) & \xrightarrow{\approx} & R\wp/\wp R\wp \end{array}$$

What are the prime ideals in these rings? Going through the map $\pi_{\wp} : R \to R/\wp$, only prime ideals containing $\wp$ will survive by the correspondence theorem: ideals in $R/\wp$ are in correspondence with ideals in R containing $\wp$. And through the map $f : R \to R_{\wp} = S^{-1}R$, only prime ideals contained in $\wp$ will survive: by (iv) of the last proposition, prime ideals in R with $\wp \cap S = \emptyset$ are in correspondence with prime ideals in $S^{-1}R$. Now since $S = R \backslash \wp$, we have $q \cap S = \emptyset$ implies $q \subset \wp$. So only ideals contained in $\wp$ survive in $R_{\wp}$. The last isomorphism $\approx$ is left as an exercise.

CHAPTER 3

Modules

Note: We denote module isomorphisms by $\cong$ instead of $\approx$, following the notation of [1]. The $\approx$ is the notation used in [2]. But we use them interchangeably in this notes.

3.1 Modules and Module Homomorphisms

Definition 3.1. Let R be a commutative ring with 1. An abelian group M is called an **R-module** if there exists a function $a : R \times M \to M$ where $(r, m) \mapsto r \cdot m$ such that

(1) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ for all $r \in R, m_1, m_2 \in M$.

(2) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$ for all $r_1, r_2 \in R$ and $m \in M$.

(3) $(r_1 r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$ for all $r_1, r_2 \in R$ and $m \in M$.

(4) $1 \cdot m = m$ for all $m \in M$.

When there is no confusion, we will omit the dot and write $r \cdot m = rm$.

Example 3.2. Here are some examples of modules:

(1) The ring R is itself an R-module with addition and multiplication defined on R, and the map $a : R \times R \to R$ is simply multiplication $(r, s) \mapsto rs$.

(2) If I is an ideal of R, then I is also an R-module. This is because I is closed under multiplication by elements in R.

(3) If V is an vector space over the field F, then V is an F-module. In fact, the definition above applied to this special case is equivalent to the definition of an F-vector space, which we will take as our definition of a vector space.

(4) Let G be an abelian group, then G is a $\mathbb{Z}$-module by the following definition of $a : \mathbb{Z} \times G \to G$: For $n \in \mathbb{Z}, g \in G$, let

$$n \cdot g = \begin{cases} \underbrace{g + \cdots + g}_{n \text{ times}} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-g) + \cdots + (-g)}_{n \text{ times}} & n < 0. \end{cases}$$

In fact, all $\mathbb{Z}$-modules are abelian groups. So the notion of an abelian group and a $\mathbb{Z}$-module is equivalent.

(5) Let V be an F-vector space where F is a field. Let $\theta : V \to V$ be an F-linear map. Then we can regard V as an $F[x]$-module via the action

$$a : F[x] \times V \to V \qquad \left(\sum_i a_i x^i, v\right) \mapsto \sum_i a_i \theta^i(v).$$

Proposition 3.3. Let M be an R-module. Then we have

(i) $0 \cdot m = r \cdot 0 = 0$ for all $m \in M, r \in R$.

(ii) $(-r) \cdot m = r \cdot (-m) = -(r \cdot m)$ for all $m \in M, r \in R$.

Proof. Exercise. □

We make one remark. If M is an R-module and let $m \in M$. then

$$I = \{r \in R : r \cdot m = 0\}$$

is an ideal in R and M is naturally an R/I module via $(r + I, m) \mapsto r \cdot m$. This is well defined by the definition of I. We call I the **annihilator** of M in R, denoted by $\mathrm{Ann}_R(m)$.

Definition 3.4. Let M be an R-module. A subgroup N of the (additive) group M is called a **submodule** if $r \in R, n \in N$ implies $r \cdot n \in N$.

Proposition 3.5. A subset $N \subset M$ is a submodule iff it satisfies the following:

(i) $N \neq \emptyset$.

(ii) $n_1, n_2 \in N$ implies $n_1 + n_2 \in N$.

(iii) $r \in R, n \in N$ implies $r \cdot n \in N$.

Proof. This is just a restatement of the definition, and condition (i)-(iii) will imply N is a subgroup of M in addition. □

Example 3.6. Here are some example of submodules:

(1) If R is a commutative ring regarded as an R-module, then submodules of R are exactly ideals in R.

(2) If V is an F-vector space over a field, the submodules of V are exacly subspaces of V.

(3) If G is an abelian group regarded as a $\mathbb{Z}$-module, then submodules of G are exacly subgroups of G.

(4) If V is an F-vector space with an endomorphism $\theta : V \to V$, regarded as an $F[x]$-module, then submodules of V are exactly θ-invariant subspaces, i.e. subspaces $W \subset V$ such that $\theta(W) \subset W$.

Definition 3.7. Let R be a commutative ring with 1. Let M, N be R-modules. Then a grpup homomorphism $\phi : M \to N$ is called a **module homomorphism** or just a **R-homomorphism** if $\phi(r \cdot m) = r \cdot \phi(m)$, for all $r \in R$ and $m \in M$. If ϕ is a bijection, then it is an **isomorphism** and we write $M \cong N$.

The definition above is a generalization of linear maps over an F-vector space V. We use $\mathrm{Hom}_R(M, N)$ to denote all R-homomorphisms $\phi : M \to N$. Note that this is again naturally an R-module via the map

$$R \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N) \qquad (r, \phi) \mapsto (r \cdot \phi : m \mapsto r \cdot \phi(m)).$$

For example, if V, W are F-vector spaces, then $\mathrm{Hom}_R(V, W) = \mathcal{L}(V, W)$, the set of all linear maps from V to W. If G, H are abelian groups, then similarly $\mathrm{Hom}_{\mathbb{Z}}(G, H)$ are just all grpup homomorphisms between them.

Proposition 3.8. If $\phi : M \to N$ is an R-module, then $\mathrm{im}\,\phi = \phi(M)$ is a submodule of M, and $\ker\phi$ is a submodule of N.

Proof. Exercise. □

Definition 3.9. If $N \subset M$ is a submodule, then the quotient abelian group

$$M/N = \{m + N : m \in M\}$$

can be made into an R-module via the map

$$R \times M/N \to M/N \qquad (r, m + N) \mapsto (r \cdot m) + N.$$

This map is well-defined, because N is a subgroup (check). We call M/N the **quotient module**. Then the natural map $\pi : M \to M/N$ by $m \mapsto m + N$ is a module homomorphism.

Theorem 3.10 (1st Isomorphism Theorem)**.** *If $\theta : M \to M'$ is an R-module homomorphism, then θ induces an R-module isomorphism via the map*

$$M/\ker\theta \to \mathrm{im}\,\theta \qquad m + \ker\theta \mapsto \theta(m).$$

Proof. Same as for (abelian) groups. Exercise. □

3.2 Free Modules

Definition 3.11. Let M be an R-module, and $A \subset M$ a subset. The **submodule of M generated by** A is defined by

$$\langle A \rangle = \bigcap_{\text{submodule } A \subset N \subset M} N.$$

It is eacy to check that

$$\langle A \rangle = \left\{ \text{finite sums } \sum_i \lambda_i a_i : \lambda_i \in R, a_i \in A \right\}.$$

Definition 3.12. If an R-module M is generated by a set $A = \{a_i\}_{i\in I} \subset M$ (possibly infinite) and every element $m \in M$ can be written uniquely in the form $m = \sum_i \lambda_i a_i$ with $\lambda_i \in R, a_i \in A, \lambda_i = 0$ for all but finitely many is, then we say M is a **free module with basis A.**

Example 3.13. Here are some examples/nonexamples of free modules:

(1) R is a free module since $\{1\}$ is a basis.

(2) Similarly the n-fold product $R^n = R \times \cdots \times R$ is a free R-module with standard basis $\{e_i\}_{1\le i\le n}$.

(3) If F is a field, then every F-module is free: By definition, every F-module is an F-vector space, which admits a basis.

(4) $\mathbb{Z}/2\mathbb{Z}$ is NOT a free $\mathbb{Z}$-module: It is generated by 1, but the element $1 \cdot 1 = 3 \cdot 1 \in \mathbb{Z}/2\mathbb{Z}$ does not have a unique representation.

(5) Generalizing the nonexample above, if G is an abelian group which is not torsion-free, i.e. there exists an element $g \in G$ and $n \in \mathbb{Z}$ nonzero such that $ng = 0$, then $1 \cdot g = (1 + n) \cdot g$. Hence g does not have a unique representation by its basis element, making G impossible to be a free module.

We make an observation: If M is a free R-module with basis A, and N is another R-module, then any function $f : A \to N$ extends uniquely to an R-homomorphism $\theta_f : M \to N$ by defining

$$\theta_f\left(\sum_i \lambda_i a_i\right) = \sum_i \lambda_i f(a_i).$$

Proposition 3.14. Let L be a free R-module, and let $\phi : N \to N''$ be a surjective R-homomorphism, and $\theta : L \to N''$ be an R-homomorphism. Then there exists an R-homomorphism $\psi : L \to N$ such that $\phi \circ \psi = \theta$. That is, we have the diagram:

$$\begin{array}{ccc} & & L \\ & \overset{\exists\psi}{\swarrow} & \downarrow{\scriptstyle\theta} \\ N & \xrightarrow[\phi]{} & N'' \end{array}$$

Proof. Let $A = \{a_i\}_{i\in I}$ be a basis for L and for each i, choose $n_i \in N$ with $\phi(n_i) = \theta(a_i)$. Then define the function $f : A \to N$ by $f(a_i) = n_i$ and extend f uniquely to an R-homomorphism $\psi : L \to N$ such that

$$\psi\left(\sum_i \lambda_i a_i\right) = \sum_i \lambda_i n_i.$$

Then by construction,

$$\phi \circ \psi\left(\sum_i \lambda_i a_i\right) = \phi\left(\sum_i \lambda_i n_i\right) = \sum_i \lambda_i \phi(n_i) = \sum_i \lambda_i \theta(a_i) = \theta\left(\sum_i \lambda_i a_i\right).$$

□

Note that in general ψ is not unique. Any n_i such that $\phi(n_i) = \theta(a_i)$ can be used to define $\psi(a_i) = n_i$. Also, in general, the statement of the proposition above is not true when L is not free. For example, $\mathbb{Z}/2\mathbb{Z}$ is not free. Does there exist a ψ that makes the following diagram commute?

$$\begin{array}{ccc} & & \mathbf{Z}/2\mathbf{Z} \\ & \overset{\exists ?\psi}{\swarrow} & \downarrow 1 \\ \mathbf{Z} & \xrightarrow[\mod 2]{} & \mathbf{Z}/2\mathbf{Z} \end{array}$$

Suppose $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ has the desired property. Then let $\psi(1) = n \in \mathbb{Z}$. So then $2n = 2 \cdot \psi(1) = \psi(2 \cdot 1) = \psi(2) = \psi(0) = 0$. And $2n = 0$ is an equality in $\mathbb{Z}$, so $n = 0$. Thus $\psi \equiv 0$. So there is no way by composing ψ and $\mod 2$ we get the identity on $\mathbb{Z}/2\mathbb{Z}$.

In fact, the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ will continue to be important counterexamples in many cases, as we will see.

Proposition 3.15. Let M be an R-module, then there exists a free module L and a submodule $K \subset L$, such that $M \cong L/K$. Thus any module is a quotient of some free module.

Proof. First, we note that given any set A, we may construct a free R-module with basis A given by

$$R^A = \{\text{functions } f : A \to R \text{ with } f(a) = 0 \text{ for all but finitely many } a\}.$$

We can add functions, multiply them by elements in R. And note R^A has basis $\{\delta_a\}_{a \in A}$, where $\delta_a(m)$ is 1 if $m = a$ and is 0 otherwise.

Now let $A \subset M$ be any generating set, (e.g. $A = M$). Take $L := R^A$. Let $\theta : L \to M$ be the unique R-homomorphism extending the inclusion $f : A \to M$ by the following:

$$\theta\left(\sum_i \lambda_i \delta_{a_i}\right) = \sum_i \lambda_i f(a_i) = \sum_i \lambda_i a_i.$$

Then θ is surjective because A generates M. And set $K := \ker\theta$, use 1st isomorphism theorem we have $L/K \cong M$. □

3.3 Exact Sequences

Definition 3.16. A sequence of R-modules and R-Homomorphisms

$$\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \to \cdots$$

is called **exact** at M_i if $\text{im}(f_{i-1}) = \ker(f_i)$. A sequence like this is called an **exact sequence** if it is exact at every M_i, for $i = 1, 2, 3, ...$

Example 3.17. Here are three extremely important example that will serve as the building block of exact sequences:

(1) The following sequence is exact iff f is injective: $0 \to M' \xrightarrow{f} M$.

(2) The following sequence is exact iff g is surjective: $M \xrightarrow{g} M' \to 0$.

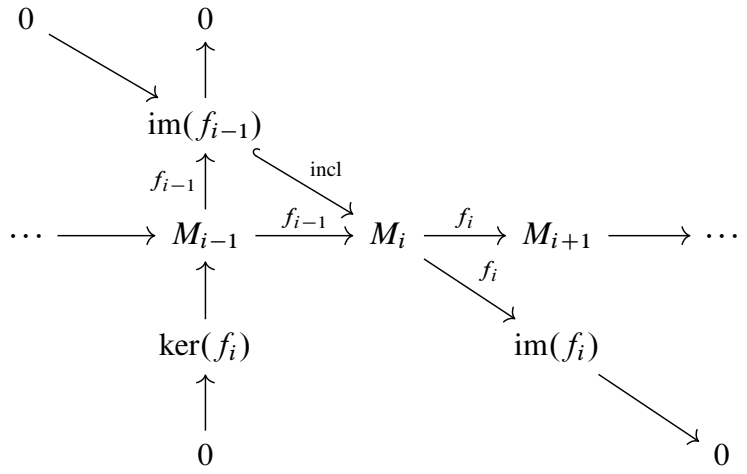
(3) The following sequence, known as a **short exact sequence**, is exact iff f is injective, g is surjective, and $\mathrm{im}(f) = \ker(g)$:

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

Here is an example of a short exact sequence. If $f : M \to N$ is an R-homomorphism, then

$$0 \to \ker(f) \xhookrightarrow{\text{incl}} M \xrightarrow{f} \mathrm{im}(f) \to 0$$

is a short exact sequence by (3) above. We also note that, any exact sequence can be split up into short exact sequences, specifically by the following, using the fact that $\mathrm{im}(f_{i-1}) = \ker(f_i)$:



and we can continue this process. The remaining of this section will be devoted to the following proposition. From a categorical language, this proposition says that Hom is a left exact functor.

Proposition 3.18.

(1) Let $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ be an exact sequence consisting of R-modules and R-homomorphisms. Then for any R-module M, the sequence

$$0 \to \mathrm{Hom}(M, N') \xrightarrow{\overline{f}} \mathrm{Hom}(M, N) \xrightarrow{\overline{g}} \mathrm{Hom}(M, N'')$$

is also exact. Here, we define $\overline{f}$ to be the map $\phi \mapsto f \circ \phi$, and similarly $\overline{g}$ to be the map $\psi \mapsto g \circ \psi$.

(2) Let $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be an exact sequence consisting of R-modules and R-homomorphisms. Then the sequence

$$0 \to \mathrm{Hom}(M', N) \xrightarrow{\overline{g}} \mathrm{Hom}(M, N) \xrightarrow{\overline{f}} \mathrm{Hom}(M'', N)$$

is also exact. Here we define $\overline{g} : \phi \mapsto \phi \circ g$ and $\overline{f} : \psi \mapsto \psi \circ f$.

Proof. We will only prove (1), since (2) is entirely analogous to (1). Suppose we have an exact sequence

$$0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$$

given above, to check that

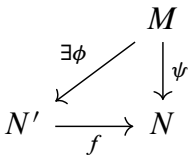
$$0 \to \mathrm{Hom}(M, N') \xrightarrow{\overline{f}} \mathrm{Hom}(M, N) \xrightarrow{\overline{g}} \mathrm{Hom}(M, N'')$$

is exact, we need to check two things:

- $\overline{f}$ is injective: Let $\phi \in \mathrm{Hom}(M, N')$ be such that $\overline{f}(\phi) = f \circ \phi = 0$. Then $\mathrm{im}\,\phi \subset \ker f$. But f is injective by assumption, so $\ker f = 0$ implies $\phi \equiv 0$.
- $\mathrm{im}(\overline{f}) = \ker(\overline{g})$: By definition, for any $\phi \in \mathrm{Hom}(M, N')$, we have

  $$(\overline{g} \circ \overline{f})(\phi) = \overline{g}(f \circ \phi) = g \circ f \circ \phi.$$

  Since $\mathrm{im}\, f = \ker g$ by exactness, we have $(\overline{g} \circ \overline{f})(\phi) = 0$ for arbitrary ϕ. Thus $\mathrm{im}(\overline{f}) \subset \ker(\overline{g})$. To prove the inclusion in other direction, let $\psi \in \ker \overline{g}$. Then $\overline{g}(\psi) = g \circ \psi = 0$. Thus $\mathrm{im}\,\psi \subset \ker g = \mathrm{im}\, f$ by exactness. Now let $m \in M$, then $\psi(m) \in \mathrm{im}(f)$ as we just saw. And since f is injective by exactness, there exists a unique $n' \in N'$ such that $\psi(m) = f(n')$. Then define the map $\phi : M \to N$ by letting $\phi(m)$ be the unique $n' \in N$ such that $\psi(m) = f(n')$. Then we have the following commutative diagram:

  Now, we see that ϕ is well-defined, because f is injective and $\mathrm{im}\,\psi \subset \mathrm{im}\, f$. Also, ϕ is R-linear since both ψ and f are. Finally, commutativity of the diagram implies $f \circ \phi = \psi = \overline{f}(\phi)$. So $\psi \in \mathrm{im}(\overline{f})$. Thus $\ker(\overline{g}) \subset \mathrm{im}(\overline{f})$. This gives the two-sided inclusion, hence the equality.

Together, these two condition will show that the desired sequence is indeed exact. □

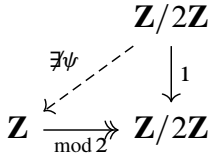
Remark 3.19. In the context of part (1) in the previous proposition, suppose now

$$0 \to N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$$

is exact. That is, suppose in addition g is surjective. Then obviously for general M, the sequence

$$0 \to \mathrm{Hom}(M, N') \xrightarrow{\overline{f}} \mathrm{Hom}(M, N) \xrightarrow{\overline{g}} \mathrm{Hom}(M, N'')$$

is still exact. But $\overline{g}$ need not be surjective in general even if g is. That is, the sequence above with "$\to 0$" added in the end need not be exact in general. For a counter example, we have shown that



So $1 : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is not in $\mathrm{im}(\overline{g})$. However, there are cases where $\overline{g}$ is surjective. And such a module M is called a **projective module**, which we will discuss later.

Similarly, in (2), if f is in addition injective, $\overline{f}$ need not be injective in general. But when the module N is chosen such that $\overline{f}$ is injective, N is called an **injective module**, which we will discuss later as well.

3.4 Snake's Lemma

Definition 3.20. Let $\alpha : M \to N$ be an R-homomorphism. Then define

$$\operatorname{coker}\alpha := N/\operatorname{im}\alpha.$$

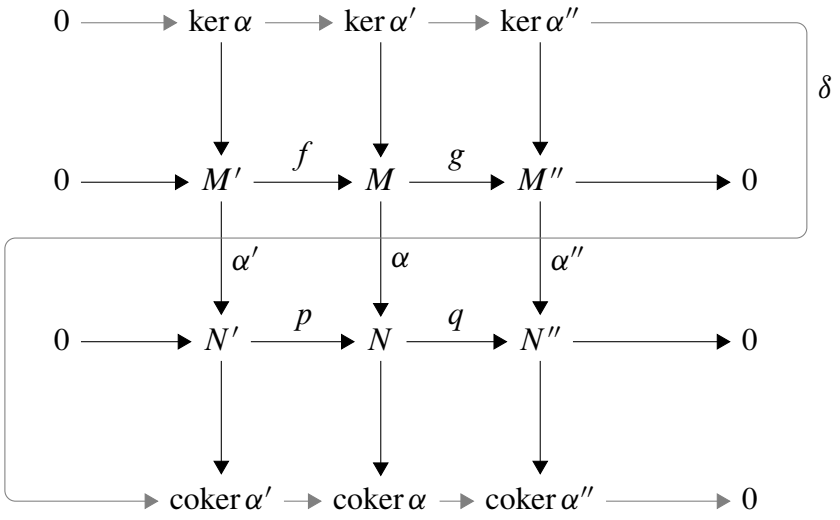
Proposition 3.21. Let the following be a commutative diagram of R-modules and R-homomorphisms with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha''} & & \\ 0 & \longrightarrow & N' & \xrightarrow[p]{} & N & \xrightarrow[q]{} & N'' & \longrightarrow & 0 \end{array}$$

Then there exists an exact sequence:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker\alpha' & \longrightarrow & \ker\alpha & \longrightarrow & \ker\alpha'' & & \\ & & & & & & & \searrow^{\delta} & \\ & & & & \operatorname{coker}\alpha' & \longrightarrow & \operatorname{coker}\alpha & \longrightarrow & \operatorname{coker}\alpha'' \longrightarrow 0. \end{array}$$

If we arrange the diagram as below, the boundary homomorphism $\delta : \ker\alpha'' \to \operatorname{coker}\alpha'$ "connects" the diagram like a snake, giving the lemma its name:

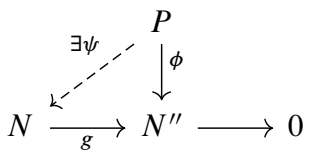


Proof. See [4] Lemma 4.7, which contains a full proof. □

3.5 Projective Modules

Theorem 3.22. *For an R-module P, the following are equivalent:*

(1) For every diagram of R-module and R-homomorphisms as follows, with g surjective, there exists $\psi : P \to N$ such that $\phi = g \circ \psi$.



(2) For every surjective R-homomorphism $g : N \to N''$, the induced map that we had before $\overline{g} : \mathrm{Hom}(P, N) \to \mathrm{Hom}(P, N'')$ given by $\overline{g}(\psi) = g \circ \psi$ is surjective.

(3) P is a direct summand of a free R-module: i.e. there exists a free R-module F and an R-module M such that $P \oplus M \cong F$.

(4) Every short exact sequence of the form

$$0 \to M \to N \xrightarrow{\alpha} P \to 0$$

***splits**, i.e. there exists $\beta : P \to N$ such that $\alpha \circ \beta = 1_P$.*

Proof. Clearly (1) and (2) are equivalent.

To show (2) implies (3): We know from Proposition 3.15 that P is the quotient of a free R-module F. So there exists a surjective R-homomorphism $g : F \to P$. Then by (2), the induced map $\overline{g} : \mathrm{Hom}(P, F) \to \mathrm{Hom}(P, P)$ is surjective. In particular, there exists $\psi : P \to F$, such that $g \circ \psi = 1_P$. Now

$$g \circ \psi = 1_P \Longrightarrow g \text{ is surjective and } \psi \text{ is injective.}$$

Injectivity of ψ follows by applying g to $\psi(p) = \psi(q)$ and gives $p = q$. If $p \in P$, then $g(\psi(p)) = p$ so g is surjective. Now let $M = \ker g$. We claim that then the map

$$\Phi : M \oplus P \to F \qquad (x, y) \mapsto x + \psi(y)$$

is an isomorphism. Clearly Φ is R-linear.

- Φ is injective: Let $(x, y) \in \ker \Phi$. Then $x \in M = \ker g$ in particular. Then $x + \psi(y) = 0$ implies $x = -\psi(y) = \psi(-y)$. So $0 = g(x) = g(\psi(-y)) = -y$ since $g \circ \psi = 1_P$. Then $y = 0$. So $x = -\psi(y) = 0$ as well and Φ is injective.

- Φ is surjective: Let $z \in F$. Consider the element $z' = z - \psi(g(z))$. Then $g(z') = g(z - \psi(g(z))) = g(z) - g \circ \psi(g(z)) = 0$. So $z' \in \ker g = M$. Thus $z = z' + \psi(g(z)) \in \mathrm{im}\, \Phi$. So Φ is surjective.

Thus we proved this direction.

To show (3) implies (2): Suppose P is such that $F \cong P \oplus M$ with F being a free module. Then by proportion 3.14, for any surjective $g : N \to N''$, the map $\overline{g} : \mathrm{Hom}(F, N) \to \mathrm{Hom}(F, N'')$ is also surjective. And since $F \cong P \oplus M$, we have that

$$\mathrm{Hom}(F, N) \cong \mathrm{Hom}(P, N) \oplus \mathrm{Hom}(M, N)$$
$$\mathrm{Hom}(F, N'') \cong \mathrm{Hom}(P, N'') \oplus \mathrm{Hom}(M, N'').$$

This forces $\overline{g} = \overline{g}_P \oplus \overline{g}_M$ to split as well. Thus $\overline{g}_P : \mathrm{Hom}(P, N) \to \mathrm{Hom}(P, N'')$ is surjective. This proves (2).

To show (1) implies (4): By (1), given a surjective R-homomorphism $\alpha : N \to P$, the map 1_P is in the image of $\overline{\alpha} : \mathrm{Hom}(P, N) \to \mathrm{Hom}(P, P)$ where $\overline{\alpha} : \beta \mapsto \alpha \circ \beta$. Since there exists a $\beta : P \to N$ with $\alpha \circ \beta = 1_P$, we have proven (4).

To show (4) implies (3): Let N be a free R-module. By exactness α is surjective. Now do exactly the same argument as we did in the proof of (2) implies (3) above, with F replaced by N and g replaced by α.

Thus we have shown that (1),(2),(3) are equivalent. And since (4) implies (3) and can be obtained from (1), we conclude that (4) is equivalent to (1),(2),(3), concluding the proof. □

Definition 3.23. An R-module satisfying the equivalent conditions (1)-(4) above is called a **projective R-module.**

Example 3.24. Free R-modules are projective by (3) of the theorem above.

Note that although free modules are projective, the converse is not necessarily true. Consider (once again) $P = \mathbb{Z}/2\mathbb{Z}$ as a module over $\mathbb{Z}/6\mathbb{Z}$ via

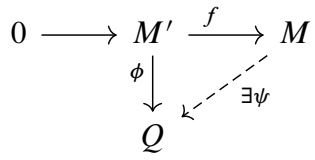
$$\mathbb{Z}/6\mathbb{Z} \times P \to P \qquad (a, b) \mapsto (a \bmod 2) \cdot b.$$

Now, $\mathbb{Z}/6\mathbb{Z} \cong P \oplus \mathbb{Z}/3\mathbb{Z}$ by the Chinese remainder theorem, with $\mathbb{Z}/6\mathbb{Z}$ being a free $\mathbb{Z}/6\mathbb{Z}$-module with basis 1. So P is projective. But P is not free, otherwise say $P = \langle 1 \rangle$ (since 0 is not a choice), then P must contain all elements of the form $\lambda \cdot 1$ with $\lambda \in \mathbb{Z}/6\mathbb{Z}$, and different λ corresponds to different elements uniquely. So $|P| = |\mathbb{Z}/2\mathbb{Z}| = |2| > 6$, which cannot be true.

3.6 Injective Modules

Lemma 3.25. *An R-module Q is called **injective** if it satisfies the following equivalemt conditions:*

(1) For every diagram below of R-modules and R-homomorphisms with f injective, there exists $\psi : M \to Q$ such that $\phi = \psi \circ f$.



(2) *For every injective* $f : M' \to M$*, the map* $\overline{f} : \mathrm{Hom}(M, Q) \to \mathrm{Hom}(M', Q)$ *defined by* $\overline{f} : \psi \mapsto \psi \circ f$ *is surjective.*

(3) *For every short exact sequence*

$$0 \to Q \xrightarrow{\alpha} N \to M \to 0$$

splits, i.e. there exists $\beta : N \to Q$ *such that* $\beta \circ \alpha = 1_Q$.

Proof. Parallel to the theorem of projective modules before. □

Theorem 3.26 (Baer's Lemma)**.** *Let* Q *be an* R*-module. If for all ideals* $I \subset R$*, every* R*-homomorphism* $\phi : I \to Q$ *extends to* R*, i.e. if the following diagram commutes,*

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \hookrightarrow & R \\ & & {\scriptstyle\phi}\downarrow & \swarrow_{\exists\psi} & \\ & & Q & & \end{array}$$

then Q *is an injective module.*

Proof. Consider a diagram of R-modules and R-homomorphisms with f injective:

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M \\ & & {\scriptstyle\phi}\downarrow & & \\ & & Q & & \end{array}$$

We want to show that ϕ extends to a homomorphism $\psi : M \to Q$, which proves the claim by (1) of the lemma above. We identify M' with its image under f, which is an injection. Therefore, we assume WLOG that M' is a submodule of M, i.e. $M' \subset M$ and the map f is given by inclusion. Consider the set

$$\mathscr{A} = \big\{\text{submodules } N \text{ s.t. } M' \subset N \subset M \text{ and } \exists \phi_N : N \to Q \text{ with } \phi_N|_{M'} = \phi\big\}.$$

That is, $\mathscr{A}$ is the set of all intermediate submodules between M' and M to which the map ϕ extends. This set $\mathscr{A}$ is ordered by the following relation:

$$N_1 \preceq N_2 \iff N_1 \subset N_2 \text{ and } \phi_{N_2}|_{N_1} = \phi_{N_1}.$$

Every chain has an upper bound, which is the union of all the chain elements. Hence by Zorn's lemma, there exists a maximal element N in $\mathscr{A}$. We claim that $N = M$.

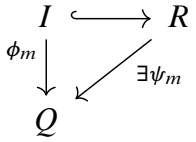
Suppose otherwise $N \subsetneq M$. Let $m \in M \backslash N$ and consider the ideal

$$I = \{r \in R : rm \in N\}.$$

By hypothesis, the R-homomorphism $\phi_m : I \to Q$ defined by

$$\phi_m : r \longmapsto rm \in N \xmapsto{\phi_N} \phi_N(rm) \in Q$$

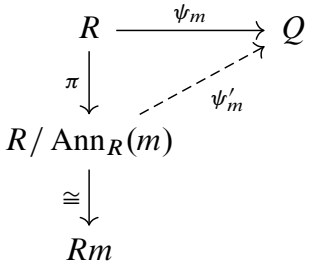
extends to R:



Clearly we have

$$\mathrm{Ann}_R(m) = \{r \in R : rm = 0\} \subset \ker \phi_m \subset \ker \psi_m.$$

Hence the map ψ_m factors as follows:



The isomorphism $R/\operatorname{Ann}_R(m) \cong Rm$ is given by the map $r \mapsto rm$ whose kernel is exactly $\mathrm{Ann}_R(m)$, and isomorphism follows from the first isomorphism theorem. The factored map $\psi_m : R/\operatorname{Ann}_R(m) \to Q$ is defined as

$$\psi'_m(r + \mathrm{Ann}_R(m)) = \psi_m(r).$$

This map is well-defined, for if $r + \mathrm{Ann}_R(m) = r' + \mathrm{Ann}_R(m)$, then $r - r' \in \mathrm{Ann}_R(m)$, and $\psi_m(r) - \psi_m(r') = \psi_m(r - r') = 0$ since $\mathrm{Ann}_R(m) \subset \ker \psi_m$. Also, we note that if $x \in Rm \cap N$, then we can write $x = rm$ for some $r \in R$. Then

$$\psi'_m(x) = \psi'_m(rm) = \psi_m(r) = \phi_m(r).$$

In the first step we identified $R/\operatorname{Ann}_R(m)$ with Rm, and in the second step we used the definition of ψ'_m. In the last step we used the fact that $rm \in N$ implies $r \in I$, so ϕ_m can take values on r. Thus

$$\psi'_m|_{Rm\cap N} = \phi_N|_{Rm\cap N}.$$

But since $m \in M\backslash N$, we have $N + Rm$ is strighly larger than N. And we can extend $\phi_N : N \to Q$ to the map $\phi_{N'} : N + Rm \to Q$ by $\phi'_N = \phi_N + \psi'_m$. That is, we let $\phi'_N = \phi_N$ on N and $\phi'_N = \psi'_m$ on Rm. This contradicts the maximality of N and $\phi|_N$. Thus we conclude that $N = M$, proving the claim. □

Definition 3.27. An abelian group G is called **divisible** if for every $n \in \mathbb{Z}\backslash\{0\}$, the multiplication by n map $G \to G, g \mapsto ng$ is surjective.

Proposition 3.28. Let G be an abelian group (thus also a $\mathbb{Z}$-module). Then G is an injective $\mathbb{Z}$-module iff G is divisible.

Proof. Suppose G is injective. Let $g \in G$ and $n \in \mathbb{Z}\backslash\{0\}$. Consider the following $\mathbb{Z}$-modules and $\mathbb{Z}$-homomorphisms, where we choose ϕ such that $g = \phi(1)$ (since ϕ is a

homomorphism, this is all the information we need to know what ϕ is) and let $f = \times n$ be the multiplcation map. Then there exists $\psi : \mathbb{Z} \to G$ such that $\phi = \psi \circ f$:

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{\times n} & \mathbf{Z} \\ {\scriptstyle\phi}\downarrow & \swarrow_{\exists\psi} & \\ G & & \end{array}$$

The existence of ψ follows from the hypothesis that G is injective. Then from commutativity of the diagram we have

$$g = \phi(1) = \psi(f(1)) = \psi(n \cdot 1) = n\psi(1).$$

And since $\psi(1) \in G$, we jabe that $g = n \times \psi(1) \in \text{im } f$. So G is divisible.

Conversely, let G be divisible. Then by Baer's lemma, we want to show for all ideals $I \subset \mathbb{Z}$, any $\mathbb{Z}$-homomorphism $\phi : I \to G$ can be extended to $\mathbb{Z}$. If $I = (0)$, then just take the extension to be the zero map. If I is not trivial, then since every ideal in $\mathbb{Z}$ is principal, we assume $I = (n)$ with $n \neq 0$. Let $g = \phi(n)$. Since G is divisible, we have $g = ng'$ for some $g' \in G$. Then let $\psi : \mathbb{Z} \to G$ by mapping 1 to g'. Then the following diagram commutes and ψ is an extension of ϕ:

$$\begin{array}{ccc} I = (n) & \hookrightarrow & \mathbf{Z} \\ {\scriptstyle\phi}\downarrow & \swarrow_{\exists\psi} & \\ G & & \end{array}$$

To see that ψ agrees with ϕ on I, we note

$$\psi(n) = \psi(n \times 1) = n \times \psi(1) = n \cdot g' = g.$$

And since ψ is a $\mathbb{Z}$-linear map that agrees with ϕ on the generator, they agree everywhere on I. This concludes the proof. □

3.7 Localization of Modules

Let R be a commutative ring with 1. Let M be an R-module. Let $S \subset R$ be a multiplicative set. We can define a relation $\sim$ on $M \times S$ by

$$(m, s) \sim (m', s') \iff t(ms' - sm') = 0 \text{ for some } t \in S.$$

Then this is an equivalence relation, as you should check. We then define

$$\frac{m}{s} = \{\text{equivalence classes of } (m, s)\}.$$

And we define

$$S^{-1}M = \left\{\frac{m}{s} : m \in M, s \in S\right\}.$$

Then $S^{-1}M$ is an $S^{-1}R$-module via

$$\frac{m}{s} + \frac{m'}{s'} = \frac{ms' + sm'}{ss'} \qquad \frac{r}{s} \cdot \frac{m}{t} = \frac{rm}{st}.$$

If $f : M \to N$ is an R-homomorphism, then the map

$$S^{-1}M \to S^{-1}N \qquad \frac{m}{s} \mapsto \frac{f(m)}{s}$$

is an $S^{-1}R$-module homomorphism. We denote this map by $S^{-1}f$.

Proposition 3.29. Let $M' \xrightarrow{f} M \xrightarrow{g} M''$ be an exact sequence of R-modules and R-homomorphisms, then

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

is an exact sequence of $S^{-1}R$-modules and $S^{-1}R$-homomorphisms.

Proof. We need to check that $\mathrm{im}(S^{-1}f) = \ker(S^{-1}g)$. On one hand, we know $\mathrm{im}(f) = \ker(g)$ by assumption, so $g \circ f \equiv 0$. Therefore $S^{-1}(g \circ f) \equiv 0$. Also, it is clear from definition that $0 = S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$. Thus we have $\mathrm{im}(S^{-1}f) \subset \ker(S^{-1})g$. This already gives half of the proof. Conversely, let $m/s \in \ker(S^{-1}g)$. So $g(m)/s = 0$. Thus by definition $tg(m) = 0$ for some $t \in S$. Since g is R-linear, we have that $g(tm) = 0$. So we get $tm \in \ker(g) = \mathrm{im}(f)$, which implies $tm = f(m')$ for some $m' \in M'$. Then we have that

$$\frac{m}{s} = \frac{tm}{ts} = \frac{f(m')}{ts} = S^{-1}f\left(\frac{m'}{ts}\right).$$

Therefore $\ker(S^{-1}g) \subset \mathrm{im}(S^{-1}f)$. This completes the proof. □

Corollary 3.30. *If $N \subset M$ is an R-submodule, then $S^{-1}N$ is an $S^{-1}R$-submodule of $S^{-1}M$. And we have a $S^{-1}R$-module isomorphism $S^{-1}M/S^{-1}N \cong S^{-1}(M/N)$.*

Proof. Apply Proposition 3.29 to the following exact sequence

$$0 \longrightarrow N \xhookrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0$$

where ι is the inclusion map and π is the natural projection. Then we will have an exact sequence

$$S^{-1}N \xhookrightarrow{S^{-1}\iota} S^{-1}M \xrightarrow{S^{-1}\pi} S^{-1}(M/N).$$

Then $S^{-1}\pi$ is a surjective homomorphism from $S^{-1}M$ to $S^{-1}(M/N)$ with $\ker(S^{-1}\pi) = \mathrm{im}(S^{-1}\iota) = S^{-1}N$. Now applying first isomorphism theorem concludes the proof. □

We introduce some notation now. Let R be a commutative ring with 1 and let $\wp$ be a prime ideal of R. Then $S = R\backslash\wp$ is a multiplicative set. We use the notation $M_\wp$ and $f_\wp$ to denote the localization module and maps $S^{-1}M$ and $S^{-1}f$.

Proposition 3.31. Let M be an R-module. Then the following are equivalent:

(1) $M = 0$.

(2) $M_\wp = 0$ for all prime ideal $\wp \subset R$.

(3) $M_m = 0$ for all maximal ideal $m \subset R$.

Proof. The implication (1) $\Rightarrow$ (2) is obvious. And since every maximal ideal is prime, we have (2) $\Rightarrow$ (3). It remains to show that (3) $\Rightarrow$ (1). We argue by contradiction. Suppose (3) holds but (1) fails. Then let $x \neq 0 \in M$. Then denote

$$I = \mathrm{Ann}_R(x) = \{r \in R : rx = 0\} \subsetneq R$$

be the annihilator of x in R, which is a proper ideal of R since $x \neq 0$, so $1 \notin I$. Therefore there exists some maximal ideal $m \subset R$ containing I by Theorem 1.18. Now since $x/1 \in M_m$ and by (3) we have $M_m = 0$. So $x/1 = 0$ implies $tx = 0$ for some $t \in R\backslash m \subset R\backslash I$ (since $m \supset I$). Then $t \notin I$. But $tx = 0$ implies $t \in \mathrm{Ann}_R(x) \in I$. So this gives the desired contradiction. □

Corollary 3.32. *Let $f : M \to N$ be an R-module homomorphism. Then the following are equivalent:*

(1) f is injective.

(2) $f_\wp : M_\wp \to N_\wp$ is injective for all prime ideal $\wp \subset R$.

(3) $f_m : M_m \to N_m$ is injective for all maximal ideal $m \subset R$.

Proof. To show (1) implies (2), let f be injective. So the sequence $0 \to M \xrightarrow{f} N$ is exact. By 3.29, the sequence

$$0 \to M_\wp \xrightarrow{f_\wp} N_\wp$$

is exact. So $f_\wp$ is injective for all prime ideals $\wp \subset R$. To prove that (2) implies (3), just use the fact that every maximal ideal is prime. To prove (3) implies (1), let $K = \ker f$. Then the sequence

$$0 \to K \hookrightarrow M \xrightarrow{f} N$$

is exact. Apply the proposition again gives an exact sequence

$$0 \to K_m \hookrightarrow M_m \xrightarrow{f_m} N_m$$

Therefore $\ker(f_m)$ is the image of the inclusion from K_m to M_m, which we identify with K_m. And by assumption of (3) we know that $K_m \cong \ker f_m = 0$. So by Proposition 3.31, we have $K = 0$ implies f is injective. □

Remark 3.33. In the statement of the corollary, the same holds if we replace "injective" by "surjective" everywhere. The proof is similar and is left as an exercise.

3.8 Noetherian Rings and Modules

Recall that an R-module M is called finitely generated if there exists $f_1, ..., f_r \in M$ such that $M = (f_1, ..., f_r)$. In other words, if every element in M is of the form $\sum_{i=1}^{r} \lambda_i f_i$ with $\lambda_i \in R$. From the experience of linear algebra, it would be reasonable to guess that every submodule of a finitely generated module is also finitely generated, since the subspace of every finite dimensional vector space is also finite dimensional. This, however, is not true in general. We give a counterexample below.

Example 3.34. Let k be a field and let $R = k[x_1, x_2, ...]$ be the polynomial ring over k with countably many variables. Then R, viewed as an R-module, is clearly finitely generated, since $R = (1)$. But the ideal $I = (x_1, x_2, ...) \subset R$ is not finitely generated as an R-module. $(f_1, ..., f_r) \subset I$. We want to show that this subset is proper in I. Then take $N > \max(\deg f_1, ..., \deg f_r)$. Then the variable $x_N, x_{N+1}, ...$ don't occur in any f_i. Then consider the the k-linear homomorphism $\varphi : R \to k$ defined by

$$\varphi : x_j \mapsto \begin{cases} 0 & 1 \leq j \leq N \\ 1 & j \geq N. \end{cases}$$

Note that if we pick any x_k for $k \geq N$, then $x_k \in I$ but $x_k \notin \ker\varphi$. Then since any element in $(f_1, ..., f_r)$ can be factored as a linear combination $r_1x_1 + \cdots + r_Nx_N$, we have that

$$(f_1, ..., f_r) \subset \ker\varphi \subsetneq I.$$

This counterexample motivates us to look at a nice subset of modules. Thus we introduce the following definition:

Definition 3.35. Let R be a commutative ring with 1.

- An R-module M is called a **Noetherian R-module** if every submodule of M is finitely generated. In particular, M itself is finitely generated.
- We say R is a **Noetherian ring** if R is Noetherian as an R-module. Equivalently, if every ideal of R is finitely generated.

Example 3.36. If F is a field, then F is a Noetherian ring, since the only ideals are $(0), (1)$. If V is an F-module (vector space), then V is Noetherian if and only if V is finite dimensional.

Example 3.37. If R is a PID, for example $\mathbf{Z}$, $F[x]$ where F is a filed, then every ideal is generated by a single element. Therefore it is a Noetherian ring. If M is a finitely generated R-module with R being a PID, then M is a Noetherian R-module. In fact, we will see that R can be any Noetherian ring.

Proposition 3.38. If M is a Noetherian R-module, then so is every submodule and every quotient module of M.

Proof. Let N be a submodule of M. Then every submodule of N is also a submodule of M, so finitely generated. It follows that N is Noetherian. For quotient, let M/N be a quotient module of M, i.e. N is a submodule of M. Let $L \subset M/N$ be a submodule, we want to show L is finitely generated. Let $q : M \to M/N$ be the natural projection. Consider $q^{-1}(L) \subset M$, this is a submodule (check this). So $q^{-1}(L) = (a_1, ..., a_r)$. Then we claim that

$$L = (q(a_1), ..., q(a_r)).$$

Clearly $q(a_i) \in L$. Let $\lambda \in L$. Then since q is surjective, we have $\lambda = q(m)$ for some $m \in q^{-1}(L)$. If we write $m = \sum_i r_i a_i$ then $\lambda = \sum_i r_i q(a_i)$. □

Definition 3.39. An R-module M satisfies the **ascending chain condition** (ACC) if any chain of submodules of M

$$N_1 \subset N_2 \subset N_3 \subset \cdots$$

eventually stabilizes, i.e. there exists $r \geq 1$ such that $N_r = N_{r+1} = N_{r+2} = \cdots$.

Theorem 3.40. *M is a Noetherian R-module if and only if M satisfies the ACC.*

Proof. Suppose M is Noetherian. Let $N_1 \subset N_2 \subset N_3 \subset \cdots$ be a chain of submodules of M. Let $N = \bigcup_{i \geq 1} N_i$. Then one can check that N is a submodule of M (in general no but in this case yes). So $N = (a_1, ..., a_r)$ since M is Noetherian. Then for some sufficiently large k we have $a_i \in N_k$ for all i. So $N = (a_1, ..., a_r) \subset N_k \subset N$. Thus the chain stabilizes at N_k.

Conversely, let $N \subset M$ be a submodule. We'll show this is finitely generated. Pick $a_1 \in N$. Then $(a_1) \subset N$. If $(a_1) = N$ we are done. Otherwise pick $a_2 \in N \backslash (a_1)$ and consider $(a_1, a_2) \subset N$, and repeat this process. Thus we have a chain

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

that will eventually stabilizes by ACC. Therefore, $N = (a_1, ..., a_n)$ for some n. □

Proposition 3.41. Let M be an R-module and $N \subset M$ be a submodule. If N and M/N are Noetherian, then so is M.

Proof. Let $L_1 \subset L_2 \subset \cdots$ be an ascending chain of submodules in M. We want to show this chain stabilizes. Now $L_1 \cap N \subset L_2 \cap N \subset \cdots$ is a chain of submodules of N. Let $q : M \to M/N$ be the projection then $q(L_1) \subset q(L_2) \subset \cdots$ is a chain of submodules of M/N. So these chains will stabilizes at some step, say:

$$L_r \cap N = L_{r+1} \cap N = \cdots \qquad q(L_r) = q(L_{r+1}) = \cdots .$$

The index r can be taken to be the same in both cases WLOG since we can take the max of both index. We claim that

$$L_r = L_{r+1} = \cdots$$

It suffices to show that $L_r \supset L_{r+1}$, and the case for $r + k$ follows. Let $m \in L_{r+1}$. Then $m + N = q(m) \in q(L_{r+1}) = q(L_r)$. So we can write $m + N = y + N$ for some $y \in L_r$. Then $m = y + n$ for some $n \in N$. Therefore $n = m - y \in N \cap L_{r+1} = N \cap L_r \subset L_r$ (since $m \in L_r$ and $y \in L_{r+1}$). Hence $m = n + y \in L_r$ (since $n, y \in L_r$). □

Corollary 3.42. *If M and N are Noetherian R-modules, then so is $M \oplus N$. In particular, if R is a Noetherian ring, then $R^n = \bigoplus_n R$ is Noetherian.*

Proof. Since $N \cong N \oplus \{0\} \subset N \oplus M$ is a submodule and $M \cong N \oplus M/(N \oplus \{0\})$, the claim follows from the previous proposition. □

Proposition 3.43. If R is a Noetherian ring and M is a finitely generated R-module, then M is Noetherian.

Proof. If M is generated by $(a_1, ..., a_n)$, then the map $\phi : R^n \to M$ defined by taking the ith standard basis e_i to a_i extended by linearity realizes $M \cong R^n / \ker \phi$. Since R^n is Noetherian by the corollary above, its quotient ring $R^n / \ker \phi$ is also Noetherian. Thus M is Noetherian. □

3.9 Hilbert's Basis Theorem

Theorem 3.44 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring, then so is $R[x]$.*

Proof. Let $J \subset R[x]$ be an ideal. We want to show that J is finitely generated. For each $n \geq 0$, consider

$$I_n := \{r \in R : J \text{ contains a polynomial of the form } f(x) = rx^n + \cdots\}.$$

Then Notice two things: (1) I_n is an ideal of R, since J is closed under $R[x]$-multiples, hence R-multiples. (2) $I_n \subset I_{n+1}$, since if $f(x) \in J$, then $xf(x)$ is also in J. Since R is a Noetherian ring, there exists $N \geq 0$, such that $I_N = I_{N+1} = I_{N+2} \cdots$. Now for each $0 \leq n \leq N$, we write

$$I_n = (a_n^1, ..., a_n^{k_n}).$$

Here k_n is some constant depending on n. We can do this since every ideal in R is finitely generated. Pick

$$f_n^j(x) = a_n^j x^n + \cdots \in J.$$

We claim that

$$J = (f_n^j(x))_{0 \leq n \leq N, 1 \leq j \leq k_n}.$$

Denote the thing on the right hand side by A, we say $J = \text{span}(A)$. Clearly $\text{span}(A) \subset J$ since $f_n^j(x) \in J$ for each $0 \leq n \leq N, 1 \leq j \leq k_n$ and J is an ideal. Now we show that $J \subset \text{span}(A)$.

Let $g(x) \in J$. WLOG assume $g(x) \neq 0$. We argue by induction on the number $\deg(g(x)) = d$. Write $g(x) = rx^d + \cdots$. If $d = 0$, then

$$r \in I_0 = (a_0^1, ..., a_0^k) = (f_0^1(x), ..., f_0^{k_0}(x)) \subset \text{span}(A)$$

since $\deg f_0^j = 0$. Now suppose $d > 0$. We have two cases:

1. If $d \leq N$, then $r \in I_d = (a_d^1, ..., a_d^{k_d})$ implies that $r = \sum_{j=1}^{k_d} \lambda_j a_d^j$ for some $\lambda_j \in R$. Consider $h(x) = \sum_{j=1}^{k_d} \lambda_j f_d^j(x) \in \text{span}(A) \subset J$. Then the leading term of $h(x)$ is rx^d. So we have $\deg(g(x) - h(x)) < d$. By induction hypothesis, $g(x) - h(x) \in \text{span}(A)$, and combined with the fact that $h(x) \in \text{span}(A)$ we have $g(x) \in \text{span}(A)$.

2. If $d > N$, then $r \in I_d = I_N$ by ACC. Write $r = \sum_{j=1}^{k_N} \lambda_j a_N^j$. Now argue just as above in 1 but now with $h(x) = (\lambda_1 f_N^1 + \cdots + \lambda_{k_N} f_N^{k_N}) x^{d-N} \in \text{span}(A)$.

This concludes the proof. □

CHAPTER 4

Tensor Products of Modules

4.1 Existence and Uniqueness of Tensor Product

Definition 4.1. Let R be a commutative ring with 1. Let M, N, P be R-modules. Then a function $f : M \times N \to P$ is called **bilinear** if it is linear on each argument:

$$f(rm_1 + m_2, n) = rf(m_1, n) + f(m_2)$$
$$f(m, rn_1, +n_2) = rf(m, n_1) + f(m, n_2).$$

for all $m, m_1, m_2 \in M, n, n_1, n_2 \in N, r \in R$.

Proposition 4.2. Let M, N be R-modules. Then there exists an unique pair of R-module $M \otimes_R N$ together with an R-bilinear map $g : M \times N \to M \otimes_R N$ satisfying the following **universal property**: For any R-module P and any R-bilinear map $f : M \times N \to P$, there exists a unique $f' : M \otimes_R N \to P$ such that $f = f' \circ g$. That is, the following diagram commutes:

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & P \\ {\scriptstyle g}\downarrow & \nearrow_{\exists! f'} & \\ M \otimes_R N & & \end{array}$$

Proof. We first prove the uniqueness of the pair $(M \otimes_R N, g)$. Suppose there is another pair (T, g') satisfying the universal property stated above. Then by the universal property of $M \otimes_R N$, we have the following diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{g'} & P \\ {\scriptstyle g}\downarrow & \nearrow_{\exists! j} & \\ M \otimes_R N & & \end{array}$$

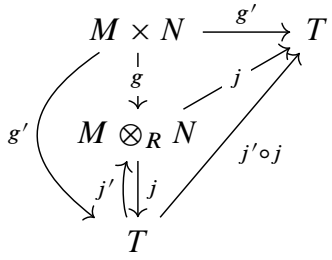
And similarly by the univeral property of the pair (T, g'), we have

$$\begin{array}{ccc} M \times N & \xrightarrow{g} & M \otimes_R N \\ {\scriptstyle g'}\downarrow & \nearrow_{\exists! j'} & \\ T & & \end{array}$$

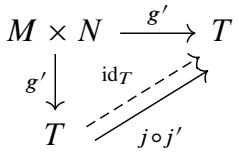
Thus we have the relation

$$g' = j \circ g \qquad g = j' \circ g'.$$

But notice that if we connect these two diagrams together we have



But then we have two choices of maps $T \to T$ to make the diagram below commutes:



And by the universal property of the pair (T, g'), we have that $j \circ j' = \mathrm{id}_T$. By a similar argument $j' \circ j = \mathrm{id}_T$. Therefore $M \otimes_R N \cong T$ via the isomorphism j, and the two maps are related by an isomorphism $g = j' \circ g$.

Next, we prove the existence of the pair $(M \otimes_R N, g)$. Let $R^{M\times N}$ be the free module with basis $M \times N$, that is, the set of all finite linear combinations $\sum_i \lambda_i(m_i, n_i)$ with $\lambda_i \in R$, and $m_i \in M, n_i \in N$. Next, consider $\langle A\rangle \subset R^{M\times N}$ generated over R by all "bilinear relators"

$$\begin{aligned} A = \{&(m_1 + m_2, n) - (m_1, n) - (m_2, n), (m, n_1 + n_2) - (m, n_1) - m(n_2), \\ &(rm, n) - r(m, n), (m, rn) - r(m, n) : m, m_1, m_2 \in M, n, n_1, n_2 \in N, r \in R\}. \end{aligned}$$

Now define $M \otimes_R N = R^{M\times N}/\langle A\rangle$, and let $g : M \times N \to M \otimes_R N$ be defined by sending the pair (m, n) to $q(e_{(m,n)})$, where $q : R^{M\times N} \to M \otimes_R N$ is the projection and $e_{(m,n)}$ is the basis element corresponding to (m, n). We abuse the notation and write $q(e_{(m,n)}) = q(m, n)$. And often this is denoted by $m \otimes n := q(m, n)$. Then notice that $M \otimes_R N$ is generated by elements of the form $m \otimes n$, subject to the bilinear relations

$$\begin{aligned} (m_1 + m_2) \otimes n &= m_1 \otimes n + m_2 \otimes n \\ m \otimes (n_1 + n_2) &= m \otimes n_1 + m \otimes n_2 \\ (rm) \otimes n &= m \otimes (rn) = r(m \otimes n). \end{aligned}$$

Now we check two things:

1. g is bilinear. This is easy from definition. We have that

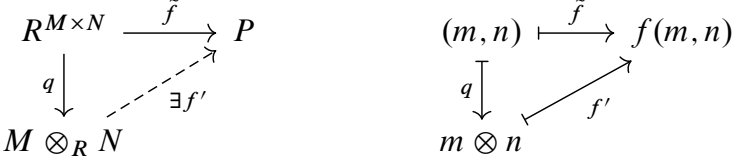
$$\begin{aligned} g(m_1 + m_2, n) = q(m_1 + m_2, n) &= q((m_1, n) + (m_2, n)) \\ &= q(m_1, n) + q(m_2, n) \\ &= g(m_1, n) + g(m_2, n). \end{aligned}$$

And all other bilinear relations follows similarly.

2. $(M \otimes_R N, g)$ satisfies the universal property. Let P be an R-module and $f : M \times N \to P$ be an R-bilinear map. Then f extends uniquely to an R-linear map $\tilde{f} : R^{M\times N} \to P$ by

$$\tilde{f} : \sum \lambda_i (m_i, n_i) \mapsto \sum_i \lambda_i f(m_i, n_i).$$

Since $\tilde{f}$ is bilinear, we have $\tilde{f}(a) = 0$ for all $a \in A$. So $\tilde{f}$ factors through the quotient $M \otimes_R N = R^{M\times N}/\langle A \rangle$:



and f' is uniquely determined by $m \otimes n \mapsto f(m,n)$, and it satisfies

$$f(m,n) = \tilde{f}(m,n) = f'(q(m,n)) = f'(g(m,n)).$$

So $f = f' \circ g$. This proves the universal property.

Therefore, we have proven the existence and uniqueness of the module $M \otimes_R N$. This module is called the **tensor product** of M and N over R. When the context is clear, we simply write $M \otimes N$. □

4.2 Properties of Tensor Products

Before we study some properties of tensor products, let us calculate a few examples:

Example 4.3. We claim that $(\mathbb{Z}/3\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) = 0$. To see this, let $a \in \mathbb{Z}_3, b \in \mathbb{Z}_2$. Then we see that

$$a \otimes b = 3(a \otimes b) - 2(a \otimes b) = (3a) \otimes b - a \otimes (2b) = 0.$$

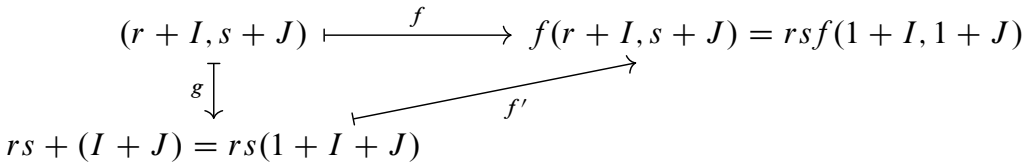
Example 4.4. Let R be a commutative ring with 1. Let $I, J \subset R$ be ideals (hence R-submodules of R). So $R/I, R/J, R/(I + j)$ are R-modules. Then we have

$$R/I \otimes R/J \cong R/(I + J).$$

In particular

$$(\mathbb{Z}/m\mathbb{Z}) \otimes (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z} \text{ where } d = \gcd(m,n).$$

To see the isomorphism above, we check that $R/(I + J)$ satisfies the univeral property of the tensor product. Let us consider the map $g : R/I \times R/J \to R/(I + J)$ be $(r + I, s + J) \mapsto rs + (I + J)$. Then g is bilinear. Let P be an R-module and f:$R/I \times R/J \to P$ be an R-bilinear map. We need to find an R-linear map $f' : R/(I + J) \to P$ such that $f = f' \circ g$. Note that



So f' must send $1+(I+J) \mapsto f(1+I, 1+J)$. And this uniquely determines f' with the desired property $f' : t+I+J \mapsto tf(1+I, 1+J)$ such that $f' \circ g = f$. So by the univeral property, we have $R/(I+J) \cong (R/I) \otimes_R (R/J)$.

Now we study the properties of tensor product. All of these can be proven by univeral property:

Proposition 4.5. Let L, M, N, M_1, M_2 be R-modules. We view R as R-module. Then:

(a) $R \otimes_R M \cong M$.

(b) $M \otimes_R N \cong N \otimes_R M$.

(c) $(L \otimes_R M) \otimes_R N \cong L \otimes_R (M \otimes_R N)$.

(d) $(M_1 \oplus M_2) \otimes_R N \cong (M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$.

Proof. All of these are proven via the univeral properties.

(a) The map $g : R \times M \to M$ by $(r, m) \to rm$ is R-bilinear. Given any R-bilinear map $f : R \times M \to P$, we have the diagram

$$\begin{array}{ccc} R \times M & \xrightarrow{f} & P \\ {\scriptstyle g}\downarrow & \nearrow_{\exists! f'} & \\ M & & \end{array} \qquad \begin{array}{ccc} (r,m) & \xmapsto{f} & f(r,m) = rf(1,m) \\ {\scriptstyle g}\downarrow & \nearrow_{\exists! f'} & \\ rm & & \end{array}$$

So there exists a unique map $f' : M \to P$ such that $f' \circ g = f$. Namely $f'(m) = f(1, m)$ for all $m \in M$ and extended bilinearly. Since the pair (M, g) satisfies the univeral property of $R \otimes_R M$, we conclude that they are isomorphic.

(b) Let $\psi_1 : (m, n) \to (n, m)$ and $\psi_2(n, m) = (m, n)$ for $m \in M, n \in N$. Then from the universal properties, we have the following commutative diagram:

$$\begin{array}{ccccc} M \times N & \xrightarrow{\psi_1} & N \times M & \xrightarrow{\psi_2} & M \times N \\ {\scriptstyle g}\downarrow & & {\scriptstyle g'}\downarrow & & {\scriptstyle g}\downarrow \\ M \otimes_R N & \xrightarrow[\exists! j]{} & N \otimes_R M & \xrightarrow[\exists! k]{} & M \otimes_R N \end{array}$$

But notice that if in the second row we choose $\mathrm{id}_{M \otimes_R N} : M \otimes_R N \to M \otimes_R N$, the diagram also commutes. Therefore by uniqueness we have $\mathrm{id}_{M \otimes_R N} = k \circ j$. If we reverse the arrow, we get $j \circ k = \mathrm{id}_{N \otimes_R M}$. Therefore $M \otimes_R N \cong N \otimes_R M$.

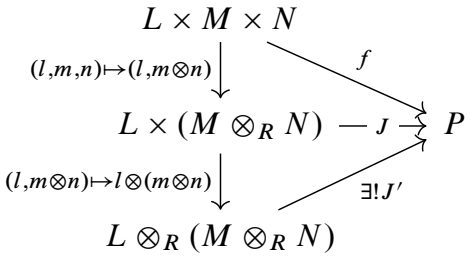
(c) We show the univeral property for R-trilinear map. Let P be an R-module and $f : L \times M \times N \to P$ be an R-trilinear map. For each $l \in L$, the map $f_l : M \times N \to P$ defined by $f_l(m, n) = f(l, m, n)$ is R-bilinear. So there exists a unique R-linear map $j_l : M \otimes_R N \to P$ such that

$$\begin{array}{ccc} M \times N & \xrightarrow{f_l} & P \\ \downarrow & \nearrow_{\exists! j_l} & \\ M \otimes_R N & & \end{array}$$

By varying $l \in L$, we get a map $J : L \times M \otimes_R N \to P$ via $J(l,h) = j_l(h)$. We check that J is R-bilinear. J is clearly linear on the second slot. To show J is linear on the first slot, let $l_1, l_2 \in L, r_1, r_2 \in R$, and we notice that

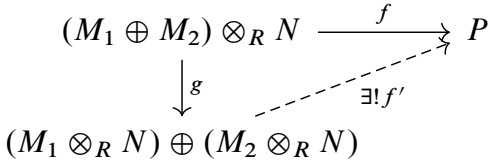
$$r_1 j_{l_1} + r_2 j_{l_2}$$

also makes the diagram above commute (check this). Therefore by uniqueness we have $j_{r_1 l_1 + r_2 l_2} = r_1 j_{l_1} + r_2 j_{l_2}$. Therefore, there exists an R-linear map J' such that the following diagram commutes:

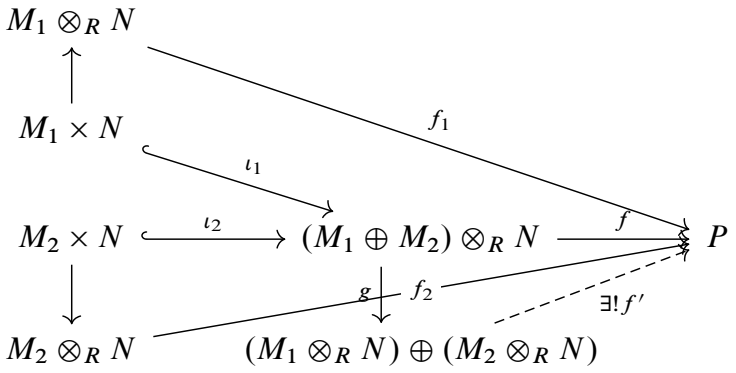


Thus $L \otimes_R (M \otimes_R N)$ together with the map $(l,m,n) \mapsto l \otimes (m \otimes n)$ satisfies the universal property of R-trilinear maps. A similar arguments shows that $(L \otimes_R M) \otimes_R N$ together with $(l,m,n) \mapsto (l \otimes m) \otimes n$ satisfies the same property. So they are isomorphic.

(d) Let $f : (M_1 \oplus M_2) \times N \to P$ be an R-bilinear map. Let $g : (M_1 \oplus M_2) \times N \to P \to (M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$ be the map such that $g(m_1 \oplus m_2, n) = (m_1 \otimes n, m_2 \otimes n)$. We will show that there exists a unique R-linear map f' such that the diagram below commutes:



Namely, this map is given by $f' = f_1 \oplus f_2$, where f_1 is induced by the universal property of $M_1 \otimes_R N$ and the map $f \circ \iota_1$, where $\iota_1 : M_1 \times N \to (M_1 \oplus M_2) \times N$ is the natural inclusion. And similarly for f_2. That is, we consider the following diagram:



And it is not hard to show that f' makes the diagram above commutes. So $(M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$ satisfies the same univeral property as $(M_1 \oplus M_2) \otimes_R N$, concluding the proof that they are isomorphic.

□

Corollary 4.6. $R^m \otimes_R R^n \cong R^{mn}$.

Proof. By (d) above, we have that $R^m \otimes_R R^n = R^m \otimes_R \left(\bigoplus^n R\right) \cong \bigoplus^n R^m = R^{mn}$. □

4.3 Exactness Properties of Tensor Product

Definition 4.7. Let $f : M \to M', g : N \to N'$ be R-linear maps. Then the map

$$\begin{aligned} \eta : M \times N &\to M' \otimes_R N' \\ (m, n) &\mapsto f(m) \otimes g(n) \end{aligned}$$

is R-bilinear. Therefore, there exists a unique R-bilinear map, denoted by $f \otimes g$, such that the diagram below commutes:

$$\begin{array}{ccc} M \times N & \xrightarrow{\eta} & M' \times N' \\ \downarrow & \nearrow_{\exists! f \otimes g} & \\ M \otimes_R N & & \end{array}$$

And by looking at the diagram, we see that

$$f \otimes g(m \otimes n) = f(m) \otimes g(n).$$

This map $f \otimes g$ is called **tensor product of maps f and g.**

Lemma 4.8. *A sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact if and only if for all R-module P, the sequence*

$$0 \to \mathrm{Hom}_R(M'', P) \xrightarrow{\overline{g}} \mathrm{Hom}_R(M, P) \xrightarrow{\overline{f}} \mathrm{Hom}_R(M', P)$$

is exact. Recall that $\overline{g} : \mathrm{Hom}(M'', P) \to \mathrm{Hom}_R(M, P)$ is defined by $\overline{g}(\phi) = \phi \circ g$, and similarly $\overline{f}(\psi) = f \circ \psi$.

Proof. The "if" part is proven already (Proposition 3.18). To prove the "only if" part, suppose the second sequence is exact. We check two things:

- g is surjective: Take $P = M''/\operatorname{im} g$. Let $\pi : M'' \to P$ be the projection, so $\ker \pi = \operatorname{im} g$. Thus $\pi \circ g \equiv 0$. But $\pi \circ g = \overline{g}(\pi) = 0$. So by exactness of the second sequence, we have that $\overline{g}$ is injective, i.e. $\pi \equiv 0$. So $\operatorname{im} g = \ker \pi = M$.

- $\operatorname{im} f = \ker g$: Take $P = M'', \phi = \mathrm{id}_{M''}$. We have that

$$0 = (\overline{f} \circ \overline{g})(\mathrm{id}_{M''}) \circ g \circ f.$$

This shows that $g \circ f = 0$ and $\operatorname{im} f \subset \ker g$. Conversely, let $P = M/\operatorname{im} f$. So $\pi \circ f = \overline{f}(\pi) = 0$. Therefore $\pi \in \ker \overline{f} = \operatorname{im} \overline{g}$ by exactness of the second sequence. So $\pi = \phi \circ g$ for some $\phi \in \mathrm{Hom}_R(M'', P)$. Then $\operatorname{im} f = \ker \pi \supset \ker g$ and we are done. The last inclusion is due to the observation that if $g(x) = 0$ then $\pi(x) = \phi \circ g(x) = 0$.

This concludes the proof. □

The following lemma says that $\otimes$ and Hom are adjoint functors.

Lemma 4.9. *There is a natural isomorphism*

$$\mathrm{Hom}_R(M \otimes_R N, P) \xrightarrow{\simeq} \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

Proof. There is a 1:1 correspondence α from the set of R-bilinear maps $M \times N \to P$ to $\mathrm{Hom}_R(M \otimes_R N, P)$, where $\alpha(f)$ is the unique f' such that the universal property of $M \otimes_R N$ is satisfied. Also, there is a map β from the set of all R-bilinear maps $M \times N \to P$ to $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$, where $\beta(f)$ is the R-linear map $m \mapsto f(m, \cdot) \in \mathrm{Hom}_R(N, P)$. And the isomorphism above is realized via $\beta \circ \alpha^{-1}$. □

The next proposition, in summary, says that $\otimes$ is a right-exact functor.

Proposition 4.10. Let $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be an exact sequence. Then for any R-module N, the sequence

$$M' \otimes N \xrightarrow{f \otimes \mathrm{id}} M \otimes N \xrightarrow{g \otimes \mathrm{id}} M'' \otimes N \to 0$$

is also exact.

Proof. By the left exactness of Hom (See Proposition 3.18), we have the following exact sequence by applying the functor $\mathrm{Hom}_R(-, \mathrm{Hom}_R(N, P))$:

$$0 \to \mathrm{Hom}_R(M'', \mathrm{Hom}_R(N, P)) \xrightarrow{\overline{g}} \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \xrightarrow{\overline{f}} \mathrm{Hom}_R(M', \mathrm{Hom}_R(N, P)).$$

By the previous lemma, this induces the following exact sequence:

$$0 \to \mathrm{Hom}(M'' \otimes N, P) \xrightarrow{f \otimes \mathrm{id}} \mathrm{Hom}(M \otimes N, P) \xrightarrow{g \otimes \mathrm{id}} \mathrm{Hom}(M' \otimes N, P).$$

By Lemma 4.8, the sequence above is exact if and only if the sequence below is exact:

$$M' \otimes N \xrightarrow{f \otimes \mathrm{id}} M \otimes N \xrightarrow{g \otimes \mathrm{id}} M'' \otimes N \to 0.$$

This proves the claim. □

Now we are in a similar position as we were in the discussion of projective and injective modules. Now, suppose that in addition, the sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact. Then the sequence

$$0 \to M' \otimes N \xrightarrow{f\otimes \mathrm{id}} M \otimes N \xrightarrow{g\otimes \mathrm{id}} M'' \otimes N \to 0$$

need not be exact. The problem is that $f \otimes \mathrm{id}$ need not be injective. This can be shown via the following counterexample:

Example 4.11. Consider the $\mathbb{Z}$-module exact sequence (abelian groups)

$$0 \to \mathbb{Z} \xrightarrow[\times 2]{f} \mathbb{Z} \xrightarrow[\text{mod } 2]{g} \mathbb{Z}/2\mathbb{Z} \to 0.$$

Applying $\otimes_{\mathbb{Z}} N$ with $N = \mathbb{Z}/2\mathbb{Z}$ we obtain

$$0 \to \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{f\otimes \mathrm{id}} \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{g\otimes \mathrm{id}} \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \to 0.$$

This is not exact, since $f \otimes \mathrm{id}$ is not injective: For all $x \otimes y \in \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$, we have that

$$(f \otimes \mathrm{id})(x \otimes y) = f(x) \otimes \mathrm{id}(y) = 2x \otimes y = x \otimes (2y) = x \otimes 0 = 0.$$

We will remedy the situation, again, by introducing a class of nice modules called flat modules.

4.4 Flat Modules

Definition 4.12. We say an R-module N is **flat** over R if for every R-module exact sequence

$$\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \to \cdots$$

the sequence

$$\cdots \to M_{i-1} \otimes N \xrightarrow{f_{i-1}\otimes \mathrm{id}} M_i \otimes N \xrightarrow{f_i \otimes N} M_{i+1} \otimes N \to \cdots$$

is also exact.

Proposition 4.13. Let N be an R-module. Then the following are equivalent:

(1) N is flat over R.

(2) If $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is a short exact sequence of R-modules, then

$$0 \to M' \otimes N \xrightarrow{f\otimes \mathrm{id}} M \otimes N \xrightarrow{g\otimes \mathrm{id}} M'' \otimes N \to 0$$

is also exact.

(3) For any injective R-homomorphism $f : M' \to M$ with M, M' arbitrary R-modules, the R-homomorphism $f \otimes \mathrm{id} : M' \otimes_R N \to M \otimes_R N$ is also injective.

(4) For any injective R-homomorphism $f : M' \to M$ with M, M' finitely generated R-modules, the R-homomorphism $f \otimes \mathrm{id} : M' \otimes_R N \to M \otimes_R N$ is also injective.

Proof. (1) $\Rightarrow$ (2) follows from definition, and (2) $\Rightarrow$ (1) since every exact sequence splits into short exact sequences. (2) $\Leftrightarrow$ (3) follows from Proposition 4.10 and the remarking following it, which suggests that (2) fails if and only if $f \otimes \mathrm{id}$ is not injective. (3) $\Rightarrow$ (4) is clear. So the only statement that needs some work is (4) $\Rightarrow$ (3).

To prove this claim, suppose that (4) holds and that $f : M' \to M$ is an injective R-homomorphism with M', M arbitrary. Let $u \in \ker(f \otimes \mathrm{id} : M' \otimes N \to M \otimes N)$. We want to show $u = 0$. We write

$$u = \sum_{i=1}^{n} x_i \otimes y_i \text{ with } x_i \in M', y_i \in N$$

where we have absorbed constant λ_is into x_is. Then consider the restriction of f to the span of $\{x_i\}$s, denoted by f_0. By (4), $f_0 \otimes \mathrm{id}$ is injective. Since

$$\begin{aligned} 0 = (f \otimes \mathrm{id})(u) = (f \otimes \mathrm{id})\left(\sum_{i=1}^{n} x_i \otimes y_i\right) = \sum_{i=1}^{n} f(x_i) \otimes y_i = \sum_{i=1}^{n} f_0(x_i) \otimes y_i \\ = (f_0 \otimes \mathrm{id})(u) \end{aligned}$$

we have that $u = 0$, as desired. □

Example 4.14. If N is free, then N is flat (over R). Indeed, suppose $N \cong R^n$ (the infinite case is similar) and $g : M' \hookrightarrow M$ is injective. Consider $g \otimes \mathrm{id} : M' \otimes_R N \to M \otimes_R N$. But the isomorphism $M' \otimes N \cong M' \otimes R^n \cong (M')^n$ and similarly for M implies we have the following diagram:

$$\begin{array}{ccc} M' \otimes_R N & \xrightarrow{g \otimes \mathrm{id}_N} & M \otimes_R N \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} \\ (M')^n & \xrightarrow[g^n]{} & M^n \end{array}$$

Now, $g^n = \oplus^n g$ is injective, and φ, ψ^{-1} are bijections, so $g \otimes \mathrm{id}_N$ is also injective.

4.5 Restriction and Extension of Scalars

Definition 4.15. Let $f : R \to S$ be a ring homomorphism.

(1) If N is an S-module, then N becomes an R-module via

$$\begin{aligned} R \times N &\to N \\ (a, n) &\mapsto f(a)n. \end{aligned}$$

This is called **restriction of scalars** of N from R to S.

(2) If M is an R-module, then $M_S := M \otimes_R S$, which is an R-module (since S has R-module structure), becomes an S-module via

$$\begin{aligned} S \times M_S &\to M_S \\ (s, m \otimes b) &\mapsto m \otimes sb. \end{aligned}$$

This is called the **extension of scalars** of M from R to S.

Proposition 4.16. Let $f : R \to S$ be a ring homomorphism, M be an R-module and N, P be S-modules. Then we have

$$M \otimes_R (N \otimes_S P) \cong (M \otimes_R N) \otimes_S P.$$

This equation can be viewed as either an R-homomorphism or an S-homomorphism via the following two perspectives:

- $N \otimes_S P$ is an S-module, which can be viewed as an R-module via restriction of scalars, thus the LHS is an R-module. Similarly, $(M \otimes_R N)$ can be viewed as an S-module via extension of scalars. So $(M \otimes_R N) \otimes_S P$ is an S-module, which becomes an R-module via restriction on scalars.
- $N \otimes_S P$ is an S-module, so $M \otimes_R (N \otimes_S P)$ can be viewed as an S-module via extension of scalars. Similarly, $M \otimes_R N$ can be viewed as an S-module via extension of scalars, so the RHS is also an S-module.

Proof. Basically the same as associativity of tensor products, so we omit the proof. □

Corollary 4.17. *Let $f : R \to S$ be a ring homomorphism, and M be an R-module. Then M is R-flat implies that M_S is S-flat. Thus flatness is preserved under extension of scalars.*

Proof. Let $g : N' \hookrightarrow N$ be an injective S-homomorphism. This is also an injective R-homomorphism by restriction of scalars. Since M is R-flat, we have that $g \otimes \mathrm{id}_M$ is injective. Then we have the following diagram:

$$\begin{array}{ccc} N' \otimes_R M & \xrightarrow{g \otimes \mathrm{id}_M} & N \otimes_R M \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} \\ (N' \otimes_S S) \otimes_R M & & (N' \otimes_S S) \otimes_R M \\ \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_2} \\ N' \otimes_S M_S & \xrightarrow[g \otimes \mathrm{id}_{M_S}]{} & N \otimes_S M_S \end{array}$$

where $\varphi_1, \varphi_2, \psi_1, \psi_2$ are all isomorphisms. Since the diagram commutes, we have that $g \otimes \mathrm{id}_{M_S}$ is also injective. Thus M_S is S-flat. □

However, note that for arbitrary ring homomorphism $f : R \to S$, if we assume M_S is S-flat, then M need not be R-flat. That is, the converse of the corollary above need not be true. For example, take $f : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be the natural projection and $M = \mathbb{Z}/2\mathbb{Z}$ viewed as a $\mathbb{Z}$-module. Then

$$M_S = (\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

is a flat $\mathbb{Z}/2\mathbb{Z}$-module since it is free (Example in the last section). But we already saw that $\mathbb{Z}/2\mathbb{Z}$ is not flat over $\mathbb{Z}$ by the example in section 4.3.

4.6 Local Nature of Flatness

Proposition 4.18. Let $S \subset R$ be a multiplicative subset, and M be an R-module. Then we have

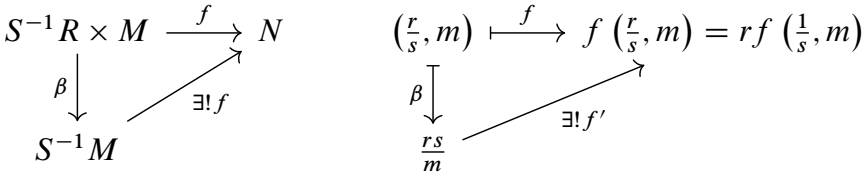
$$(S^{-1}R) \otimes_R M \cong S^{-1}M$$

where the RHS is the localization of module M.

Proof. Consider the R-bilinear map

$$\begin{aligned} \beta : S^{-1}R \times M &\to S^{-1}M \\ \left(\frac{r}{s}, m\right) &\mapsto \frac{rm}{s}. \end{aligned}$$

If $f : S^{-1}R \times M \to N$ is any R-bilinear map and N is an arbitrary R-module, and f' is the map that makes the following diagram commutes:



Then $f' : \frac{m}{s} \mapsto f(\frac{1}{s}, m)$ is the unique R-linear map such that the diagram commutes. Thus by the univeral property of $(S^{-1}R) \otimes_R M$, we have the desired isomorphism. □

An example of this is given by the following: Recall that if R is a local ring with m being the unique maximal ideal, then $S = R \backslash m$ is a multiplicative subset. Denote $S^{-1}R = R_m$. Then by the Proposition above we have that

$$R_m \otimes_R M \cong S^{-1}M = M_m.$$

The same result holds if we consider a ring R with the multiplcative subset $S = R \backslash \wp$ where $\wp$ is a prime ideal. Then we have that

$$R_\wp \otimes_R M \cong S^{-1}M = M_\wp.$$

Corollary 4.19. *For any multiplcative subset $S \subset R$, $S^{-1}R$ is R-flat.*

Proof. If M is an R-module and $M' \subset M$ a submodule (this is sufficient instead of considering any injection $M' \hookrightarrow M$). Then $S^{-1}M' \subset S^{-1}M$ is a submodule. By the Proposition above we have the isomorphism $S^{-1}M' \cong (S^{-1}R) \otimes_R M'$ and $S^{-1}M \cong (S^{-1}R) \otimes_R M$. This proves the claim. □

Now we prove a statement which says that flatness is a local property:

Proposition 4.20. Let M be an R-module. Then the following are equivalent:

(1) M is flat over R.

(2) $M_\wp$ is flat over $R_\wp$ for all prime ideals $\wp \subset R$.

(3) M_m is flat over R_m for all maximal ideals $m \subset R$.

Proof. (1) $\Rightarrow$ (2): Let M be R-flat. Since flatness is preserved under extension of scalars by Corollary 4.17, if M is R-flat, then $M_\wp \cong R_\wp \otimes_R M$ is $R_\wp$-flat if we consider the natural ring homomorphism $f : R \to R_\wp$.

(2) $\Rightarrow$ (3) is easy since any maximal ideal is prime.

To show (3) $\Rightarrow$ (1): Let $g : N' \to N$ be an injective R-homomorphism. We want to show that $g \otimes \mathrm{id}_M$ is injective. Let $K = \ker(g \otimes \mathrm{id}_M : N' \otimes_R M \to N \otimes_R M)$. We need to show $K = 0$. We notice that from definition the following R-module sequence is exact:

$$0 \to K \to N' \otimes M \xrightarrow{g \otimes \mathrm{id}} N \otimes M.$$

For any $m \subset R$ maximal, we know R_m is R-flat by Corollary 4.19. So tensor the sequence above by R_m gives the exact sequence in the first row below, and the diagram commutes with vertical maps all being isomorphisms by Proposition 4.18:

$$\begin{array}{ccccccc} 0 & \longrightarrow & K \otimes_R R_m & \xrightarrow{\text{incl}} & N' \otimes_R R_m & \xrightarrow{g \otimes \mathrm{id}_M \, \mathrm{id}_{R_m}} & N \otimes_R R_m \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & K_m & \longrightarrow & N'_m \otimes_{R_m} M_m & \longrightarrow & N_m \otimes_{R_m} M_m \end{array}$$

where we have used the equality

$$N' \otimes_R \otimes_R R_m \cong N' \otimes_R M_m \cong N' \otimes_R (R_m \otimes_{R_m} M_m) \cong N'_m \otimes_{R_m} M_m$$

where we have repeatedly used Proposition 4.18. Therefore the sequence of the second row is also exact, hence

$$K_m \cong \ker(N'_m \otimes_{R_m} M_m \to N_m \otimes_{R_m} M_m).$$

But $g : N' \to N$ is injective, and R_m is R-flat. Therefore the map $g \otimes \mathrm{id}_{R_m} : N' \otimes_R R_m \to N \otimes_R R_m$ is injective. Since $N' \otimes_R R_m = N' \otimes_R (S^{-1}R) \cong S^{-1}N' = N'_m$ and similarly $N \otimes_R R_m \cong N_m$, and by the assumption that M_m is R_m-flat, we have that the map $N'_m \otimes_{R_m} M_m \to N_m \otimes_{R_m} M_m$ is injective. Thus $K_m = 0$. And since $K_m = 0$ for all maximal ideals $m \subset R$, we have that $K = 0$ by Proposition 3.31. □

4.7 Equivalence of Flatness and Free

The last section of this chapter is dedicated to the goal of proving the following theorem:

> **Theorem.** Let (R, m) be a local ring with residule field $\kappa = R/m$ and let M be a finitely generated module. Then M is R-flat if and only if M is R-free.

This is such a nice result, and few nice results in mathematics can be obtained without hard work. Indeed, to be able to carry out this long and technical proof, we need a number of preliminary results first. We start with a Proposition, which is a generalization of Caley-Hamilton theorem in linear algebra:

Proposition 4.21. Let M be a finitely generated R-module and $I \subset R$ be an ideal. If $\phi : M \to M$ is an endomorphism, i.e. R-linear map to itself, such that $\phi(M) \subset IM$, then ϕ satisfies an equation of the form

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n = 0$$

where $a_i \in I$.

Proof. Let $\{x_1, \cdots, x_n\}$ be a generating set for M. Then $\phi(x_i) \in IM$, so we can write

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j \text{ with } a_{ij} \in I.$$

So we have the system of equations

$$\begin{pmatrix} \phi - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \phi - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \phi - a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

The matrix on the LHS has entries in the ring $\mathrm{End}_R(M)$. If we denote this big $n \times n$ matrix by A and the column vector by x, then we have $Ax = 0$. Let $\mathrm{adj}(A)$ denote the adjugate matrix of A. Then we have $\mathrm{adj}(A)Ax = 0$. But since we have the identity

$$\mathrm{adj}(A) \cdot A = (\det A) \cdot 1_{n\times n}$$

which is a generalize version of the determinant formula $A^{-1} = \mathrm{adj}(A)/\det A$ from linear algebra, except now A need not be invertible. Therefore

$$\begin{aligned} \mathrm{adj}(A) \cdot Ax = 0 \Rightarrow (\det A)x_i = 0 \forall i &\Rightarrow (\det A) = 0 \forall m \in M \\ &\Leftrightarrow (\det A) \cdot \mathrm{id}_M = 0 \in \mathrm{End}_R(M). \end{aligned}$$

Expanding $\det A$ in the last equation gives the desired equation. □

Corollary 4.22 (Nakayama's Lemma)**.** *Let (R, m) be a local ring with m maximal. Let M be a finitely generated R-module. Then $mM = M$ implies $M = 0$.*

Proof. Take $\phi = \mathrm{id}_M$ in the Proposition above. We get that

$$\mathrm{id}_M + a_1 \mathrm{id}_M + \cdots + a_n = 0 \in \mathrm{End}_R(M) \quad \text{where } a_i \in m.$$

So we get $(1 + a_1 + \cdots + a_n)\,\mathrm{id}_M = 0$. But $x := 1 + a_1 + \cdots + a_n \equiv 1 (\mathrm{mod}\, m)$. Therefore $x \notin m$. Since R is local, we have that x is invertible in R: If x is not a unit, then (x) is proper, so $(x) \subset m$ implies $x \in m$ by Theorem 1.18. Now since x is invertible and $x\,\mathrm{id}_M = 0$, if we take any $y \in m$, we have that $x^{-1}x\,\mathrm{id}_M = y = 0$. So $M = 0$. □

Corollary 4.23. *Let (R, m) be local and M be a finitely generated R-module. Let $N \subset M$ be a submodule. Then $M = mM + N$ implies that $N = M$.*

Proof. Since $M = mM + N$ by assumption, we have

$$m(M/N) = (mM + N)/N = M/N.$$

Since M is finitely generated, so is M/N. Now apply Nakayama's lemma to M/N we get $M/N = 0$ and $M = N$. □

Corollary 4.24. *Let (R, m) be a local ring with residue field $\kappa = R/m$. Let M be a finitely generated R-module. If $\{x_1, ..., x_n\} \subset M$ maps to a κ-basis for M/mM (i.e. maps to a basis of the finite dimensional vector space M/mM over the field κ) via the quotient map, then $\{x_1, ..., x_n\}$ generates M.*

Proof. Let $N = (x_1, ..., x_n) \subset M$. We want to show $N = M$. The composition

$$N \overset{\text{incl}}{\hookrightarrow} M \overset{\text{proj}}{\longrightarrow} M/mM$$

is surjective by hypothesis. In general, this composition has image $\{n + mM : n \in N\} = (N + mM)/mM$. To see this, clearly LHS is included on the RHS, which is the same as $\{n + mM : n \in N + mM\}$. Also, if $n \in N + mM$, then $n + mM \in n' + mM$ where $n' \in N$. So we have $M/mM = (N + mM)/mM$, thus $N + mM = M$. Apply Corollary 4.23 gives $N = M$. □

Lemma 4.25. *Let R be a commutative ring with 1. Let $I \subset R$ be an ideal, i.e. R-submodule of R, and M an R-submodule. Then we have the isomorphism*

$$\begin{aligned} M \otimes (R/I) &\overset{\simeq}{\to} M/IM \\ m \otimes (r + I) &\mapsto rm + IM. \end{aligned}$$

Proof. Consider the exact sequence

$$0 \to I \overset{\text{incl}}{\hookrightarrow} R \overset{\text{proj}}{\longrightarrow} R/I \to 0.$$

Then by Proposition 4.10, the first row of the diagram below is also exact:

$$\begin{array}{ccccccc} I \otimes_R M & \xrightarrow{\varphi} & R \otimes_R M & \xrightarrow{\psi} & (R/I) \otimes_R M & \longrightarrow & 0 \\ & \searrow^{j} & \downarrow \simeq & & & & \\ & & M & & & & \end{array}$$

Therefore, we have that

$$(R/I) \otimes_R M \cong R \otimes_R M / \ker \psi = R \otimes_R M / \operatorname{im} \varphi \cong M / j(I \otimes_R M).$$

This proves the claim. □

Finally we arrive at the big result of this section:

Theorem 4.26. *Let (R, m) be a local ring with residule field $\kappa = R/m$ and let M be a finitely generated module. Then M is R-flat if and only if M is R-free.*

Proof. Suppose M is R-free, then we have seen that M is flat from the last example of section 4.4. It remains to prove the other direction.

To this end, let $\{x_1, ..., x_n\} \subset M$ maps to a basis of M/mM over the field $\kappa = R/m$ under the projection $M \to M/mM$. By Corollary 4.24, $\{x_1, ..., x_n\}$ generates M. So now it is enough to check that $x_1, ..., x_m$ are R-linearly independent. Then they form a basis, which proves the claim.

Suppose $a_1, ..., a_n \in R$ are such that

$$\sum_{i=1}^{n} a_i x_i = 0. \tag{4.1}$$

We want to show that $a_i = 0$ for all i. Consider the exact sequence

$$0 \to \ker(f) \to R^n \xrightarrow{f} R$$

where

$$f : (b_1, ..., b_n) \mapsto \sum_{i=1}^{n} a_i b_i.$$

Since M is R-flat, the sequence above tensored with M is also exact. Now we have the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \ker(f) \otimes_R M & \longrightarrow & R^n \otimes_R M \xrightarrow{f \otimes \mathrm{id}} R \otimes_R M \\ & & & & \downarrow{\scriptstyle \varphi} \qquad\qquad \downarrow{\scriptstyle \psi} \\ & & & & M^n \xrightarrow[(y_1,...,y_n) \mapsto \sum_{i=1}^n a_i y_i]{} M \end{array}$$

and by exactness of the first row we have an isomorphism:

$$\begin{aligned} \phi : \ker(f) \otimes_R M &\xrightarrow{\simeq} \ker(f \otimes \mathrm{id}_M) \\ (b_i)_i \otimes M &\mapsto (b_i m)_i \subset M^n \end{aligned}$$

where we identify ϕ with $\varphi \circ \phi$. By (4.1), we have that $(x_1, ..., x_n) \in \ker(\psi \circ (f \otimes \mathrm{id}) \circ \varphi^{-1})$. But since ψ, φ^{-1} are isomorphisms, so they do not affet the kernel. Therefore we may assume WLOG that $(x_1, ..., x_n) \in \ker(f \otimes \mathrm{id})$. Then we can write

$$\phi^{-1}(x_1, ..., x_n) = \sum_j \beta_j \otimes m_j$$

where $\beta_j = (\beta_j^1, ..., \beta_j^n) \in \ker(f) \subset R^n$ and $m_j \in M$. So we have that

$$x_i = \sum_j \beta_j^i m_j \text{ for all } i = 1, ..., n \qquad \sum_{i=1}^{n} a_i \beta_j^i = 0 \text{ for all } j. \tag{4.2}$$

For the case $n = 1$ (4.1) reads: $a_1 x_1 = 0$ and (4.2) read:

$$x_1 = \sum_j \beta_j^1 m_j \qquad a_1 \beta_j^1 = 0 \text{ for all j.}$$

Since $x_1 \notin mM$ by hypothesis (basis element is nonzero), we must have $\beta_j^1 \notin m$ for some j. WLOG $\beta_1^1 \notin m$, which means it is invertible since R is local, so we get $a_1 = 0$. This proves the base case.

For the case $n \geq 2$, assumpe the statement is true for the case $n-1$. If $\beta_j^1 \in m$ for all j, then the first equation of (4.2) shows that $x_1 \in mM$, so x_1 maps to 0 in M/mM, which is impossible, since the reduction of x_1 is part of a basis for M/mM.

So WLOG, assume $\beta_1^1 \notin m$. So β_1^1 is invertible in R since R is local. Then

$$\beta_1 = (\beta_1^1, ..., \beta_1^n) \in \ker(f)$$

since $\beta_j \in \ker(f)$ by definition. hus from the definition of f we have that

$$\sum_{i=1}^{n} a_i \beta_1^i = 0.$$

Multiply on both sides by the inverse of β_1^1 gives that

$$a_1 + a_2\gamma_2 + \cdots + a_n\gamma_n = 0 \quad \text{where } \gamma_i = (\beta_1^1)^{-1}\beta_1^i \quad i \geq 2.$$

then equation above implies

$$a_2x_2 + \cdots + a_nx_n = -a_1x_1 = x_1(a_2\gamma_2 + \cdots + a_n\gamma + n).$$

This implies that

$$a_2(x_2 - x_1\gamma_2) + \cdots + a_n(x_n - x_1\gamma_n) = 0.$$

Now define $x_i' := x_i - x_1\gamma_i$. The elements $x_2', ..., x_n'$ are κ-linearly independent in M/mM since so do $x_1, ..., x_n$. Then we have that $a_2 = \cdots = a_n = 0$. Thus $a_1 = -a_2\gamma_2 - \cdots - a_n\gamma_n = 0$ as well. This proves the claim. □

Bibliography

[1] Michael F. Atiyah and Ian G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley (1969).

[2] Serge Lang, *Algebra*, (Revised Third Edition), Springer (2002).

[3] David S. Dummit, Richard M. Foote, *Abstract Algebra*, (Third Edition), Wiley (2004).

[4] Andreas Gathmann, *Commutative Algebra*, Class Notes TU Kaiserslautern (2014).