Advanced Algebra HT 2023

Benjamin Andersson
Victor Groth

Last updated 2026-01-10

Contents

Chapter 1

First lecture

1.1 Modules

1.1.1 Modules over a ring

Modules generalizations of vector spaces.

Suppose $\mathbb{F}$ is a field. A vector space over $\mathbb{F}$ is an abelian group V on which $\mathbb{F}$ "acts" in the sense that every $x \in \mathbb{F}$ defines a homomorphism $x\cdot\colon V \to V$. Namely $v \mapsto x \cdot v$. Modules are abelian groups with an "action" of a ring that is not necessarily a field.

Definition 1.1.1. Let R be a ring with unity, and let M be an abelian group. A left R-module structure on M consists of a function $\mu : R \times M \to M$ defined explicitly by the mapping

$$(r, m) \mapsto \mu(r, m) = r \cdot m.$$

This has to satisfy:

1. $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2, \quad \forall r \in R, \forall m_1, m_2 \in M.$
2. $(r_1 + r_2) \cdot m_1 = r_1 \cdot m + r_2 \cdot m, \quad \forall r_1, r_2 \in R, \forall m \in M.$
3. $1 \cdot m = m, \quad 1 \in R, \forall m \in M.$
4. $(rs) \cdot m = r \cdot (s \cdot m) \quad \forall r, s \in R, \forall m, \in M.$

A right module structure is a map

$$M \times R \to M$$

satisfying the same properties except

4') $m \cdot (r \cdot s) = (m \cdot r) \cdot s$

- If R is commutative then left and right-module structures are equal.
- Unless stated otherwise, by "module" we will mean "left-module".

Suppose M is an abelian group: Then $\mathrm{Hom}(M,M) = \mathrm{End}(M)$ is a ring, where we define addition as

$$(f+g)(m) := f(m) + g(m), \quad f,g \in \mathrm{End}(M), m \in M$$

and multiplication as

$$(f \circ g)(m) = f(g(m)).$$

A module structure

$$\mu : R \times M \to M$$

induces a unital ring-homomorphism

$$\tau_\mu : R \to \mathrm{End}(M)$$

defined explicitly by the mapping

$$r \mapsto \tau_\mu(r)(m) = r \cdot m.$$

Check: τ_μ is a well-defined homomorphism.

Conversely, given a unital ring homomorphism

$$\tau \colon R \to \mathrm{End}(M)$$

one can use it to define a module structure on M, by the formula

$$r \cdot m = \tau(r)(m).$$

It is not hard to check that the two constructions are inverse of each other.

Conclusion: A left module structure on $M \Leftrightarrow$ A *unital* ring-homomorphism

$$R \to \mathrm{End}(M)$$

so that

$$1_R \mapsto 1_{\mathrm{End}(M)}.$$

Similarly, a right module structure on $M \Leftrightarrow$ A *unital* ring *anti*-homomorphism

$$\tau \colon R \to \mathrm{End}(M)$$

so that

$$\tau(xy) = \tau(y)\tau(x).$$

Lemma 1.1.2. *For any R-module structure on M we have:*

$$0_R \cdot m = 0_M.$$

Proof.

$$\begin{aligned} 0_R \cdot m &= (0_R + 0_R) \cdot m \\ &= 0_R \cdot m + 0_R \cdot m \\ \Leftrightarrow 0_M &= 0_R \cdot m \quad (\forall m \in M). \end{aligned}$$

□

Lemma 1.1.3.

$$(-1_R) \cdot m = -m$$

Proof.

$$\begin{aligned} 0_R \cdot m &= (1_R + (-1)_R) \cdot m && (1.1)\\ &= m + (-1)_R \cdot m && (1.2)\\ &= 0_M && (1.3) \end{aligned}$$

1.1.2, i.e., that $0_R \cdot m = 0_M$. □

1.2 Examples

1.2.1 Vector spaces

If $\mathbb{F}$ is a field then a module over $\mathbb{F}$ is the same as a vector space over $\mathbb{F}$.

1.2.2 Abelian groups and $\mathbb{Z}$-modules

Every abelian group M has a *unique* $\mathbb{Z}$-module structure. This means that $\mathbb{Z}$-modules are the same thing as abelian groups. The structure is defined by the following formulas.

$$\begin{aligned} 1 \cdot m &= m\\ 2 \cdot m &= m + m\\ &\vdots\\ i \cdot m &= \underbrace{m + \ldots + m}_{i \text{ times}}\\ 0 \cdot m &= 0\\ (-1) \cdot m &= -m. \end{aligned}$$

The $\mathbb{Z}$-module structure is unique because there is a *unique* unital ring homomorphism $\mathbb{Z} \to \mathrm{End}(M)$ so that $1 \mapsto 1_{\mathrm{End}(M)}$ and $n \mapsto n \cdot 1_{\mathrm{End}(M)}$ is uniquely determined.

Comment 1.2.1.

$$1_{\mathrm{End}(M)} : M \to M$$

is the multiplicative identity (with multiplication defined as composition) in the *ring* of *endomorphisms*, defined explicitly by

$$1_{\mathrm{End}(M)}(x) = x, \quad (\forall x \in M).$$

1.2.3 $\mathbb{Z}/n\mathbb{Z}$-modules and n-torsion abelian groups

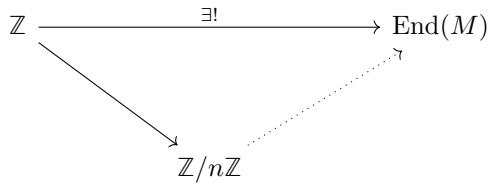
An abelian group M has a $\mathbb{Z}/n\mathbb{Z}$-module structure if and only if it is n-torsion. I.e., if for every element $x \in M$,

$$nx = 0_M.$$

If M has a $\mathbb{Z}/n\mathbb{Z}$-module structure, then it is unique.

One may say that being a module over $\mathbb{Z}/n\mathbb{Z}$ is a *property* of an abelian group rather than *structure*.

Remark 1.2.2. We can see that M can have at most *one* $\mathbb{Z}/n\mathbb{Z}$-module structure by viewing module structure as a ring homomorphism. Being a $\mathbb{Z}/n\mathbb{Z}$-module is a property of an abelian group.



1.2.4 Modules over polynomial ring in one variable

A module over the polynomial ring $\mathbb{Z}[x]$ is the same thing as an abelian group M with a fixed endomorphism $f : M \to M$. To see this, consider unital ring homomorphisms

$$\mathbb{Z}[x] \to \mathrm{End}(M)$$

Such a homomorphism is uniquely determined by its value on x, and x can be sent to any endormorphism f. If x is mapped to f then

$$x^2 \mapsto f^2$$

$$a_2x^2 + a_1x^1 + a_0 \mapsto a_2 \cdot f^2 + a_1 \cdot f + a_0 \cdot 1$$

etc.

There is a bijection

$$\mathrm{Ring}(\mathbb{Z}[x], R) \cong R$$

where $\mathrm{Ring}(S, T)$ denotes the set of unital ring homomorphisms from S to T.

1.2.5 Ideals and quotients

A module R is canonically a module *over itself*, with action $R \times R \to R$ defined explicitly by $(x, y) \mapsto x \cdot y$. More generally, if $I \lhd R$ is a (left) ideal of R, then I is a (left) module over R. Also, the quotient R/I has an R-module structure by the formula

$$r \cdot (x + I) = (r \cdot x) + I.$$

To see that this is well-defined, suppose $z \in I$. Then

$$r \cdot (x + z) = r \cdot x + r \cdot z \in r \cdot x + I.$$

1.3 Direct sums and direct products

Suppose $M_1, \ldots, M_n$ are abelian groups. Then

$$M_1 \oplus \cdots \oplus M_n = M_1 \times \cdots \times M_n. \quad \text{(cartesian product)}$$

If $M_1, \ldots, M_n$ are R-modules, then

$$M_1 \oplus \cdots \oplus M_n$$

is an R-module.

– If I is an infinite set, and for each $\alpha \in I$ we have that M_α is an R-module. Then

$$\prod_{\alpha \in I} M_\alpha := \{(\ldots, x_\alpha, \ldots) \mid x_\alpha \in M_\alpha, \alpha \in I\}.$$
$$\bigoplus_{\alpha \in I} M_\alpha := \{(\ldots, x_\alpha, \ldots) \mid \text{only finitely many of } x_\alpha \text{ are non-zero}\}.$$

– An arbitrary direct sum or product of R-modules is again an R-module.

– Every vector space is isomorphic to a direct sum of copies of $\mathbb{F}$ with itself, but this is not true over other rings, such as $\mathbb{Z}$. R-modules that *are* isomorphic to a direct sum of copies of R are called *free* modules.

1.4 Bases and linear independence, free modules

1.4.1 Bases and linear independence

Definition 1.4.1. Suppose M is an R-module and $A \subset M$. We say that A **generates** M *if* for all $x \in M$, there exists $a_1, \ldots, a_n \in A$ and $r_1, \ldots r_n \in R$ such that

$$x = r_1 a_1 + \ldots + r_n a_n.$$

Definition 1.4.2. Suppose M is an R-module and $A \subset M$. We say that A is **linearly independent** if for each finite subset $\{a_1, \ldots, a_n\} \subset A$ and $r_1, \ldots, r_n \in R$ it is the case that if

$$r_1 a_1 + \ldots + r_n a_n = 0_M \tag{1.4}$$

then

$$r_1 = \ldots = r_n = 0_R. \tag{1.5}$$

Definition 1.4.3. Suppose M is an R-module and $A \subset M$. A is a **basis** of M if it *generates* (1.4.1) M and is *linearly independent* (1.4.2).

1.4.2 Free modules

Definition 1.4.4. A module M is **free** if it has a *basis* (1.4.3).

Example 1.4.5. For any set I, we have that

$$\bigoplus_{x \in I} R$$

is a free module.

Proof. For every $\alpha \in I$ (where I is just an indexing set) let

$$e_\alpha := (0, \ldots, \underbrace{1}_{\text{position } \alpha}, \ldots, 0). \tag{1.6}$$

Then, the set $\{e_\alpha\}_{\alpha \in I}$ is a basis. □

Lemma 1.4.6 (converse)**.** *Suppose $A = \{m_\alpha \mid \alpha \in I\} \subset M$ is a basis (so M is free). Then there is an isomorphism*

$$\bigoplus_{m_\alpha \in A} R \to M$$

defined explicitly by

$$(\ldots, r_\alpha, \ldots) \mapsto \sum r_\alpha m_\alpha.$$

Definition 1.4.7. We say that M is **free of rank** n if M has a basis with n elements, or equivalently if

$$M \cong \bigoplus_{i=1}^{n} R. \tag{1.7}$$

Remark 1.4.8. Rank is well-defined for free modules over commutative rings [1, Exc 10.3.2], and also for "many" *non*-commutative rings. But *not* all rings [1, Exc 10.3.27].

1.5 Homomorphisms

Definition 1.5.1. Suppose M, N are R-modules. A module homomorphism $f : M \to N$ is an *abelian group homomorphism* that satisfies

$$f(r \cdot m) = r \cdot f(m) \quad (\forall r \in R, m \in M).$$

If $f, g : M \to N$ are module homomorphism then $f + g$ is also a module homomorphism.

$$\mathrm{Hom}_R(M, N) = \text{Group of } R\text{-module homomorphisms } f : M \to N$$

where we have that

$$\mathrm{Hom}_R(M, N) \leqslant \mathrm{Hom}(M, N)^{1}.$$

Example 1.5.2. Suppose M, N are $\mathbb{Z}/n\mathbb{Z}$-modules, i.e., they are n-*torsion* abelian groups. Then

$$\mathrm{Hom}_{\mathbb{Z}/n\mathbb{Z}}(M, N) = \mathrm{Hom}_{\mathbb{Z}}(M, N).$$

Example 1.5.3. Suppose M is a $\mathbb{Z}[x]$-module via some *endomorphism* $x \cdot m = f(m)$ where $f : M \to M$. Then $\mathrm{Hom}_{\mathbb{Z}[x]}(M, M) \subset \mathrm{Hom}(M, M)$ consists of abelian group homomorphisms $\alpha : M \to M$ such that $f \circ \alpha = \alpha \circ f$ or, that is, the following diagram commutes

$$\begin{array}{ccc} M & \xrightarrow{\alpha} & M \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ M & \xrightarrow{\alpha} & M \end{array}$$

Lemma 1.5.4 (Properties of $\mathrm{Hom}_R(-,-)$)**.**

[1] $\leqslant$ being the subgroup symbol

(a) *For any R-module M we have that* $\mathrm{Hom}_R(R, M) \cong M$ *where we define the isomorphism explicitly by*

$$f \mapsto f(1).$$

(b) *Suppose $\{M_\alpha | \alpha \in I\}$ are R-modules, and N is an R-module. We get*

$$\mathrm{Hom}_R(\bigoplus_{\alpha \in I} M_\alpha, N) \cong \prod_{\alpha \in I} \mathrm{Hom}_R(M_\alpha, N).$$

(c)

$$\mathrm{Hom}_R(R^{\oplus n}, M) \cong M^n.$$

Chapter 2

Second lecture

2.1 Isomorphism theorems

2.1.1 Submodules

Definition 2.1.1. Suppose R is a ring, and M is an R-module, where $N \subset M$. We say that N is a **submodule** of M if:

1. N is an abelian subgroup of M.
2. $\forall n \in N, \forall r \in R$ we have that $r \cdot n \in N$.

Remark 2.1.2. $(1) + (2) \Leftrightarrow \forall r_1, r_2 \in R, x, y \in N$ we have that $r_1 x + r_2 y \in N$.

Example 2.1.3.

1. A subset $I \subset R$ is a submodule $\Leftrightarrow$ I is an ideal.
2. $\mathbb{Z} \subset \mathbb{Q}$ is a subgroup, so it is a $\mathbb{Z}$-submodule. But it is *not* a $\mathbb{Q}$-submodule.

Definition 2.1.4. Let $f : M \to N$ is an R-module homomorphism. We define

$$\ker(f) := \{m \in M \mid f(m) = 0\} \tag{2.1}$$

as the **kernel** of f.

Lemma 2.1.5. *For* any *R-module homomorphism $f : M \to N$, we have that* $\ker(f)$ *is a submodule of M, and* $\mathrm{im}(f)$ *is a submodule of N.*

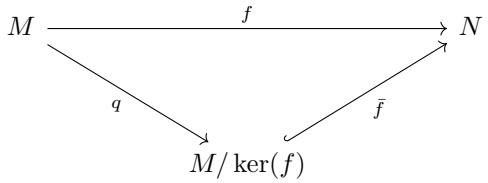
2.1.2 Quotient modules

Suppose M is an R-module and $N \subset M$ is a submodule, then the quotient M/N has an R-module structure, given by the formula

$$r \cdot (m + N) = r \cdot m + N.$$

2.1.3 Isomorphism theorems

Theorem 2.1.6 (First Isomorphism Theorem)**.** *An R-module homomorphism $f : M \to N$ factors* uniquely *as*



where $q : M \to M/\ker(f)$ is the quotient homomorphism defined explicitly by the mapping

$$m \mapsto m + \ker(f).$$

Furthermore, we have the mapping $\bar{f}$ defined by $\bar{f}(m + \ker(f)) = f(m)$. Let's note that q is (almost by definition) surjective, and that $\bar{f}$ is injective.

There is also an isomorphism of R-modules

$$\bar{f} : M/\ker(f) \xrightarrow{\cong} \mathrm{Im}(f)$$

(cf. isomorphism theory for groups and rings).

Remark 2.1.7. Suppose $N \subset M$ is a submodule. Often the best way to understand the quotient module M/N is to realize N as the kernel of some homomorphism

$$f : M \to Z$$

so that

$$M/N \cong \mathrm{im}(f).$$

Example 2.1.8. Let $\mathbb{Z}[x]$ act on $\mathbb{Z} \oplus \mathbb{Z}$ by

$$x \cdot (a, b) = (b, a)$$

For example:

$$(a_0 + a_1 x + a_2 x^2) \cdot (m, n) = (a_0 + a_2)(m, n) + a_1(n, m).$$

Examples of submodules: the diagonal

$$\Delta^+ := \{(m, m) \mid m \in \mathbb{Z}\} \subset \mathbb{Z} \oplus \mathbb{Z}$$

and the anti-diagonal

$$\Delta^- := \{(m, -m) \mid m \in \mathbb{Z}\} \subset \mathbb{Z} \oplus \mathbb{Z}.$$

Question 2.1.9. What is

$$\mathbb{Z} \oplus \mathbb{Z}/\Delta^+?$$

Claim 2.1.10. We have a $\mathbb{Z}[x]$-module isomorphism $\mathbb{Z} \oplus \mathbb{Z}/\Delta^+ \cong \Delta^-$.

Proof. Consider the homomorphism

$$\pi : \mathbb{Z} \oplus \mathbb{Z} \to \Delta^-$$

explicitly defined by

$$\pi(m, n) = (m - n, n - m).$$

Multiply by

$$x(m, n) = (n, m)$$

and

$$x(m - n, n - m) = (n - m, m - n)$$

so that

$$\begin{aligned} \pi(x \cdot (m, n)) &= \pi(n, m) \\ &= (n - m, m - n) \end{aligned}$$

and

$$\begin{aligned} x \cdot \pi(m, n) &= x(m - n, n - m) \\ &= (n - m, m - n). \end{aligned}$$

Furthermore, we have that

$$(1, 0) \overset{\pi}{\longmapsto} (1, -1)$$

so that for all $(m, -m) \in \Delta^-$ we find that $(m, 0)$ gets sent to $(m, -m)$, hence we have a surjection.

$$\begin{aligned} \ker(\pi) &= \{(m, n) \mid m - n = n - m = 0\} \\ &= \Delta^+. \end{aligned}$$

Hence we see that under π,

$$\begin{aligned} \mathbb{Z} \oplus \mathbb{Z}/\Delta^+ &\cong \operatorname{im}(\pi) \\ &= \Delta^- \quad \text{(since we have a surjection).} \end{aligned}$$

□

2.2 Submodules generated by a subset

Definition 2.2.1. Suppose M is an R-module, and $A \subset M$. Then the submodule **generated** by A is

$$\langle A \rangle := \{r_1 a_1 + \ldots + r_n a_n \mid n \in \mathbb{N},\ r_1, \ldots, r_n \in R,\ a_1, \ldots, a_n \in A\}$$

Remark 2.2.2. $\langle A \rangle$ is the *smallest* submodule of M *containing* A. This means that $\langle A \rangle$ is the intersection of all submodules of M containing A. The submodule $\langle A \rangle$ is characterized by the property that every submodule of M that contains A contains $\langle A \rangle$.

Definition 2.2.3. An R-module M is **finitely generated** if there *exists* a finite subset $A := \{a_1, \ldots, a_n\} \subset M$ such that $\langle A \rangle = M$.

Example 2.2.4.

1. $$\mathbb{Z} \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/2 = \{(x, y, z) \mid x \in \mathbb{Z}, y \in \mathbb{Z}/4, z \in \mathbb{Z}/2\}$$

   is a *finitely* generated $\mathbb{Z}$-module.

Indeed, the set

$$\{(1,0,0),(0,1,0),(0,0,1)\}$$

generates

$$\mathbb{Z}\oplus\mathbb{Z}/4\oplus\mathbb{Z}/2$$

but we see that the set is not linearly independent (over $\mathbb{Z}$), since we have for example, that

$$4(0,1,0)=0.$$

2. $\mathbb{Q}$ is *not* finitely generated as a $\mathbb{Z}$-module.

3. $\bigoplus_{i=1}^{\infty}\mathbb{Z}$ and $\prod_{i=1}^{\infty}\mathbb{Z}$ are *not* finitely generated $\mathbb{Z}$-modules.

2.3 Functoriality of Hom: pushforward and pullback

Recall that

$$\mathrm{Hom}_R(M,N)=\{\text{the abelian group of } R\text{-module homomorphisms } f:M\to N\}$$

2.3.1 Pushforward

Suppose we have an R-module homomorphism $\alpha:N\to N_1$. Then α *induces* a homomorphism

$$\alpha_*:\mathrm{Hom}_R(M,N)\to\mathrm{Hom}_R(M,N_1)$$

which is explicitly defined by

$$\alpha_*(f)=\alpha\circ f\quad(f\in\mathrm{Hom}_R(M,N)).$$

Furthermore, if

$$\beta:N_1\to N_2$$

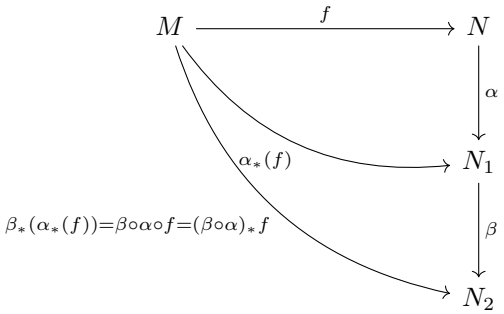
is another homomorphism, then there is an equality of homomorphisms $\mathrm{Hom}_R(M,N)\to\mathrm{Hom}_R(M,N_2)$:

$$\beta_*\alpha_*=(\beta\circ\alpha)_*.$$

More explicitly, this means that

$$\beta_*(\alpha_*(f))=(\beta\circ\alpha)_*(f).$$

The diagram below illustrates the points we just made



Furthermore, note that:

$$(1_N)_*=1_{\mathrm{Hom}_R(M,N)}\quad\text{(The identity homomorphism)}.$$

2.3.2 Pullback

Similarly, suppose we have a homomorphism $\alpha : M \to M_1$. It induces a homomorphism

$$\alpha^* : \mathrm{Hom}_R(M_1, N) \to \mathrm{Hom}_R(M, N)$$

explicitly, we get

$$\alpha^*(f) = f \circ \alpha : M \to N \quad (f \in \mathrm{Hom}_R(M_1, N))$$

so that α^* acts as a **pullback**.

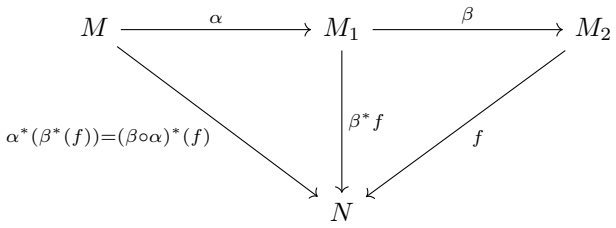
Furthermore, if $\beta : M_1 \to M_2$ is another homomorphism, then

$$\alpha^* \circ \beta^*(f) = \alpha^*(f \circ \beta) = (f \circ \beta) \circ \alpha \underset{\circ \text{ being associative}}{=} f \circ (\beta \circ \alpha) = (\beta \circ \alpha)^*(f) \quad (f \in \mathrm{Hom}_R(M_2, N))$$

so that

$$(\beta \circ \alpha)^* : \mathrm{Hom}_R(M_2, N) \to \mathrm{Hom}_R(M, N).$$

We can put this in a diagrammatic form as



2.4 Module structure on Hom

Does $\mathrm{Hom}_R(M, N)$ have an R-module structure? We know that $\mathrm{Hom}_R(M, N)$ is an abelian group under pointwise addition. Let's try to define an R-module structure on this group as follows. Suppose $r \in R$ and $f \in \mathrm{Hom}_R(M, N)$. Define the function $r \cdot f \colon M \to N$ by the formula

$$(r \cdot f)(m) = rf(m).$$

Question: Is $r \cdot f$ an R-module homomorphism?

To avoid confusion, let us introduce notation $g = r \cdot f$. The question is whether g is an R-module homomorphism.

$$g(r' \cdot m) \stackrel{?}{=} r' \cdot g(m)$$

$$g(r' \cdot m) = r \cdot f(r' \cdot m) = r \cdot r' \cdot f(m)$$

$$r' \cdot g(m) = r' \cdot r \cdot f(m).$$

Conclusion: It R is commutative, then multiplication by r endows $\mathrm{Hom}_R(M, N)$ with an obvious R-module structure. But if R is *not commutative* then this does not work, because $r \cdot f$ will not necessarily be a module homomorphism.

2.4.1 Bimodules

In general, $\mathrm{Hom}_R(M,N)$ has a module structure if M or N or both are *bimodules*.

Definition 2.4.1. Let R, S be *unital* rings. An R-S **bimodule** structure on M consists of

1. a *left* R-module structure, and
2. a *right* S-module structure.

such that $\forall r \in R, \forall s \in S$ and $\forall m \in M$, we have

$$r \cdot (m \cdot s) = (r \cdot m) \cdot s \quad \text{(associative)}.$$

In the case $R = S$, an R-R-bimodule structure is usually called an R-bimodule structure.

Example 2.4.2.

1. R is a bimodule over itself.
2. $\bigoplus_{i \in I} R$ is an R-bimodule, where I is an index-set.

If M is a left R-module and N is an R-S-bimodule, then $\mathrm{Hom}_R(M,N)$ is a *right* S-module by the formula

$$(f \cdot s)(m) = f(m) \cdot s.$$

As usual, Hom_R denotes homomorphisms of left modules.

Note that $(f \cdot s) \cdot s_1 = f \cdot (ss_1)$ which is the associativity condition of a right module structure.

If M is an R-S-bimodule and N is a left R-module then $\mathrm{Hom}_R(M,N)$ is a *left* S-module by the formula

$$(s \cdot f)(m) = f(m \cdot s).$$

Exercise: check that $g = s \cdot f$, i.e., $g(m) = f(m \cdot s)$, is a homomorphism of left R-modules.

We calculate:

$$(s_1 \cdot (s \cdot f))(m) = (s_1 \cdot g)(m) = g(m \cdot s_1) = f(m \cdot s_1 \cdot s) = ((s_1 s) \cdot f)(m). \tag{2.2}$$

That is, $s_1 \cdot (s \cdot f) = (s_1 s) \cdot f$ which is the associativity condition of a left module structure.

Basically if multiplying by s and then by s_1 is the same as multiplying by $s \cdot s_1$, then it is a right module structure. If multiplying by s and then by s_1 is the same as multiplying by $s_1 \cdot s$ then it is a left module structure.

The point is that a right module structure on M endows $\mathrm{Hom}_R(M,N)$ with a left module structure (and vice versa), because the dependence of $\mathrm{Hom}_R(M,N)$ on M is contravariant (i.e, it reverses the direction of arrows).

- In order to formalise the idea that $\mathrm{Hom}_R(M,N)$ "depends covariantly on N and contravariantly on M" we need to introduce the language of...

2.5 Categories and functors

Definition 2.5.1. • A **Category** $\mathcal{C} = (\mathrm{ob}(\mathcal{C}), \mathrm{Mor}(\mathcal{C}))$ consists of

1. A "set" $\mathrm{ob}(\mathcal{C})$ whose elements are **objects** of $\mathcal{C}$.

2. For every $x, y \in \mathrm{ob}(\mathcal{C})$, a set $\mathrm{Hom}_{\mathcal{C}}(x, y)$ where elements in $\mathrm{Hom}_{\mathcal{C}}(x, y)$ are called **morphisms** in $\mathcal{C}$ *from* x *to* y.

3. For every $x \in \mathrm{ob}(\mathcal{C})$, there is a special element $1_x \in \mathrm{Hom}_{\mathcal{C}}(x, x)$ called the *identity* on x.

4. For every $x, y, z \in \mathrm{ob}(\mathcal{C})$ a *function* called *composition*

$$\mathrm{Hom}_{\mathcal{C}}(y, z) \times \mathrm{Hom}_{\mathcal{C}}(x, y) \to \mathrm{Hom}_{\mathcal{C}}(x, z)$$

denoted by

$$(g, f) \to g \circ f = gf.$$

The composition satisfies:

(a) *Associativity*:

$$h(gf) = (hg)f \quad (\textit{when} \text{ both sides make sense}).$$

(b) *Unitality*: If $f \in \mathrm{Hom}_{\mathcal{C}}(x, y)$ then $1_y \circ f = f \circ 1_x = f$.

Chapter 3

Third lecture: Tensors; universal properties, construction, ...

3.1 Bilinearity and universal property of tensor product

3.1.1 Recall

- If R is commutative and M, N are R-modules, then $\mathrm{Hom}_R(M, N)$ is an R-module.
- if R *non*-commutative and M, N are R-modules, then $\mathrm{Hom}_R(M, N)$ abelian group.
- If R is non-commutative and M, N bimodules then $\mathrm{Hom}_R(M, N)$ is a bimodule.

3.2 Bilinearity and R-linearity

Let R be a (unital) **commutative** ring.

Definition 3.2.1. Let $M, N, \mathcal{L}$ be R-modules. A map

$$M \times N \xrightarrow{\varphi} \mathcal{L}$$

is R-**bilinear** if it satisfies the following conditions:

(a) $\varphi(r_1 m_1 + r_2 m_2, n) = r_1\varphi(m_1, n) + r_2\varphi(m_2, n) \quad (\forall r_1, r_2 \in R, \forall m_1, m_2 \in M, \forall n \in N)$

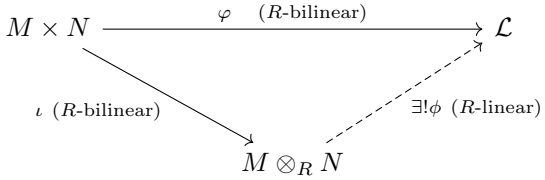
(b) $\varphi(m, r_1 n_1 + r_2 n_2) = r_1\varphi(m, n_1) + r_2\varphi(m, n_2) \quad (\forall m \in M, \forall r_1, r_2 \in R, \forall n_1, n_2 \in N)$

A map $\phi\colon M \to \mathcal{L}$ is called R-**linear** if it is an R-module homomorphism.

Note: It is not hard to check that if $\varphi\colon M \times N \to \mathcal{L}$ is R-bilinear, and $\phi\colon \mathcal{L} \to \mathcal{P}$ is R-linear, then the composition $\phi \circ \varphi$ is R-bilinear.

3.3 Definition of the tensor product $M \otimes_R N$ via universal property [1, Cor. 10.12]

Definition 3.3.1. Suppose M, N and R are as above. A tensor product of M and N over R is an R-module $M \otimes_R N$, endowed with an R-bilinear map $\iota\colon M \times N \to M \otimes_R N$ such that for every R-bilinear map $\varphi\colon M \times N \to \mathcal{L}$ where $\mathcal{L}$ is another R-module, there exists a unique R-linear map $\phi\colon M \otimes_R N \to \mathcal{L}$, making the following diagram commute:



$$\underset{\phi \circ \iota}{\{R\text{-bilinear maps } \varphi\}} \quad \Leftrightarrow \quad \underset{\phi}{\{R\text{-linear } \phi : \varphi = \phi \circ \iota\}}$$

Note: $\otimes$ relates *bilinear* maps with *linear* maps.

Remark 3.3.2. When $R = \mathbb{Z}$ it is customary to denote $M \otimes_{\mathbb{Z}} N$ simply by $M \otimes N$. More generally, R is sometimes omitted from the notation when it is clear from the context.

3.4 Universal property uniquely determines $(M \otimes_R N, \iota)$ up to canonical isomorphism

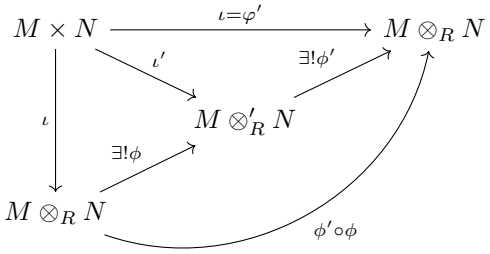
Theorem 3.4.1. *Suppose $(M \otimes'_R N, \iota')$ is some other R-module $M \otimes'_R N$ and bilinear map*

$$i' : M \times N \to M \otimes'_R N$$

satisfying the same property as $M \otimes_R N$ in 3.1.3. *Then*

$$M \otimes_R N \cong M \otimes'_R N.$$

Proof.



We have

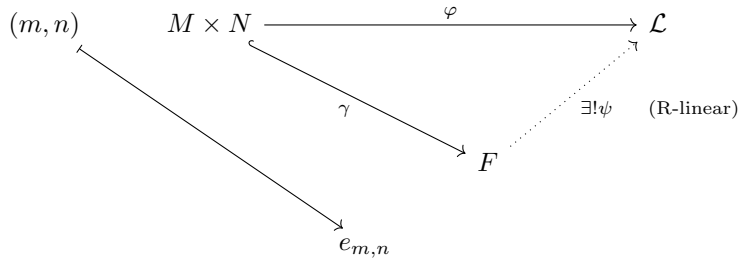
- A *unique* map
$$\phi' : M \otimes'_R N \to M \otimes_R N$$
from the *universal property* of $(M \otimes'_R N, \iota')$, for
$$\varphi' = \iota.$$

- We get a *unique* map
$$\phi : M \otimes_R N \to M \otimes'_R N$$
from the *universal property* of $(M \otimes_R N, \iota)$, for
$$\varphi = \iota'.$$

- By *uniqueness* in the universal properties, we also obtain
$$\phi' \circ \phi = \mathrm{id},$$
and
$$\phi \circ \phi' = \mathrm{id} \qquad \square$$

3.5 *Construction* of $M \otimes_R N$

1. Take the *free* R-module on the set $M \times N$
$$F = \bigoplus_{(m,n) \in M \times N} R \tag{3.1}$$
with basis $\{e_{m,n}\}$. By the **Universal property of free modules**, any function $\phi\colon M \times N \to \mathcal{L}$ extends uniquely to an R-linear function $F \to \mathcal{L}$, as in the following diagram



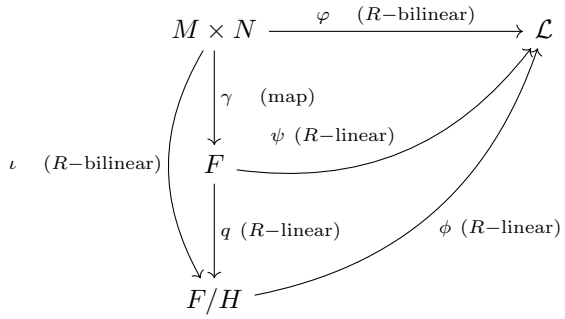
For $\varphi = \psi \circ \gamma$ we need
$$\psi(e_{m,n}) = \varphi((m,n)).$$
Note: γ is *not* bilinear, e.g.
$$\begin{aligned} \gamma((rm,n)) &= e_{rm,n} \\ &\neq r e_{m,n}. \end{aligned}$$

2. Impose relations *forcing bilinearity.*
   (a) $e_{r_1 m_1 + r_2 m_2, n} - r_1 e_{m_1,n} - r_2 e_{m_2,n} = 0 \quad (\forall r_1, r_2 \in R, \forall m_1, m_2 \in M, n \in N)$.
   (b) Same in 2^{nd} argument.

   Let $H \subset F$ be the *R-submodule* of F generated by LHS of (a) and (b).

3. Define $M \otimes_R N := F/H$.

4. Let's verify that the construction of $M \otimes_R N$ satisfies the *universal property*.



To show that the homomorphism $\psi\colon F \to \mathcal{L}$ factors uniquely through an R-linear homomorphism $\phi\colon F/H \to \mathcal{L}$ one needs to check that for every generator x of H, $\psi(x) = 0$. Let us consider for example a generator of the form $e_{r_1m_1+r_2m_2,n} - r_1e_{m_1,n} - r_2e_{m_2,n}$. We have

$$\psi(e_{r_1m_1+r_2m_2,n} - r_1e_{m_1,n} - r_2e_{m_2,n}) = \varphi(r_1m_1 + r_2m_2, n) - r_1\varphi(m_1, n) - r_2\varphi(m_2, n)$$
$$\underbrace{=}_{\text{if } \varphi \text{ is bilinear}} 0.$$

We conclude that

$$\psi(H) = 0 \Leftrightarrow \varphi \text{ bilinear} \Leftrightarrow \exists! \phi : \psi = \phi \circ q.$$

5. It is not hard to check that the composition $q \circ \gamma\colon M \times N \to F/H$ is R-bilinear.

Remark 3.5.1. If R is a non-commutative ring then $M \otimes_R N$ can be defined when M is a right R module and N is a left R-module. R-bilinearity is then replaced with R-balanced and the tensor product $M \otimes_R N$ as well as the target $\mathcal{L}$ are merely abelian groups.

3.6 Tensors

The elements of $M \otimes_R N$ are called **tensors**. The *simple* or *pure* tensors are elements of the form

$$m \otimes n := \iota(m, n) = q(e_{m,n}).$$

Any tensor can be written as a finite sum/linear combination of simple tensors.

$$\sum_{i=1}^{n} m_i \otimes n_i \quad (m_i \in M, n_i \in N, \text{for } i \in \{1, \ldots, n\})$$

Note: by construction

$$- \otimes -$$

is *bilinear*.

$$(r_1m_1 + r_2m_2) \otimes n = r_1(m_1 \otimes n) + r_2(m_2 \otimes n).$$

3.6.1 Generators

If $m_1, \ldots, m_a$ are generators for M and $n_1, \ldots, n_b$ are generators for N then $\{m_i \otimes n_j\}_{i=1,\ldots,a}^{j=1,\ldots,b}$ are generators for $M \otimes_R N$(also works for *infinite* generator sets).

- We'll see that if $\{m_i\}$ is a basis for M and $\{n_j\}$ basis for $N \Rightarrow \{m_i \otimes n_j\}$ basis for $M \otimes_R N$.

Example 3.6.1. We have that $\mathbb{C}$ is an $\mathbb{R}$-vector space with basis $\{1, i\}$ and that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ has basis

$$\{1 \otimes 1\}, \{1 \otimes i\}, \{i \otimes 1\}, \{i \otimes i\};$$

$$a(1 \otimes 1) + b(1 \otimes i) + c(i \otimes 1) + d(i \otimes i) \quad (a, b, c, d \in \mathbb{R})$$

$$(x + iy) \otimes (z + iw) = xz(1 \otimes 1) + xw(1 \otimes i) + yz(i \otimes 1) + yw(i \otimes i).$$

Example 3.6.2.

$$\begin{aligned} x \otimes 0 &= 0(x \otimes 0) \\ &= 0 \end{aligned}$$

Example 3.6.3.

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$$

defined by

$$\begin{aligned} x \otimes y &= x \otimes \frac{yn}{n} \\ &= n\left(x \otimes \frac{y}{n}\right) \\ &= nx \otimes \frac{y}{n} \\ &= 0 \otimes \frac{y}{n} \\ &= 0 \\ \Rightarrow \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} &= 0. \end{aligned}$$

3.7 Canonical Isomorphisms

(1) Identity: $R \otimes_R M \cong M$ defined explicitly by

$$r \otimes m \mapsto r \cdot m.$$

(2) Commutativity: $M \otimes_R N \cong N \otimes_R M$ defined by

$$m \otimes n \mapsto n \otimes m.$$

(3) Associativity: $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$ defined explicitly by

$$(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p).$$

(4) Distributivity: $M \otimes (N \oplus P) \cong (M \otimes N) \oplus (M \otimes P)$ defined by

$$m \otimes (n + p) \mapsto (m \otimes n) + (m \otimes p)$$

(5) From (1)+(4) we obtain $M \otimes_R R^a \cong M^a$ so that

$$\begin{aligned} R^a \otimes_R R^b &\cong (R^a)^b \\ &= R^{ab}. \end{aligned}$$

More precisely, given bases of M and N one obtains a basis of $M \otimes_R N$ as described above.

Example 3.7.1.

$$\underbrace{R[x]}_{\text{basis } 1,x,x^2,\ldots} \otimes_R \underbrace{R[y]}_{\text{basis } 1,y,y^2,\ldots} \cong R[x,y] \Rightarrow \text{basis } \{x^i \otimes y^j\}_{i,j}.$$

Example 3.7.2. Let M be an R-module. We have

$$R/I \otimes_R M \cong M/IM$$

explicitly

$$\bar{r} \otimes_R m \mapsto \bar{r}\bar{m} \quad \text{(isomorphism of R-module and even R/I-module).}$$

3.8 Restriction and Extension of Scalars

$$R \xrightarrow{\varphi} S \quad \text{ring homomorphism (between commutative rings)}$$

Given an S-module N, we can consider it via φ as an R-module

$$r \cdot n = \varphi(r) \cdot n.$$

- This is called *restriction of scalars* and sometimes denoted N_R or N_φ or $N_{[\varphi]}$.
- Given an R-module M, consider $S \otimes_R M$. This is an S-module via

$$s \sum_i s_i \otimes m_i = \sum_i (ss_i) \otimes m_i$$

called *extension of scalars*.

Example 3.8.1.

1. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n$ (isomorphism of $\mathbb{C}$-vector space)
2. $\underbrace{\mathbb{C}}_{\{1,i\}} \otimes_{\mathbb{R}} \underbrace{\mathbb{R}[x]}_{1,x,x^2,\ldots} \cong \mathbb{C}[x]$

Example 3.8.2. Let M be a $\mathbb{Z}$-module $\rightsquigarrow \mathbb{Q} \otimes_{\mathbb{Z}} M$ is a $\mathbb{Q}$-vector space.

Example 3.8.3. Let M be an R-module *annihilated* by $I \triangleleft R$

$$\rightsquigarrow M \text{ is an } R/I - \text{module}$$

where

$$\begin{aligned} M \otimes_R R/I &\cong M/IM \\ &\cong M. \end{aligned}$$

3.9 Tensor product of algebras

Definition 3.9.1. Let R be a *commutative* ring. An R-algebra is a ring S together with a ring homomorphism $f : R \to S$ such that $f(R) \subset Z(S)$, that is, the R-algebra is (S, f).

Proposition 3.9.2. *Let S_1, S_2 be R-algebras. Then*

$$S_1 \otimes_R S_2$$

is an R-algebra with

1. *multiplication defined by*
$$(s_1 \otimes_R s_2)(s_1' \otimes_R s_2) = s_1 s_1' \otimes_R s_2 s_2'$$

2. *R-algebra structure*
$$\varphi : R \to S_1 \otimes_R S_2$$
explicitly defined by
$$\begin{aligned} r \mapsto r(1 \otimes_R 1) &= \varphi_1(r) \otimes_R 1 \\ &= 1 \otimes \varphi_2(r). \end{aligned}$$

Example 3.9.3.

1.
$$\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{C} \quad \text{(isomorphism of rings)}$$

2.
$$R[x] \otimes_R R[y] \cong R[x, y] \quad \text{(isomorphism of rings)}.$$

3.10 Functoriality of tensor product

Given
$$M_1 \xrightarrow{f} M_2, \quad N_1 \xrightarrow{g} N_2$$
we obtain
$$f \otimes g : M_1 \otimes N_1 \to M_2 \otimes N_2.$$
defined on simple tensors as $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$. This makes the tensor product covariantly functorial in both the first and second factor.

Chapter 4

Fourth lecture: Exact sequences, projective and flat modules

Today

1. Exact sequences
2. Exactness properties of functors
   - $\mathrm{Hom}_R(D, -)$ (covariant)
   - $\mathrm{Hom}_R(-, D)$ (*contra*variant)
   - $D \otimes_R -$ (covariant)
3. Properties of modules; projective, injective, flat.

4.1 Exact sequences

$$\cdots \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to \cdots$$

Exact at Y if $\mathrm{Im}(\alpha) = \ker(\beta)$.

Example 4.1.1.

$$0 \to X \xrightarrow{f} Y \quad \text{(exact at } X\text{)}$$
$$\Leftrightarrow$$
$$\ker(f) = 0 \Leftrightarrow f \text{ injective}$$

Example 4.1.2.

$$Y \xrightarrow{g} Z \to 0 \quad \text{(exact at } Z\text{)}$$
$$\Leftrightarrow$$
$$\mathrm{Im}(g) = Z \Leftrightarrow g \text{ surjective}$$

4.2 Short Exact Sequences (SES)

$$0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0 \quad (*) \tag{4.1}$$

(*) exact *equivalent* to the following conditions:

- f injective
- g surjective
- $\mathrm{Im}(f) = \ker(g)$

$$\Leftrightarrow$$

- f injective
- $$\begin{aligned} Y/\operatorname{im}(f) &= Y/\ker(g) \\ &= \operatorname{im}(g) \\ &= Z. \end{aligned}$$

Example 4.2.1.

$$0 \to X \xhookrightarrow{f} Y \xrightarrow{g} Y/X \to 0.$$

Example 4.2.2 (Left Exact Sequence = LES)**.**

$$0 \to X \xrightarrow{f} Y \xrightarrow{g} Z.$$

Example 4.2.3 (Right Exact Sequence = RES)**.**

$$X \xrightarrow{f} Y \xrightarrow{g} Z \to 0.$$

Example 4.2.4 (Presentations)**.** Let M be an R-module with generators $m_1, \ldots, m_n$.

$$R^{\oplus n} \xrightarrow{p} M \to 0 \quad \text{(exact)}$$

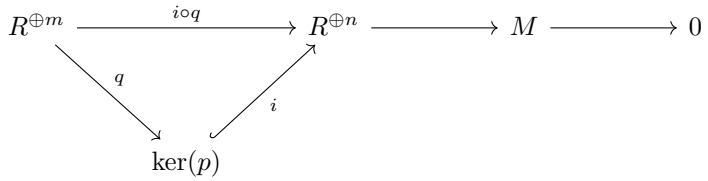
Gives SES with $\ker(p)$:

$$\begin{aligned} 0 \to \ker(p) \xrightarrow{i} R^{\oplus n} &\xrightarrow{p} M \to 0 \\ e_j &\mapsto m_j \end{aligned}$$

Find generators for $\ker(p) : r_1, \ldots, r_m$

$$R^{\oplus m} \xrightarrow{q} \ker(p) \to 0$$

gives RES



called a presentation of M.

Example 4.2.5. $R = k[x, y]$ and $M = (x, y)$.

$$\begin{aligned} R^{\oplus 2} &\xrightarrow{p} (x, y) \to 0 \\ e_1 &\mapsto x \\ e_2 &\mapsto y \end{aligned}$$

$$\begin{aligned} \ker(p) &= \langle ye_1 - xe_2 \rangle \\ &\cong R^{\oplus 1} \end{aligned}$$

gives SES

$$0 \to R \to R^{\oplus 2} \to (x, y) \to 0$$

where we note that

$$(x, y) = R\langle e_1, e_2 \rangle / \langle ye_1 - xe_2 \rangle$$

with 2 generators and 1 relation.

4.3 Extensions

$$0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0 \quad \text{SES}$$

We say that Y is an **extension** of Z by X.

Definition 4.3.1. An SES (4.1) is **split** if

$$\text{Im}(f) \subset Y \text{ has a complement } W \subset Y.$$

That is,

$$Y = \text{Im}(f) \oplus W \quad (\textit{inner} \text{ direct sum}).$$

Example 4.3.2. What are the possible extensions of $\mathbb{Z}/2$ by $\mathbb{Z}/2$?

$$0 \to \mathbb{Z}/2 \to Y \to \mathbb{Z}/2 \to 0$$

(1) $Y = \mathbb{Z}/4$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & \mathbb{Z}/4 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & 0 \\ & & 1 & \longmapsto & 2 & & & & \end{array}$$

(2) $Y = \mathbb{Z}/2 \oplus \mathbb{Z}/2$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & \mathbb{Z}/2 \oplus \mathbb{Z}/2 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & 0 \\ & & a & \longmapsto & (a, 0) & & & & \\ & & & & (a, b) & \longmapsto & b & & \end{array}$$

(1) is *not* split.

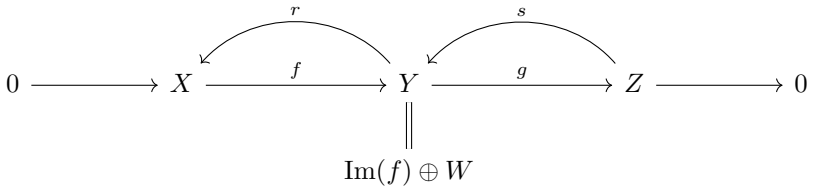
(2) is a *split exact sequence.*

Proposition 4.3.3 ([1, Props 10.25 & 26])**.** *Let (4.1) be a SES. The following are equivalent:*

1. *(4.1) is split.*

2. *There exists a* ***section*** s *of* g*, that is*
$$g \circ s = \mathrm{id}_Z \,.$$

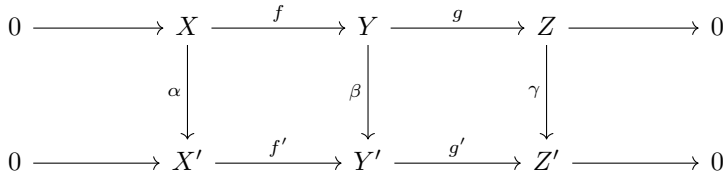
3. *There exists a* ***retraction*** r *of* f*, that is*
$$r \circ f = \mathrm{id}_X \,.$$



Proof. (2) ⇒ (1):
$$W = \mathrm{Im}(s), y \in \mathrm{Im}(f) \cap \mathrm{Im}(s) \Rightarrow y = s(z), y = f(x)$$
$$\begin{cases} g(y) = g(f(x)) = 0 \\ g(y) = g(s(z)) = z \end{cases} \Rightarrow z = 0 \Rightarrow y = s(z) = 0$$
$$\Rightarrow \mathrm{Im}(f) \cap \mathrm{Im}(s) = \{0\}$$
so that
$$\mathrm{Im}(f) \oplus \mathrm{Im}(s) = Y.$$
(3) ⇒ (1):
$$W = \ker(r) \ldots$$
□

4.4 Short 5-lemma

A morphism of SES is a diagram



where

(a) The two rows are SESs.

(b) The two squares commute, i.e.
$$\beta \circ f = f' \circ \alpha$$
and
$$\gamma \circ g = g' \circ \beta.$$

(c) α, β, γ are R-linear.

Proposition 4.4.1 ([1, Prop. 10.24]). *Consider a morphism of SES as above. If*

$$\alpha, \gamma \text{ are injective/surjective/bijective} \Rightarrow \beta \text{ injective/surjective/bijective.}$$

Proof. Suppose α, γ are *surjective*. We then want to show β surjective. We do it by type of reasoning called **diagram chasing**).

Let $y' \in Y'$. We want to prove that there exists a $y \in Y$ such that $\beta(y) = y'$. Consider $g'(y') \in Z'$. Since $\gamma\colon Z \to Z'$ is surjective, there exists a $z \in Z$ such that $\gamma(z) = g'(y')$. Since $g\colon Y \to Z$ is surjective, there exists a $\tilde{y} \in Y$ such that $g(\tilde{y}) = z$. It follows that

$$\begin{aligned} g'(\beta(\tilde{y})) &= \gamma(g(\tilde{y})) \\ &= \gamma(z) \\ &= g'(y'). \end{aligned}$$

We can not conclude that $\beta(\tilde{y}) = y'$, but we do know that $y' - \beta(\tilde{y}) \in ker(g')$. By exactness, $ker(g') = \mathrm{Im}(f')$, so $y' - \beta(\tilde{y}) \in \mathrm{Im}(f')$. It follows that there exists an $x' \in X'$ such that $f'(x') = y' - \beta(\tilde{y})$.

We assumed that $\alpha\colon X \to X'$ is surjective. So there exists an $x \in X$ such that $\alpha(x) = x'$. But then

$$\begin{aligned} \beta(f(x)) &= f'(\alpha(x)) \\ &= f'(x') \\ &= y' - \beta(\tilde{y}). \end{aligned}$$

It follows that $y' = \beta(f(x) + \tilde{y})$. So $y' \in \mathrm{Im}(\beta)$, and we are done.

□

4.5 The functor $\mathrm{Hom}_R(D, -)$

Let D be a fixed R-module. Then $\mathrm{Hom}_R(D, -)$ is a *left-exact covariant* functor.

Theorem 4.5.1 ([1, Thm. 10.28]). *Let*

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z$$

be a LES.

Then

$$0 \longrightarrow \mathrm{Hom}_R(D, X) \xrightarrow{f_*} \mathrm{Hom}_R(D, Y) \xrightarrow{g_*} \mathrm{Hom}_R(D, Z)$$

$$g_* f_*$$

is LES.

Proof. 1. (f_* is injective). Take

$$\alpha : D \to X$$

and

$$f_*\alpha : D \xrightarrow{\alpha} X \xrightarrow{f} Y$$

$$f(\alpha(x)) = 0$$
$$\Rightarrow \alpha(x) = 0 \quad (f \text{ injective})$$

2. $(\mathrm{Im}(f_*) \subseteq \ker(g_*))$. This is equivalent to $g_* \circ f_* = 0$
$$g_* \circ f_* = (g_* f_*) = 0_* = 0$$

3. $(\mathrm{Im}(f_*) \supseteq \ker(g_*))$. Pick
$$\beta : D \to Y$$
such that
$$g_*\beta : D \longrightarrow Y \longrightarrow Z$$
$$d \mapsto \beta(d) \mapsto g(\beta(d)) = 0.$$
is zero. By exactness,
$$\exists! x_d : f(x_d) = \beta(d).$$
Define $\alpha(d) := x_d$. This gives
$$\alpha : D \to X$$
such that
$$f_*\alpha = \beta.$$
Exc: α is a homomorphism.

□

Example 4.5.2. $\mathrm{Hom}_R(D, -)$ does not take SES to SES *in general*. Consider the SES
$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/n \to 0 \quad (\textit{not} \text{ split exact})$$
and take $D = \mathbb{Z}/n$. This gives

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/n) & \longrightarrow & 0 \\ & & \| & & \| & & \cong \downarrow & & \\ & & 0 & & 0 & & \mathbb{Z}/n & & \end{array}$$

$$0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z}/n \longrightarrow 0$$

which is not SES, only LES.

Proposition 4.5.3. $\mathrm{Hom}_R(D, -)$ *takes split SES to split SES.*

$\mathrm{Hom}_R(D, -)$ *sends the SES*
$$0 \longrightarrow X \longrightarrow X \oplus Z \longrightarrow Z \longrightarrow 0$$
to the SES

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_R(D, X) & \longrightarrow & \mathrm{Hom}_R(D, X \oplus Z) & \longrightarrow & \mathrm{Hom}_R(D, Z) & \longrightarrow & 0 \\ & & & \searrow^{\iota} & \downarrow \cong & \nearrow_{\pi} & & & \\ & & & & \mathrm{Hom}_R(D, X) \oplus \mathrm{Hom}_R(D, Z) & & & & \end{array}$$

Remark 4.5.4. Let $R = k$ be a field. *Then every* SES is split. This is because then every subspace $X \subset Y$ has a complement; Extend a basis

$$\{x_1, \dots, x_n\}$$

of X to a basis

$$\{x_1, \dots, x_n, w_1, \dots, w_m\}$$

of Y.

Set

$$W = \langle w_1, \dots, w_n \rangle \Rightarrow Y = X \oplus W$$

(This also works for X and Y infinite-dimensional.)

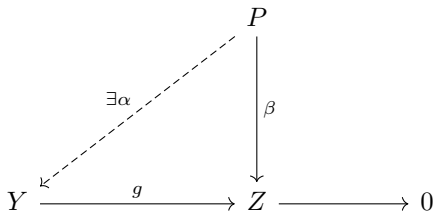
4.6 Projective Modules

Definition 4.6.1. An R-module is **projective** if $\mathrm{Hom}_R(P, -)$ is *exact*, i.e. takes SES to SES $\Leftrightarrow$ $\mathrm{Hom}_R(P, -)$ takes surjections to surjections

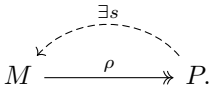
Proposition 4.6.2 ([1, Prop. 10.30])**.** *Let P be an R-module. Then the following are equivalent:*

(1) P is projective

(2) Given a surjection $g : Y \to Z$ and $\beta : P \to Z$, there exists $\alpha : P \to Y$ such that $\beta = g \circ \alpha$, that is, the following diagram commutes



(3) Given a surjection $\rho : M \twoheadrightarrow P$ there exists a section *$s : P \to M$ such that $\rho \circ s = \mathrm{id}_P$*



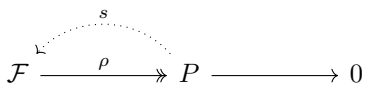
(4) P is a direct summand *of a free module (exists Q such that $P \oplus Q$ is free).*

Proof. (3) $\Rightarrow$ (4):

Take free module $\mathcal{F}$ surjecting onto P, that is, choose generators $p_1, \dots, p_n$ which gives $\mathcal{F} := R^n \to P$. In general, we can always take all elements of P as generators

$$\Rightarrow R^{\oplus P} \longrightarrow$$
$$Pe_p \longmapsto p$$

(3) says



$$\begin{aligned} \Rightarrow \mathcal{F} &= \ker(\rho) \oplus \mathrm{Im}(s) \\ &= Q \oplus P \end{aligned}$$ □

Corollary 4.6.3 ([1, Cor. 10.31])**.** *Free ⇒ Projective.*

In the following cases free ⇔ projective:

1. *R = field (every R-module is free, hence projective).*
2. *R = P.I.D. then a projective R-module M is free!*
3. *$R = k[x_1, \ldots, x_n]$ and the $k[x_1, \ldots, x_n]$-module M is finitely generated. (This is Quillen–Suslin's theorem, proven 1976.)*

Example 4.6.4 (Example of projective but not free.)**.**

$$R = R_1 \times R_2$$

$$M_{a,b} = R_1^{\oplus a} \times R_2^{\oplus b} \quad (a \neq b)$$

Then

$$\begin{aligned} M_{a,b} \oplus M_{N-a,N-b} &= M_{N,N} \\ &= R^{\oplus N} \end{aligned}$$

so $M_{a,b}$ direct summand of free module ⇒ $M_{a,b}$ are projective for all a, b by (4). Only free if $a = b$.

Example 4.6.5 (Dedekind domain not PID)**.**

$$I \text{ any ideal} \Leftrightarrow I \text{ projective}$$

$$I \text{ principal} \Leftrightarrow I \text{ free}$$

Example 4.6.6.

$$R = \mathbb{Z}[\sqrt{-5}], I = (3, 1 + \sqrt{-5})$$

$$\begin{array}{ccc} & \overset{s}{\curvearrowright} & \\ R^2 & \twoheadrightarrow & I \\ e_1 & \longmapsto & 3 \\ e_2 & \longmapsto & 1 + \sqrt{-5} \end{array}$$

Exercise: Find an explicit section s.

4.7 The contravariant Hom-functor

The contravariant $\mathrm{Hom}_R(-, D)$ takes RES to LES.

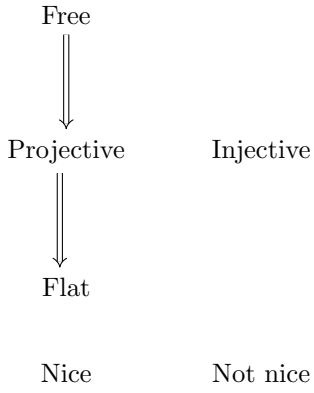
Definition 4.7.1. An R-module D is **injective** if $\mathrm{Hom}_R(-, D)$ takes SES to SES. Equivalently, it takes *injective* maps to *surjective* maps.

4.8 The tensor-functor

The functor $D \otimes_R -$ takes RES to RES.

Definition 4.8.1. An R-module D is **flat** if $D \otimes_R -$ takes SES to SES. Equivalently, it takes injective maps to injective maps.

4.9 Relation between projective, injective, flat and more



Free, projective and flat modules are in general easier to deal with than injective modules. For example, injective modules are usually not finitely generated whereas there are always free modules of finite rank. The notions of projective and injective are dual to each other in the sense that reversing all arrows for one notion gives the other. Still they behave very differently which can be explained by the fact that the opposite of the category of R-modules, while an abelian category, is not equivalent the the category of S-modules for any ring S.

Chapter 5

Fifth lecture

Linear Algebra revisited

- Book mostly vector space/field k.
- We'll also do R-modules/commutative rings.

5.1 Coordinates, matrices

R commutative ring, free module

$$\begin{aligned} R^k &:= \{(r_1, \ldots, r_k)\} \\ &= \left\{ \begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix} \;\middle|\; r_1, ..., r_k \in R \right\} \end{aligned}$$

M free module of rank k with basis

$$\begin{aligned} & B = (m_1, \ldots, m_k) \\ \Leftrightarrow \varphi : R^k & \xrightarrow{\cong} M \\ & e_i \longmapsto m_i \end{aligned}$$

i.e.

$$\begin{aligned} x \in M : x &= \sum x_i m_i \\ \Rightarrow \varphi^{-1}(x) &= \sum x_i e_i \\ &= (x_1, \ldots, x_k). \end{aligned}$$

$$\begin{aligned} f : R^k &\to R^\ell \\ f(e_j) &= \sum a_{ij} e_i \end{aligned}$$

$$\begin{aligned}\mathrm{Hom}_R(R^k, R^\ell) &\cong \mathrm{Mat}_{\ell\times k}(R)\\ (\bar{x} \mapsto A\bar{x}) &\leftarrow\!\shortmid A = (a_{ij})\end{aligned}$$

We have $[f] = A$.

Let M be free with basis $B = \{m_1, \ldots, m_k\}$ and let N be free with basis $\xi = \{n_1, \ldots, n_\ell\}$. We get the following diagram

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ \cong \uparrow \varphi_B & & \cong \uparrow \varphi_\xi \\ R^k & \xrightarrow[\quad g \quad]{} & R^\ell \end{array}$$

where $g = \varphi_\xi^{-1} \circ f \circ \varphi_B$ and

$$\begin{aligned}[f]_B^\xi &= M_B^\xi(f)\\ &= [g]\\ &= A.\end{aligned}$$

We have $f(m_j) = \sum a_{ij} n_i$.

5.2 Dual Module

Definition 5.2.1. Let R be a commutative ring and M an R-module. The **dual** of M is the R-module

$$\begin{aligned}M^* &= M^\vee\\ &= \mathrm{Hom}_R(M, R)\end{aligned} \tag{5.1}$$

Remark 5.2.2. 5.1 also works non-commutative ring R.

Suppose M is free with basis

$$\{m_1, \ldots, m_k\} \qquad (k \in \mathbb{Z}^+)$$

that is, we have a finite basis for M. Then let $m_i^* \in M^* = \mathrm{Hom}_R(M, R)$ be defined by

$$\begin{aligned}m_i^*(m_j) &= \delta_j^i\\ &= \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \qquad \text{(extend } m^* \text{ linearly to } M)\end{aligned}$$

Warning: m_i^* depends on *whole* basis, not just m_i.

Proposition 5.2.3 (18)**.** *$\{m_1^*, \ldots, m_k^*\}$ basis of M^*. If M is free of rank k then M^* free of rank k.*

Proof. Suppose

$$\alpha \in M^* \mid \alpha : M \to R.$$

α is determined by what it does on the basis $\{m_i\}$ of M, as follows

$$\begin{aligned}\alpha\Big(\underbrace{\sum x_i m_i}_{=x}\Big) &= \sum \alpha(m_i)x_i \\ &= \sum \alpha(m_i)m_i^*(\sum x_j m_j) \\ \Rightarrow \alpha(-) &= \sum \alpha(m_i)m_i^*(-).\end{aligned}$$

So α can be written as a linear combination of m_i^*. The elements $\alpha(m_i) \in R$ are the coordinates of α in the dual basis. We proved that the m_i^* generate M^*. On the other hand, suppose $\alpha(-) = \sum_{j=1}^{k} r_j m_j^*(-)$ for some $r_j \in R$. Then for each $1 \leq i \leq k$

$$\begin{aligned}\alpha(m_i) &= \sum_{j=1}^{k} r_j m_j^*(m_i) \\ &= r_i.\end{aligned}$$

We conclude that for all i, r_i is necessarily $\alpha(m_i)$. This means that the decomposition of α as a linear combination of m_i^*s is unique, and therefore m_i^*s form a basis. □

Excercise 5: If $M = \bigoplus_{\mathbb{N}} R$ then $M^* = \prod_{\mathbb{N}} R \Rightarrow$ basis $e_0, e_1, \ldots$ of $M \Rightarrow e_0^*, e_1^*, \ldots$ *not* a basis of M^* (too small).

Example 5.2.4.

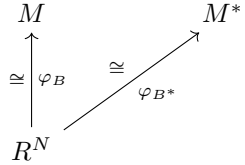
- $$\begin{aligned} R &= \mathbb{Z}, \\ M &= \mathbb{Z}/n, \\ \rightsquigarrow M^* &= \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) \\ &= 0\end{aligned}$$

- R^2, $\quad e_1, e_2 \rightsquigarrow e_1^*, e_2^* \in (R^2)^*$

$$R^2; \underbrace{e_1}_{f_1}, \underbrace{e_1 + e_2}_{f_2} \rightsquigarrow \begin{cases} f_1^*(f_1) = 1, & f_1^*(e_1) = 1 \\ f_1^*(f_2) = 0, & f_1^*(e_1 + e_2) = 0 \Rightarrow f_1^*(e_2) = -1 \end{cases}$$

  Showing dependence of other basis elements.

Warning: No *natural* isomorphism between M and M^*. If M has finite rank and we choose basis B then



so $M \cong M^*$ but *not* canonical, since depends on basis B.

Theorem 5.2.5 (19)**.** *There is a natural map*

$$M \xrightarrow[\varphi]{\cong} M^{**}.$$

This is an isomorphism if M is free of finite rank.

Proof. Given

$$x \in M \mid \varphi(x) \in M^{**} \Leftrightarrow \varphi(x) : M^* \to R$$

That is, the image of x under φ is an element α such that

$$\mathrm{Hom}_R(M^*, R) \ni \alpha \longmapsto \alpha(x) \in R$$

where we note that $\varphi(x)$ is R-linear.

$$\varphi : x \longmapsto \text{evaluation in } x.$$

If $m_1, \ldots, m_k$ is a basis for M then $m_1^*, \ldots, m_k^*$ is the dual basis for M^*. This implies that $m_1^{**}, \ldots, m_k^{**}$ is a basis for M^{**}.

$$m_1 \overset{\varphi}{\longmapsto} \text{evaluation in } m_1$$

$$m_i^{**}(m_j^*) = \delta_j^i$$

$$\begin{aligned} \underbrace{\varphi(m_i)(m_j^*)}_{\varphi \text{ isomorphism}} &= m_j^*(m_i) \\ &= \delta_j^i \end{aligned}$$

so $\varphi(m_i) = m_i^{**}$. □

5.3 Dual of Map

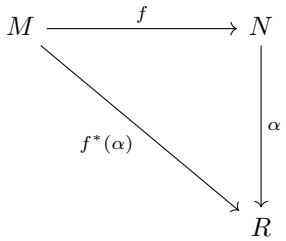
Let $M^* = \mathrm{Hom}_R(M, R)$ so that we get the *contravariant* functor $\mathrm{Hom}_R(-, R)$.

Take

$$f : M \to N \rightsquigarrow f^* : N^* \to M^*$$

i.e. we get the **pullback**

$$f^*(\alpha) = \alpha \circ f$$



Theorem 5.3.1 (20)**.** *If M has basis $\mathcal{B}$ and N has basis ξ, then*

$$f : M \to N \text{ has matrix } \left[f\right]_{\mathcal{B}}^{\xi} \tag{5.2}$$

$$f^* : N^* \to M^* \text{ has matrix } \left[f^*\right]_{\xi^*}^{\mathcal{B}^*} = \left(\left[f\right]_{\mathcal{B}}^{\xi}\right)^T \tag{5.3}$$

5.3.1 Contravariance

$$(AB)^T = B^T A^T$$

$$M \xrightarrow{f} N \xrightarrow{g} \mathcal{L} \qquad (g \circ f)^* = f^* \circ g^*$$

so that $M \xleftarrow{f^*} N \xleftarrow{g^*} \mathcal{L}$.

5.4 Duals, Hom, and $\otimes$ (*not* in [1])

Slogan:

$$M^* \otimes_R - = \mathrm{Hom}_R(M, -)$$

Theorem 5.4.1. *There exists a natural map*

$$M^* \otimes_R N \xrightarrow{\varphi} \mathrm{Hom}_R(M, N)$$

$$\varphi(m^* \otimes n) = \alpha(m)n.$$

This is an isomorphism if M is free of finite rank. (φ compatible with maps $M \to N'$ on both sides. Natural transformation of functors.)

Proof. Suppose M is free with basis $\mathcal{B} = (m_1, \ldots, m_k)$. Let $f : M \to N$ with N free with basis $\xi = \{n_1, \ldots, n_\ell\}$ Then $f(m_j) = \sum a_{ij} n_i$ and

$$\begin{aligned} A &= (a_{ij}) \\ &= [f]_{\mathcal{B}}^{\xi} \end{aligned}$$

$$\begin{aligned} f(\textstyle\sum x_j m_j) &= \sum_j x_j \sum_i a_{ij} n_i \\ &= \sum m_j^*(f(m_j)) \\ \Rightarrow f(-) &= \sum f(m_j) m_j^*(-) \end{aligned}$$

Define

$$\begin{aligned} \varphi^{-1}(f) &= \sum_j m_j^* \otimes f(m_j) \quad (\textit{verify} \text{ that } \varphi \text{ is linear}) \\ &= \sum_{i,j} a_{ij} \underbrace{(m_j^* \otimes n_i)}_{\text{basis for } M^* \otimes_R N} \end{aligned}$$

□

Corollary 5.4.2. *If $\mathcal{L}, M, N$ are R-modules and M is free of rank k, then*

$$\begin{array}{ccc} \mathrm{Hom}_R(\mathcal{L}, M^* \otimes N) & \xrightarrow[\varphi_*]{\cong} & \mathrm{Hom}_R(\mathcal{L}, \mathrm{Hom}_R(M, N)) \\ & & \Big\downarrow \cong \quad \textit{Theorem 13} \\ & & \mathrm{Hom}_R(\mathcal{L} \otimes_R M, N) \end{array}$$

Example 5.4.3.

$$f : R^2 \to R^2 \quad [f] = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad \text{(previous example)}$$
$$f^* : \underbrace{R^2}_{M^*} \to R^2$$

$$\begin{aligned} [f^*] &= [f]^T \\ &= \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{(shows contravariance)} \end{aligned}$$

$$(f^*)^{-1} : R^2 \to R^2 = M^*, \qquad \left([f]^T\right)^{-1} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \quad f_1^* = e_1^* - e_2^*$$

Since $M \cong M^*$, we get $\mathrm{Hom}_R(\mathcal{L}, M \otimes N) \xrightarrow{\cong} \mathrm{Hom}_R(\mathcal{L} \otimes M^*, N)$ by letting M and M^* be as above (?).

5.5 Trace (not in [1])

Given

$$M \xrightarrow{f} M$$

R-linear, M free of finite rank, want to define $\mathrm{tr}(f)$

$$\begin{array}{l} \mathrm{Hom}_R(M, M) \xrightarrow[\cong]{\varphi^{-1}} M^* \otimes M \xrightarrow{ev} R \\ \mathrm{tr} := ev \circ \varphi^{-1} \quad \mathrm{ev}(\alpha \otimes x) = \alpha(x) \end{array}$$

Exc: Recovers usual trace.

5.6 Multilinear & alternating maps

Definition 5.6.1. Let M and $\mathcal{L}$ be R-modules.

A map $\varphi : M^{\times n} \to \mathcal{L}$ is

(i) **multilinear** if linear in *each* argument.

(ii) **symmetric** if

$$\varphi(\ldots, x_i, \ldots, x_j, \ldots) = \varphi(\ldots, x_j, \ldots, x_i, \ldots) \qquad (\forall i, j \in \{1, \ldots, n\} \mid i \neq j)$$

(iii) **antisymmetric** if

$$\varphi(\ldots, x_i, \ldots, x_j, \ldots) = -\varphi(\ldots, x_j, \ldots, x_i, \ldots) \qquad (\forall i, j \in \{1, \ldots, n\} \mid i \neq j)$$

(iv) **alternating** if

$$\varphi(\ldots, x_i, \ldots, x_i, \ldots) = 0 \qquad (\forall i \in \{1, \ldots, n\})$$

Proposition 5.6.2 (22)**.** *Alternating multilinear* $\Rightarrow$ *antisymmetric multilinear.*

Antisymmetric $\Rightarrow \varphi(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \operatorname{sgn}(\sigma)\varphi(x_1, \ldots, x_n)$ *for any* $\sigma \in S_n$.

Proof. Left to reader. □

5.7 Determinants

Theorem 5.7.1 (24)**.** *Let* $M \cong R^n$*, that is, be a free module of finite rank. The determinant*

$$\det : (R^n)^{\times n} \to R$$

$$\det(x_1, \ldots, x_n) = \begin{vmatrix} \vdots & & \vdots \\ x_1 & \ldots & x_n \\ \vdots & & \vdots \end{vmatrix}$$

is the unique *multilinear alternating form such that* $\det(e_1, \ldots, e_n) = 1$

Remark 5.7.2. *Form* in means target of map R.

Proof. Suppose D is another such function so that

$$\begin{aligned}
D(x_1,\dots,x_n) &= D\Big(\sum a_{i1}e_i,\dots,\sum a_{in}e_i\Big)\\
&= \sum_{i_1,\dots,i_n=1}^{n} a_{i_1 1}\cdots a_{i_n n} D(e_1,\dots,e_n)\\
&= \sum_{I} a_{i_1 1}\cdots a_{i_n n} D(e_1,\dots,e_n)\\
&= \sum_{\sigma\in S_n} a_{\sigma(1)1}\cdots a_{\sigma(n)n} D(e_{\sigma(1)},\dots,e_{\sigma(n)})\\
&= \sum_{\sigma\in S_n} a_{\sigma(1)1}\cdots a_{\sigma(n)n}\operatorname{sgn}(\sigma)\underbrace{D(e_1,\dots,e_n)}_{=1}\\
&= \det(x_1,\dots,x_n)
\end{aligned}$$

where we have denoted I as the set composed of all elements $(i_1,\dots,i_n)$ such that

$$i_1 \neq i_2 \neq \dots \neq i_n.$$

□

Remark 5.7.3. We used that D is multilinear in the second equality, and alternating in the third equality above.

Corollary 5.7.4. *Any n-multilinear map* alternating *map D is a constant $\cdot \det(-)$ and the constant is $D(e_1,\dots,e_n)$.*

Theorem 5.7.5 (28)**.**

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

Proof. Keep A fixed, then LHS and RHS becomes functions of

$$B = \begin{bmatrix} \vdots & & \vdots \\ x_1 & \dots & x_n \\ \vdots & & \vdots \end{bmatrix}$$

$$\begin{aligned}
LHS &= \det(AB)\\
&= \det(Ax_1,\dots,Ax_n)\\
RHS &= \det(A)\det(x_1,\dots,x_n)
\end{aligned}$$

Exc: LHS and RHS alternating and multilinear.

$$\begin{aligned}
LHS &= \text{constant}\cdot\det(x_1,\dots,x_n)\\
&= LHS\cdot(e_1,\dots,e_n)\cdot\det(x_1,\dots,x_n)\\
&= \det(A)\det(B)\\
&= RHS
\end{aligned}$$

□

Definition 5.7.6. Let A be an $n \times n$ matrix with values in R. The **adjugate** matrix of A is

$$A^{\text{adj}} = C^T$$

where

$$C_{ij} = (-1)^{i+j} \det((i,j)\text{-minor of A})$$

(i,j)-minor = remove i^{th} row and j^{th} column of A.

Theorem 5.7.7 (30)**.**

(1)

$$\begin{aligned} \det(A)I &= AA^{\text{adj}} \\ &= A^{\text{adj}}A. \end{aligned}$$

(2)

$$A \textit{ is invertible} \Leftrightarrow \det(A) \in R \textit{ is a unit}$$

then $A^{-1} = (\det(A))^{-1}A^{\text{adj}}$.

Proof. A invertible

$$\begin{aligned} \Rightarrow 1_R &= \det(I) \\ &= \det(AA^{-1}) \\ &= \det(A)\det(A^{-1}) \\ \Rightarrow \det(A) &\text{ unit.} \end{aligned}$$

$$\det(A) \text{ unit} \Rightarrow A^{-1} = (\det(A))^{-1}A^{\text{adj}}.$$

This shows the "only if"-direction in (2)[1]. □

[1] If we have a proposition $A \Leftrightarrow B$, then $A \Rightarrow B$ is the only if direction, and $B \Rightarrow A$ is the if direction.

Chapter 6

Sixth lecture

Today:

- R is *unital* commutative ring.
- M is an R-module with
$$mr = rm \quad (\forall r \in R, \forall m \in M)$$

$M \otimes_R M$ is again an R-module. We can iterate the construction to form the modules

$$\begin{aligned}\underbrace{M \otimes_R \cdots \otimes_R M}_{n \text{ times}} &= M^{\otimes n} \\ &= T^n(M).\end{aligned}$$

Comment 6.1.1. Unless otherwise noted, we will just write $\otimes$ for $\otimes_R$.

Example 6.1.2.
$$\mathbb{Q}/\mathbb{Z} \otimes \mathbb{Q}/\mathbb{Z} \cong 0.$$

$$x \otimes y = 0 \text{ where } x \text{ is divisible by } r \text{ and } y \text{ is } r\text{-torsion} \Rightarrow (\mathbb{Q}/\mathbb{Z})^{\otimes n} = 0 \quad (\forall n \geq 2).$$

Example 6.1.3. $M \cong Rx$ free module with generator x

$$\begin{aligned}\rightsquigarrow M \otimes M &\cong Rx \otimes Ry \\ &\cong R(x \otimes y)\end{aligned}$$

Example 6.1.4. More generally than 6.1.3, suppose

$$M \cong \bigoplus_{i=1}^{n} Rx_i$$

is a free module of rank n with basis $x_1, \ldots, x_n$. Then

$$\begin{aligned} M \otimes M &\cong (Rx_1 \oplus \cdots \oplus Rx_n) \otimes (Rx_1 \oplus \cdots \oplus Rx_n) \\ &\cong \bigoplus_{i,j=1}^{n} R(x_i \otimes x_j) \end{aligned}$$

of rank n^2 with basis $\{x_i \otimes x_j\}_{i,j=1}^{n}$.

Remark 6.1.5. Note that we used (4) in 6.1.4.

Example 6.1.6. Even more generally

$$(R^{\oplus k})^{\otimes n} \cong R^{\oplus k^n}$$

with basis

$$\{x_{i_1} \otimes \cdots \otimes x_{i_n}\}_{1 \leq i_1, \ldots, i_n \leq k}$$

So, for example, we have that

$$\begin{aligned} (R^{\oplus 3})^{\otimes 3} &= (R \oplus R \oplus R) \otimes (R \oplus R \oplus R) \otimes (R \oplus R \oplus R) \\ &\cong \left(\bigoplus_{j=1}^{3} R\right) \otimes \left(\bigoplus_{j=1}^{3} R\right) \otimes \left(\bigoplus_{j=1}^{3} R\right) \\ &\cong \left(\bigoplus_{j=1}^{3} R\right) \otimes \left(\left(\bigoplus_{j=1}^{3} R\right) \otimes ((R \oplus R) \oplus R)\right) \\ &\cong \left(\bigoplus_{j=1}^{3} R\right) \otimes \left(\left(\bigoplus_{j=1}^{3} R\right) \otimes (R \oplus R) \oplus \left(\bigoplus_{j=1}^{3} R\right) \otimes R\right) \\ &\cong \left(\bigoplus_{j=1}^{3} R\right) \otimes \left(\left(\bigoplus_{j=1}^{3} R\right) \otimes R \oplus \left(\bigoplus_{j=1}^{3} R\right) \otimes R \oplus \left(\bigoplus_{j=1}^{3} R\right) \otimes R\right) \\ &\cong \left(\bigoplus_{j=1}^{3} R\right) \otimes (R^{\oplus 9}) \\ &\cong \bigoplus_{i=1}^{3} (R \otimes R^{\oplus 9}) \\ &\cong R^{\oplus 27} \\ &= R^{3^3} \end{aligned}$$

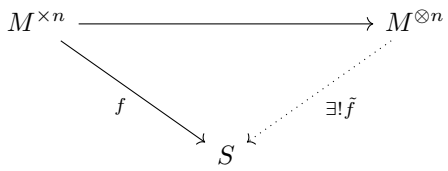
where we (aside from (4)) in the next to last equality used that $R \otimes R \cong R$.

If

$$M = \bigoplus_{i=1}^{k} Rx_i$$

then $M^{\otimes n}$ is freely generated by monomials of degree n in k non-commuting variables.

There is an R-multilinear map



that is universal in the sense that for any R-module S and any multilinear map

$$f : M^n \to S$$

there exists a unique R-linear map

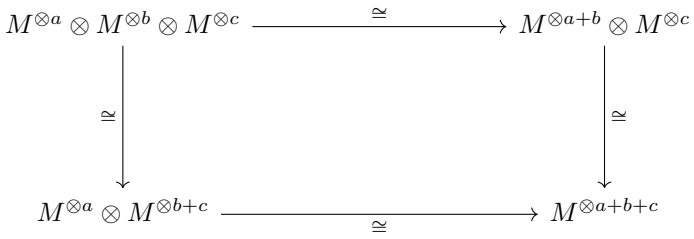
$$\tilde{f} : M^{\otimes n} \to S$$

such that the diagram above commutes.

There is a natural isomorphism

$$M^{\otimes a} \otimes M^{\otimes b} \cong M^{\otimes a+b}.$$

It is associative in the sense that the following diagram commutes



6.2 Symmetric multilinear maps

Definition 6.2.1. A multilinear map

$$f : M^n \to S$$

is **symmetric** if

$$\forall m_1, \ldots, m_n \in M$$

and

$$\forall \sigma \in S_n$$

we have

$$f(m_1, \ldots, m_n) = f(m_{\sigma(1)}, \ldots, m_{\sigma(n)}).$$

Lemma 6.2.2. *A map f is symmetric*

$$\Leftrightarrow$$

$$\forall i : 1 \leq i \leq n-1$$

we have

$$f(m_1, \ldots, m_i, m_{i+1}, \ldots, m_n) = f(m_1, \ldots, m_{i+1}, m_i, \ldots, m_n).$$

Proof. The only if direction is clear from the definition of a symmetric map.

The if statement follows from the fact that each element

$$\sigma \in S_n$$

can be written as a composition of transpositions

$$(1\ 2), (2\ 3), \ldots, (n\ n-1) \in S_n.$$

For example: Suppose

$$f(m_1, m_2, m_3) = f(m_2, m_1, m_3).$$

and

$$f(m_1, m_2, m_3) = f(m_1, m_3, m_2).$$

Then

$$f(m_1, m_2, m_3) = f(m_2, m_1, m_3) = f(m_1, m_3, m_2)$$

□

Proposition 6.2.3. *A multilinear map $f : M^{\times n} \to S$ is symmetric $\Leftrightarrow$ the associated homomorphism $\tilde{f} : M^{\otimes n} \to S$ satisfies*

$$\tilde{f}(m_1 \otimes \cdots \otimes m_n) = \tilde{f}(m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(n)}) \quad (\forall m_1, \ldots, m_n \in M, \forall \sigma \in S_n).$$

But then

$$\tilde{f}(m_1 \otimes \cdots \otimes m_n) - \tilde{f}(m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(n)}) = 0.$$

Definition 6.2.4. Let $C^n(M) \subset M^{\otimes n}$ be the submodule

$$\langle m_1 \otimes \cdots \otimes m_n - m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(n)} \mid m_i \in M, \sigma \in S_n \rangle.$$

The n^{th} **symmetric power** of M is

$$\underbrace{S^n(M)}_{\text{[1]:s notation}} = \underbrace{M^{\otimes n}/S_n}_{\text{Gregory:s notation}}$$
$$:= M^{\otimes n}/C^n(M).$$

There is a canonical surjective homomorphism

$$M^{\otimes n} \twoheadrightarrow S^n(M)$$

explicitly defined by

$$m_1 \otimes \cdots \otimes m_n \longmapsto [m_1 \otimes \cdots \otimes m_n].$$

Lemma 6.2.5. *Suppose*

$$M = \bigoplus_{i=1}^{k} Rx_i$$

is a free module of rank k with basis $x_1, \dots, x_k$.

Then $S^n(M)$ is a free module with basis

$$\{x_{i_1} \otimes \cdots \otimes x_{i_n} \mid 1 \le i_1 \le \ldots \le i_n \le k\}$$

$$S^n(R^{\oplus k}) \text{ has rank } \binom{n+k-1}{k}$$

Proof sketch. We know that $M^{\otimes n}$ has basis $x_{i_1}, \dots, x_{i_n}$. A homomorphism $\tilde{f} : M^{\otimes n} \to S$ is the same as a function $\tilde{f} : \{x_{i_1} \otimes \cdots \otimes x_{i_n}\} \to S$. $\tilde{f}$ is symmetric as a homomorphism

$$\Leftrightarrow \tilde{f}(x_{i_1} \otimes \cdots \otimes x_{i_n}) = \tilde{f}(x_{i_{\sigma(1)}} \otimes \cdots \otimes x_{i_{\sigma(n)}}) \qquad (\forall \sigma \in S_n).$$

Every sequence $(i_1, \dots, i_n)$ has a (*unique*) monotonic rearrangement.

On the other hand, any function on monic sequences

$$(i_1, \dots, i_n)$$

extends *uniquely* to a symmetric function on *all* sequences. □

Remark 6.2.6.

- If $M = Rx_1 \oplus \cdots \oplus Rx_k$ then $S^n(M)$ is the free module generated by monomials of degree n in commuting variables
$$x_1, \dots, x_n.$$
- There is a natural homomorphism $S^a(M) \otimes S^b(M) \to S^{a+b}(M)$ explicitly defined by
$$[m_1 \otimes \cdots \otimes m_a] \otimes [m'_1 \otimes \cdots \otimes m'_b] \longmapsto [m_1 \otimes \cdots \otimes m_a \otimes m'_1 \otimes \cdots \otimes m'_b]. \tag{6.1}$$
This is <u>not</u> an isomorphism. But it is associative.

6.3 Alternating maps

Definition 6.3.1. A multilinear map $f : M^n \to S$ is **alternating** if

$$f(m_1, \dots, m_m) = 0$$

whenever $m_i = m_j$ for some $i \neq j$.

Lemma 6.3.2. *An alternating map is **skew-symmetric**, meaning, for all $\sigma \in S_n$, we have*

$$f(m_1, \dots, m_n) = \operatorname{sgn}(\sigma) f(m_{\sigma(1)}, \dots, m_{\sigma(n)})$$

where

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, \text{ if } \sigma \in A_n \text{ (is an even permutation)} \\ -1, \text{if } \sigma \notin A_n \text{ (is not an even permutation)} \end{cases}$$

Proof. We prove $f(m_1, m_2, m_3, \ldots, m_n) = -f(m_2, m_1, m_3 \ldots, m_n)$.

$$\begin{aligned} 0 &= f(m_1 + m_2, m_1 + m_2, m_3, \ldots, m_n) \\ &= \underbrace{f(m_1, m_1, m_3, \ldots, m_n)}_{=0} + f(m_1, m_2, m_3, \ldots, m_n) + f(m_2, m_1, m_3, \ldots, m_n) + \underbrace{f(m_2, m_2, m_3, \ldots, m_n)}_{=0} \\ \Leftrightarrow 0 &= f(m_1, m_2, m_3, \ldots, m_n) + f(m_2, m_1, m_3, \ldots, m_n) \\ \Leftrightarrow -f(m_2, m_1, m_3, \ldots, m_n) &= f(m_1, m_2, m_3, \ldots, m_n) \text{ or } f(m_1, m_2, m_3, \ldots, m_n) = -f(m_2, m_1, m_3, \ldots, m_n). \end{aligned}$$

□

Lemma 6.3.3. *f is alternating if*

$$f(m_1, \ldots, m_{i-1}, m, m, m_{i+2}, \ldots, n) = 0 \qquad (\forall i)$$

Proof by example. Suppose f is a multilinear map such that

$$\begin{aligned} f(x, x, y) &= f(x, y, y) \\ &= 0 \qquad (\forall x, y) \end{aligned}$$

then

$$\begin{aligned} f(x + y, x + y, z) &= \underbrace{f(x, x, z)}_{0} + f(x, y, z) + f(y, x, z) + \underbrace{f(y, y, z)}_{0} \\ &= 0 \end{aligned}$$

and therefore $f(x, y, z) = -f(y, x, z)$. Similarly, the assumption $f(x, y, y) = 0$ implies that for all x, y, z, we have

$$f(x, y, z) = -f(x, z, y).$$

Now we can conclude

$$\begin{aligned} f(x, y, x) &= -f(y, x, x) \\ &= 0 \end{aligned}$$

so that f is alternating (6.3.1). □

Proposition 6.3.4. *A multilinear map $f : M^n \to S$ is alternating $\Leftrightarrow$ the associated homomorphism $\tilde{f} : M^{\otimes n} \to S$ satisfies*

$$\tilde{f}(m_1 \otimes \cdots \otimes m_{i-1} \otimes m \otimes m \otimes m_{i+2} \otimes \cdots \otimes m_n) = 0 \qquad (\forall m_i \in M, \forall i \in \{1, \ldots, n\})$$

6.4 Exterior Algebras

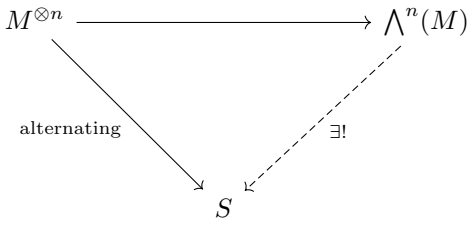
Definition 6.4.1. Define $A^n(M) \subset M^{\otimes n}$ to be the submodule generated by

$$\langle m_1 \otimes \cdots \otimes m_i \otimes \cdots \otimes m_j \otimes \cdots \otimes m_n \mid m_i = m_j, \text{ for some } i \neq j \rangle.$$

Definition 6.4.2. The n^{th} **exterior power** of M is denoted

$$\bigwedge^n(M) := M^{\otimes n}/A^n(M).$$

There is a canonical alternating map



that has the usual universal property

$$m_1 \otimes \cdots \otimes m_n \longmapsto m_1 \wedge \cdots \wedge m_n \qquad (\wedge \text{ is called the "wedge-product".})$$

Let $m_1 \wedge \cdots \wedge m_n$ be the image of $m_1 \otimes \cdots \otimes m_n$ in $\bigwedge^k(M)$:

(i) $m_1 \wedge \cdots \wedge m_n$ generates $\bigwedge^n(M)$

(ii) $m_{\sigma(1)} \wedge \cdots \wedge m_{\sigma(n)} = \operatorname{sgn}(\sigma)(m_1 \wedge \cdots \wedge m_n) \qquad (\sigma \in S_n).$

Furthermore, if $m_i = m_j$ for some $i < j$ then

$$m_1 \wedge \cdots \wedge m_i \wedge \cdots \wedge m_j \wedge \cdots \wedge m_n = 0.$$

Lemma 6.4.3. *Suppose*

$$M = \bigoplus_{i=1}^{k} Rx_i$$

is a free module of rank k with basis $x_1, \ldots, x_k$. Then $\bigwedge^n(M)$ is a free module with basis

$$\{x_{i_1} \wedge \cdots \wedge x_{i_n} \mid 1 \leq i_1 < \ldots < i_n \leq k\}$$

Proof. A function

$$f : \{x_{i_1} \wedge \cdots \wedge x_{i_n} \mid 1 \leq i_1 < \ldots < i_n \leq k\} \to S$$

determines a *unique* alternating map $M^n \to S$. The rank of $\bigwedge^n \left(R^{\oplus k}\right) = \binom{k}{n}$ in particular

$$\bigwedge^n \left(R^{\oplus k}\right) = 0 \qquad (\text{if } n > k). \tag{6.2}$$

where $\bigwedge^n \left(R^{\oplus n}\right) \cong Rx_1 \wedge \cdots \wedge x_n$ □

6.5 Functorial properties of $T^n, S^n, \bigwedge^n$

Observation: The constructions $T^n, S^n, \bigwedge^n$ are all *functors* from R-**Mod** to R-**Mod**.

This means that for *any* R-module homomorphism $f : M \to N$ one obtains homomorphisms

$$T^n(f) : T^n(M) \to T^n(N); \quad S^n(f) \colon S^n(M) \to S^n(N); \quad \text{and } \wedge^n(f) \colon \wedge^n(M) \to \wedge^n(N).$$

The homomorphism $T^n(f)$ is defined explicitly by the formula

$$m_1 \otimes \cdots \otimes m_n \longmapsto f(m_1) \otimes \cdots \otimes f(m_n).$$

The homomorphisms $S^n(f)$ and $\bigwedge^n(f)$ are defined similarly. One can also deduce these homomorphisms from the universal properties of these constructions.

Furthermore, we have functoriality properties. For example, if we have another homomorphism $g : K \to N$ then $T^n(g \circ f) = T^n(g) \circ T^n(f)$ and also $T^n(1_M) = 1_{T^n(M)}$. Similar relations hold for S^n and $\wedge^n$.

The functoriality of exterior power has perhaps the most interesting implications. Suppose

$$f : R^n \to R^n$$

is a homomorphism from a free R-module to itself. Such a homomorphism is represented by a matrix:

$$f \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix}$$

for some matrix A with entries in R.

Question 6.5.1. What is the induced homomorphism

$$\bigwedge^n(f) : \underbrace{\bigwedge^n(R^n)}_{\cong Rx_1 \wedge \cdots \wedge x_n} \to \underbrace{\bigwedge^n(R^n)}_{\cong Rx_1 \wedge \cdots \wedge x_n}$$

It is an R-module homomorphism from R to itself. We know that $\mathrm{Hom}_R(R, R) \cong R$, and any homomorphism f is just multiplication by $f(1)$. In our case, the map has the following effect on the chosen generator:

$$x_1 \wedge \cdots \wedge x_n \longmapsto (a_{11}x_1 + \ldots + a_{n1}x_n) \wedge \cdots \wedge (a_{1n}x_1 + \ldots + a_{nn}x_n)$$

What is

$$(a_{11}x_1 + \ldots + a_{n1}x_n) \wedge \cdots \wedge (a_{1n}x_1 + \ldots + a_{nn}x_n)?$$

It is an element of $\bigwedge^n(R^n) = Rx_1 \wedge \ldots \wedge x_n$, and therefore it is the multiple of $x_1 \wedge \ldots \wedge x_n$ by some element of R. Which element? We can think of it as a function from $M_{n,n}(R)$ to R. This function is alternating and multilinear in the columns of the matrix, and it clearly takes the identity matrix to 1. Therefore it must coincide with $\det(A)$.

Thus for any homomorphism $f\colon R^{\oplus n} \to R^{\oplus n}$ represented by a matrix A, the induced homomorphism $\bigwedge^n(f)$ is multiplication by $\det(A)$. The functoriality relation $\bigwedge^n(f \circ g) = \bigwedge^n(f) \circ \bigwedge^n(g)$ gives a conceptual reason for the relation

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

Chapter 7

Seventh lecture

7.1 Torsion & rank

Let R be an integral domain and M an R-module.

Definition 7.1.1. Let R be an integral domain and M an R-module. We define

$$\mathrm{Tor}(M) := \{x \in M \mid \exists r \in R \setminus \{0\} : rm = 0\}$$

as the **torsion submodule** of M.

Remark 7.1.2. Let

$$K = \mathrm{Frac}(R) \Rightarrow R \subset K$$
$$M \xrightarrow{\alpha} M \otimes_R K \qquad \ker(\alpha) = \mathrm{Tor}(M)$$
$$x \longmapsto x \otimes 1$$

Definition 7.1.3. Let R be an integral domain and M an R-module. Then M is **torsion** if $M = \mathrm{Tor}(M)$.

Definition 7.1.4. Let R be an integral domain and M an R-module. Then M is **torsionfree** if $\mathrm{Tor}(M) = \{0\}$.

We have an SES

$$0 \to \mathrm{Tor}(M) \to M \to M/\mathrm{Tor}(M) \to 0. \tag{7.1}$$

Remark 7.1.5. $M/\mathrm{Tor}(M)$ is torsionfree (7.1.4); if $y \in M/\mathrm{Tor}(M)$ is torsion $\Rightarrow \exists r \in R \setminus \{0\} : ry = 0$. Pick $x \in M$ such that $y = \bar{x}$.

Then

$$ry = 0 \in M/\mathrm{Tor}(M) \Rightarrow ry \in \mathrm{Tor}(M).$$

This implies that there exists $s \in R \setminus \{0\}$ such that

$$sry = 0 \Rightarrow y \in \mathrm{Tor}(M)$$

$$\Rightarrow y = \overline{x} = 0.$$

7.2 Structure theorem over P.I.D.:s

Let R be a P.I.D. and let M be a finitely generated R-module. Then M torsionfree $\Rightarrow$ M free. Since M free $\underbrace{\Rightarrow}_{4.9}$ M projective so (7.1) splits $\Rightarrow M \cong \operatorname{Tor}(M) \oplus M/\operatorname{Tor}(M)$.

If R Dedekind domain (note that P.I.D.:s are Dedekind domains) then

$$\text{torsionfree} \Rightarrow \text{projective}$$

so that (7.1) splits as well.

Example 7.2.1. Any ideal of $R = k[x, y]$ is torsionfree.

If I is not principal, then I not free. So take $I = (x, y)$, torsionfree (7.1.4) but not free.

Definition 7.2.2 (Rank). The rank of M, denoted $\operatorname{rk}(M)$ is the largest number of linearly independent elements of M.

Example 7.2.3.

$$\operatorname{rk}(M) = \dim_K(M \otimes_R K) \qquad (K = \operatorname{Frac} R).$$

One could also write this as $\operatorname{rk}(M) = \dim_K(M \otimes_R R_0)$ where $R_0 = (R - \{0\})^{-1}R$ is the localization (**??**) at 0 of R, which if R is an integral-domain, is the field of fraction of R (thinking about what localization does, this is quite clear). E.g.

$$\operatorname{rk}(R^r) = r \qquad (R^r \otimes_R K \cong K^r)$$

Theorem 7.2.4. *[**Fundamental theorem of finitely generated modules over a P.I.D.**(4)]*

Let M be a free R-module s.t.

$$\operatorname{rk}(M) = n.$$

Let $N \subset M$ be a submodule. Then

1. *N is free of rank $m \leq n$.*
2. *$\exists$ basis $y_1, \ldots, y_n$ of M and $a_1, \ldots, a_m \in R$ such that*

$$a_1 y_1, \ldots, a_m y_m$$

basis of N and such that

$$a_1 | a_2 | a_3 | \ldots | a_m \qquad (a_1 \text{ divides } a_2 \text{ divides } \ldots).$$

$$\begin{array}{ccccc} N & & \subset & & M \\ \Big\downarrow \cong & & & & \Big\downarrow \cong \\ R^m & & \hookrightarrow & & R^n \end{array}$$

$a_i y_i$ on the left; basis y_i on the right.

$$\begin{pmatrix} a_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_m \\ 0 & 0 & 0 \\ \vdots & \ddots & \vdots \\ 0 & 0 & 0 \end{pmatrix}$$

Theorem 7.2.5 (5/6 in [1]). *Let R be a P.I.D. and let M be a finitely generated R-module.*

Then

(1) $M \cong R^r \oplus \mathrm{Tor}(M)$.

(2) M torsionfree $\Leftrightarrow$ M free.

(3) (invariant factor form)

$$\mathrm{Tor}(M) = R/(a_1) \oplus R/(a_2) \oplus \ldots \oplus R/(a_m)$$

where

$$a_1 | a_2 | a_3 | \ldots | a_m \qquad (a_i \text{ not unit}).$$

(4) (elementary factor form)

$$\mathrm{Tor}(M) = R/(p_1^{\alpha_1}) \oplus \ldots \oplus R/(p_s^{\alpha_s})$$

where $p_i \in R$ is a prime element and $\alpha_i \in \mathbb{Z}^+$

$$\Leftrightarrow$$

Irreducible (since R is a P.I.D., hence an UFD).

Proof.

(1) $\Rightarrow$ (2): M torsionfree $\Leftrightarrow \mathrm{Tor}(M) = \{0\}$, so by assumption $M \cong R^r$ free.

(2) $\Rightarrow$ (1): $M/\mathrm{Tor}(M)$ is torsion free $\overset{(2)}{\Rightarrow}$ free, hence 7.1 splits $\Rightarrow$ (1).

(3) $\Rightarrow$ (4): $R/(a) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_s^{\alpha_s})$ by generalized chinese remainder theorem, where, since we have a P.I.D., hence a UFD, we have a unique factorization of a (up to a unit) as

$$a = u p_1^{\alpha_1} \cdots p_s^{\alpha_s} \qquad (\text{u unit}, p_i \text{ prime}, \alpha_i \in \mathbb{Z}^+).$$

(1)+(3): Pick a presentation of M (generators $x_1, \ldots, x_n$ of M).

$$\begin{aligned} F &\overset{\alpha}{\twoheadrightarrow} M \\ e_i &\longmapsto x_i \end{aligned}$$

We have that $\ker(\alpha) \subset F$ and that by 7.2.4 *ker*(α) is free of rank $m \leq n$ and if F has basis $y_1, \ldots, y_n$ then $\ker(\alpha)$ has basis $a_1 y_1, \ldots, a_m y_m$ where $a_1 | a_2 | \ldots | a_m$

$$\begin{aligned} \Rightarrow M &\cong F/\ker(\alpha) \\ &\cong (Ry_1 \oplus \ldots \oplus Ry_n)/\langle a_1 y_1, \ldots, a_m y_m \rangle \\ &\cong R/(a_1) \oplus \ldots \oplus R/(a_m) \oplus R^{n-m} \end{aligned}$$

□

Example 7.2.6.

$$\mathbb{Z}/(8) \oplus \mathbb{Z}/(9) \oplus \mathbb{Z}(5) \oplus \mathbb{Z}/(7^3) \cong \mathbb{Z}/(2^3 \cdot 3^2 \cdot 5 \cdot 7^3)$$

Example 7.2.7.

$$\underbrace{\mathbb{Z}/(12)}_{3\cdot 2^2} \underbrace{\oplus \mathbb{Z}/(10)}_{5\cdot 2} \oplus \underbrace{\mathbb{Z}/(25)}_{5^2} \cong \mathbb{Z}/(10) \oplus \mathbb{Z}/(300)$$

On theorem 9 (uniqueness): In the structure thm:

- r is unique.
- $a_1, a_2, \ldots, a_m$ is unique up to multiplication with units.
- $p_i^{\alpha_i}$ is unique up to multiplication with units and permutation of order.

On the proof: $\mathrm{Tor}(M) = \bigoplus \mathrm{Tor}_p(M)$ where p is prime.

$$\mathrm{Tor}_p(M) = \{x \in M \mid p^a x = 0 \text{ for some } a > 0\}$$

Proof of Thm 4:

$$\Sigma = \{\varphi(N) \mid N \in M^* = \mathrm{Hom}_R(M, R)\}$$

This is a set of ideals of R, ordered by inclusion.

R PID $\Rightarrow \varphi(N) = a_\varphi$. We have that Σ is not empty, since $a_0 = (0) \in \Sigma$.

If R is noetherian, then Σ has maximal elements (later). Pick $a_1 \in \Sigma$ maximal. Pick $u \in M^*$ such that $u(N) = (a_1)$.

Pick $y \in N$ such that $u(y) = a_1$.

Claim 1: $a_1 \neq 0$. Pick basis $x_1, \ldots, x_n$ of M.

Pick $z \in N \setminus \{0\}$. Then $z = \sum z_i x_i$ (some $z_i \neq 0$).

Then

$$x_i^*(z) = z_i \neq 0 \Rightarrow (x_i^*)(N) \supseteq (x_i^*)(z_i) \neq (0)$$

so that $\Sigma \neq \{(0)\}$.

Claim 2: $a_1 | \varphi(y)$ for all $\varphi \in M^*$.

Proof.

$$(a_1) + (\varphi(y)) = (d)$$

and exists $r_1, r_2 \in R$ such that $r_1 a_1 + r_2 \varphi(y) = d$. Pick

$$\psi = r_1 u + r_2 \varphi \qquad \text{(Note that this works since } \mathrm{Hom}_R(M, R) \text{ is an } R\text{-module).}$$

Then

$$\begin{aligned}\psi(y) &= r_1 u(y) + r_2 \varphi(y) \\ &= r_1 a_1 + r_2 \varphi(y) \\ &= d.\end{aligned}$$

$$\Sigma \ni (a_1) \subset (d) = (\psi(y)) \subset \psi(N) \in \Sigma$$

By maximality,

$$\begin{aligned}(a_1) &= (d) \\ &= \psi(N).\end{aligned}$$

Also, $(\varphi(y)) \subset (d) = (a_1)$. So, $a_1 | \varphi(y)$. □

Write

$$\begin{aligned}y &= \sum x_i^*(y) x_i \\ &= a_1 \sum b_i x_i.\end{aligned}$$

Claim 2: $a_1 | x_i^*(y)$.

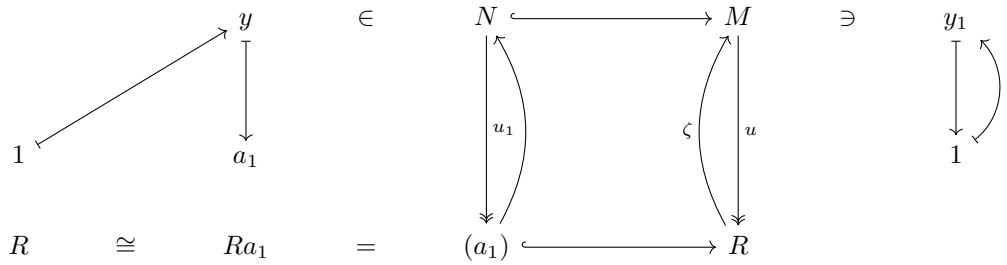
Let

$$\begin{aligned}y_1 &= \frac{y}{a_1} \\ &= \sum b_i x_i.\end{aligned}$$

Claim 3:

$$\begin{aligned}M &\cong R y_1 \oplus \ker(u). \\ N &\cong R y \oplus (N \cap \ker(u)).\end{aligned}$$

Proof.



$$R \xrightarrow{\ \zeta\ } M$$

$$1 \longmapsto y_1$$

Here, ζ is a section.

$$\Rightarrow$$

$$M \cong Ry_1 \oplus \ker(u)$$

$$0 \longrightarrow \ker(u) \hookrightarrow M \twoheadrightarrow R \longrightarrow 0 \quad (\zeta)$$

$$0 \longrightarrow \ker(u_1) \hookrightarrow N \twoheadrightarrow R \longrightarrow 0 \quad (\zeta)$$

$$\Rightarrow$$

$$N \cong Ry \oplus \ker(u_1)$$

$$\begin{aligned} Ra_1 \hookrightarrow R \text{ injection} \Rightarrow \ker(u_1) &= \ker(u|_N) \\ &= \ker(u) \cap N. \end{aligned}$$

Finish proof: Use induction on $\mathrm{rk}(M) = n$.

$$M \cong Ry_1 \oplus \ker(u)$$

Apply theorem to $N \cap \ker(u) \subset \ker(u) \Rightarrow N \cap \ker(u)$ free.

$$\Rightarrow$$

$$N \cong Ry_1 \oplus (N \cap \ker(u))$$

free.

By induction, also have basis $y_2, \ldots, y_n$ of $\ker(u)$ such that $a_2y_2, \ldots, a_ny_n$ is a basis of $N \cap \ker(u)$.

$$\Rightarrow$$

$$M \cong Ry_1 \oplus (Ry_2 \oplus \cdots \oplus Ry_n)$$

free.

$$N \cong Ry \oplus (Ra_2y_2 \oplus \cdots \oplus Ra_ny_n)$$

free.

Exc : Remains to prove that

$$a_1|a_2|a_3|\ldots|a_n.$$

□

7.3 Noetherian modules & rings

Assume R is commutative.

Definition 7.3.1. An R-module M is **noetherian** (Emmy Noether) if the ascending chain condition (ACC) for submodules of M holds, that is, every asc. chain

$$M_1 \subset M_2 \subset M_3 \subset \dots$$

for submodules M_i stabilizes; $\exists n \in \mathbb{N}$ such that $M_{n+k} = M_n$ for $k \in \mathbb{N}$.

Theorem 7.3.2. *TFAE:*

1. *M is noetherian*
2. *Every submodule of M is finitely generated.*

(1) $\Rightarrow$ (2). Let $N \subset M$ and pick $x_1, x_2, \dots$ as generators of N.

$$\Rightarrow$$

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset \dots$$

aschending chain of N is also aschending chain of M, hence it stabilizes, i.e. we find that there exists an $n \in \mathbb{N}$ such that

$$N = \langle x_1, \dots, x_n \rangle.$$

□

(2) $\Rightarrow$ (1). Given chain

$$M_1 \subset M_2 \subset \dots \Rightarrow \bigcup M_i = N$$

which is a submodule of M, hence finitely generated by $x_1, \dots, x_n \in N = \bigcup M_i$, hence exists $a \in \mathbb{N}$ such that $x_1, \dots, x_n \in M_a \Rightarrow N = M_a$ □

Chapter 8

Eight lecture

8.1 Fields

Definition 8.1.1. Fields are integral domains such that $0 \neq 1$ and *every* non-zero element is invertible $\Leftrightarrow$ rings with exactly 2 ideals: Trivial ideal (0) and improper ideal (1).

Lemma 8.1.2. *If $\varphi : \mathbb{F} \longrightarrow k$ is a homomorphism of fields, then φ is* injective*, since we require*

$$\varphi(1_{\mathbb{F}}) = 1_k.$$

Proof. $\ker(f)$ is an ideal of $\mathbb{F}$, if $\mathbb{F}$ is a field then it is (0) or (1), but $\varphi(1_{\mathbb{F}}) \neq 0$ so it must be (0), hence φ is injective. □

8.2 Prime Field

Definition 8.2.1. The **prime field** of $\mathbb{F}$ is the *smallest* subfield of $\mathbb{F}$. This is exactly $\mathrm{Frac}(\mathrm{Im}(\mathbb{Z} \to \mathbb{F}))$ which is easy to see:

$$\mathrm{Frac}(\mathrm{Im}(\mathbb{Z} \to \mathbb{F})) \subset \mathbb{F}$$

so that $1 \longmapsto 1$.

Definition 8.2.2. The **characteristic** of $\mathbb{F}$ is the smallest $n \in \mathbb{N}$ such that $n \cdot 1 = 0$ or $n = 0$ if no such n exists.

$$\ker(\mathbb{Z} \to \mathbb{F}) = (n)$$
$$1 \longmapsto 1$$

where $n = \mathrm{char}(\mathbb{F})$. If $\mathrm{char}(\mathbb{F}) = 0$ then $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{F}$ with $\mathbb{Q}$ prime-field. If $\mathrm{char}(\mathbb{F}) = p > 0$ then

$$\mathbb{Z}/p\mathbb{Z} \subset \mathbb{F} \Rightarrow p \text{ prime} \Rightarrow \mathbb{Z}/p\mathbb{Z} \text{ field} := \mathbb{F}_p.$$

- $\mathbb{F}_p(t)$ infinite field of characteristic p.

- $\mathbb{F}_p$ finite field of characteristic p.
- $\mathbb{R}$ field of characteristic 0.

8.3 Field Extensions

$$\mathbb{F} \hookrightarrow k$$

written as $k/\mathbb{F}$. k is an $\mathbb{F}$-vector space.

Definition 8.3.1. The **degree** of $k/\mathbb{F}$ is

$$[k : \mathbb{F}] = \dim_{\mathbb{F}}(k)$$

Example 8.3.2.

$$[\mathbb{C} : \mathbb{R}] = 2$$

Example 8.3.3.

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

Definition 8.3.4. If $\mathbb{F}$ is a field-extension and $\alpha_1, \ldots, \alpha_n \in k$ then $\mathbb{F}(\alpha_1, \ldots, \alpha_n) \subset k$. Subfield (smallest) containing $\mathbb{F}$ and $\alpha_1, \ldots, \alpha_n$

$$\mathbb{F}(\alpha_1, \ldots, \alpha_n) = \mathrm{Frac}(\mathrm{Im}(\underbrace{\mathbb{F}[x_1, \ldots, x_n] \hookrightarrow k}_{x_i \longmapsto \alpha_i}))$$

where $\mathrm{Im}(\mathbb{F}[x_1, \ldots, x_n] \hookrightarrow k)$ is the smallest subring containing $\mathbb{F}$ and $\alpha_1, \ldots, \alpha_n$.

Definition 8.3.5. A field extension $k/\mathbb{F}$ is **simple** if $k = \mathbb{F}(\alpha)$ for some $\alpha \in k$.

Definition 8.3.6. If $k = \mathbb{F}(\alpha)$ for a simple field extension $k/\mathbb{F}$, as in 8.3.5, then we call α a **primitive** element.

Example 8.3.7. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is actually simple.

Fact: $[k : \mathbb{F}] < \infty$ and $\mathrm{char}(\mathbb{F}) = 0 \Rightarrow k/\mathbb{F}$ simple.

If $|\mathbb{F}| = a$ and we have $k/\mathbb{F}$ then $|k| = a^d$ where $d = [k : \mathbb{F}]$

8.4 Simple Extensions

Theorem 8.4.1. *Let $\mathbb{F}$ be a field, and $p(x) \in \mathbb{F}[x]$. Then there exists a field extension $k/\mathbb{F}$ such that $p(x)$ has a root in k.*

More precisely, if $p(x)$ is an irreducible polynomial then we can take

$$\mathbb{F} \hookrightarrow \mathbb{F}[x] \twoheadrightarrow k = \mathbb{F}[x]/(p(x))$$

Proof. We can assume $p(x)$ is irreducible. We need to prove that $p(x)$ has a root in k. We have that

$$p(\theta) = 0 \tag{8.1}$$

by construction, i.e. by mapping

$$x \longmapsto \overline{x} := \theta \tag{8.2}$$

□

Theorem 8.4.2. *Let $\mathbb{F}$ be a field and $p(x) \in \mathbb{F}[x]$ be irreducible, then $\mathbb{F}[x]/(p(x))$ has basis $1, \theta, \theta^2, \ldots, \theta^{d-1}$ where $d = \deg(p(x))$.*

In part,

$$[k : \mathbb{F}] = d \text{ and } k = \mathbb{F}(\theta).$$

Proof. k generated as a vector-space by $1, \theta, \theta^2, \ldots$. If

$$\begin{aligned} p(x) &= a_d x^d + \ldots + a_1 x^1 + a_0 \qquad (a_d \neq 0) \\ \Rightarrow \theta^d &= -\frac{a_{d-1}}{a_d}\theta^{d-1} - \ldots - \frac{a_0}{a_d} \\ \Rightarrow \theta^{d+k} &\subset \langle \theta^{d+k-1}, \ldots, \theta^k \rangle \subset \langle \theta^{d+k-2}, \ldots, \theta^{k-1} \rangle \subset \ldots \subset \langle \theta^{d-1}, \ldots, 1 \rangle \end{aligned}$$

□

8.5 Linearly independent

Suppose

$$b_i \theta^i + \ldots + b_0 = 0. \tag{8.3}$$

Let

$$q(x) = b_i x^i + \ldots + b_0 \in \mathbb{F}[x]$$

then

$$\begin{aligned} q(x) \in \ker(\mathbb{F}[x] \longrightarrow k) &= (p(x)) \\ \Rightarrow q(x) &= p(x)t(x) \\ \Rightarrow \deg(q) > d \text{ or } q &= 0. \end{aligned}$$

Example 8.5.1. Fix $\mathbb{F} = \mathbb{Q}$, and let $p(x) = x^3 - 2$. Then

$$\begin{aligned} k &= \mathbb{Q}[x]/(x^3 - 2) \\ &\cong \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}. \end{aligned}$$

where $[k : \mathbb{Q}] = 3$ with basis $1, \theta, \theta^2 = 1, \sqrt[3]{2}, \sqrt[3]{4}$.

Theorem 8.5.2 (6)**.** *Let $k/\mathbb{F}$ be a field extension and let $\alpha \in k$. Suppose there exists an irreducible polynomial $p(x)$ s.t. $p(\alpha) = 0$. Then*

$$\mathbb{F}(\alpha) \cong \mathbb{F}[x]/(p(x)).$$

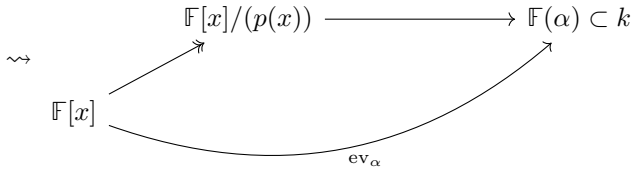
Proof. Start with

$$\mathbb{F} \xrightarrow{\text{ev}_\alpha} k \qquad \text{(evaluation in } \alpha\text{)}$$

$$x \longmapsto \alpha$$

$$f(x) \longrightarrow f(\alpha)$$

so that $p(\alpha) = 0 \Rightarrow p(\alpha) \in \ker(\text{ev}_\alpha)$ and $\text{Im}(\text{ev}_\alpha) \subset \mathbb{F}(\alpha)$



and $\mathbb{F}[x]/(p(x))$ is a field $\Rightarrow \mathbb{F}[x]/(p(x)) \longrightarrow \mathbb{F}(\alpha)$ injective.

$\Rightarrow$ isomorphism since $\mathbb{F}(\alpha)$ is the smallest field containing α. □

Theorem 8.5.3. *If*

(a) $p(\alpha) = 0$ *for some* $p(x) \in \mathbb{F}[x]$.

(b) If $p(x) = p_1(x) \cdots p_n(x)$ ***not*** *irreducible*

Then

$$\begin{aligned} p(\alpha) &= p_1(\alpha) \cdots p_n(\alpha) \\ &= 0 \\ \Rightarrow p_i(\alpha) &= 0 \qquad (\textit{for some } i \in \{1, \ldots, n\}). \end{aligned}$$

2 cases:

1. $p(\alpha) = 0$ for some polynomial (WLOG thm 6 applies).
2. $p(\alpha) \neq 0$ for some polynomial.

Definition 8.5.4. $\alpha \in k$ **algebraic** over $\mathbb{F}$ if there is a polynomial $p(x) \in \mathbb{F}[x]$ such that $p(\alpha) = 0$.

Definition 8.5.5. If $\alpha \in k$ is such that there is no polynomial $p(x) \in \mathbb{F}[x]$ such that $p(\alpha) = 0$, so that α is not algebraic (8.5.4), then we say that α is **transcendental** over $\mathbb{F}$.

Example 8.5.6.

$$\mathbb{Q} \subset \mathbb{R} \ni \sqrt{2}.$$

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \xrightarrow{\cong} & \mathbb{Q}[x]/(x^2-2) \qquad \text{basis } 1, \sqrt{2} \\ \| & & \| \\ \mathbb{Q}(-\sqrt{2}) & \xrightarrow{\cong} & \mathbb{Q}[x]/(x^2-2) \end{array}$$

but this does not commute, so we would need

$$\mathbb{Q}(\sqrt{2}) \xrightarrow{\cong} \mathbb{Q}(-\sqrt{2})$$

$$\sqrt{2} \longmapsto -\sqrt{2}$$

which makes it commute.

Example 8.5.7.

$$\mathbb{Q} \subset \mathbb{C}.$$

with $\alpha = \sqrt[3]{2}$ where $p(x) = x^3 - 2$ irreducible, where $p(\alpha) = 0$.

$$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3-2) \qquad (\text{basis } 1, \theta, \theta^2)$$

but we also have cube roots of unity

$$\xi = e^{\frac{2\pi i}{3}} \tag{8.4}$$

$$\xi^2 = e^{\frac{4\pi i}{3}} \tag{8.5}$$

such that $\mathbb{Q}(\xi\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3-2)$ and $\mathbb{Q}(\xi^2\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3-2)$, but these are *not* equal!

3 *distinct embeddings* $K \hookrightarrow \mathbb{C}$ *with*

$$K = \mathbb{Q}[x]/(x^3-2)$$

("Recent" Galois theory $\mathrm{Aut}(K) = \{1_K\}$*).*

$$x^3 - 2 = (x-\theta)(x^2 + \theta x + \theta^2) \in K[x].$$

Example 8.5.8.

$$\mathbb{Q}(\sqrt[3]{2}, \xi\sqrt[3]{2}) = \underbrace{K[y]/(y^2+y+1)}_{:=\mathcal{L}}$$

where $\theta = \overline{x}$, $\alpha = \overline{y}$.

$$\mathbb{Q}(\xi) = \mathbb{Q}[x]/(x^2+x+1)$$

with basis

$$1, \theta, \theta^2, \alpha, \alpha\theta, \alpha\theta^2$$

of degree 6.

Exc: 6 different embeddings $\mathcal{L} \to \mathbb{C}$ but all have same image

$$|\operatorname{Aut}(\mathcal{L})| = 6.$$

$\mathcal{L}$ **splitting field** of $x^3 - 2$.

Example 8.5.9. $\mathbb{F} = \mathbb{F}_2$ where $p(x) \in \mathbb{F}_2[x]$ irreducible.

$$p(x) = x^2 + x + 1$$

has no roots and degree $\leq 3 \Rightarrow$ irreducible.

$$k = \mathbb{F}_2[x]/(p(x)) \qquad (\text{basis } 1, \theta).$$

$$x^2 + x + 1 = (x - \theta)(x - (\theta + 1))$$

has roots $\theta, \theta + 1$.

8.6 Algebraic extensions

Definition 8.6.1. A field extension $k/\mathbb{F}$ is **algebraic** if $\forall \alpha \in k$ are algebraic. Otherwise $k/\mathbb{F}$ is **transcendental**.

Example 8.6.2.

$$\mathbb{Q} \subset \mathbb{Q}(t) \supset \mathbb{Q}[t] \qquad (\text{t is not algebraic} \in \mathbb{Q}).$$

Example 8.6.3.

$$\mathbb{Q} \subset \mathbb{Q}(t) \subset \mathbb{Q}(\sqrt{t})$$

where $\sqrt{t}$ is algebraic over $\mathbb{Q}(\sqrt{t})$ (take $p(x) = x^2 - t$) but not algebraic over $\mathbb{Q}$.

Proposition 8.6.4. *If $\alpha \in k$ is algebraic over $\mathbb{F}$, then there exists a unique monic irreducible polynomial $m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}[x]$ such that $m_{\alpha,\mathbb{F}}(\alpha) = 0$. Also, if $p(\alpha) = 0$ for $p(x) \in \mathbb{F}[x]$, then $m_{\alpha,\mathbb{F}}(x) \mid p(x)$.*

Proof.

$$\mathbb{F}[x] \xrightarrow{\text{ev}_\alpha} k$$

$$x \longmapsto \alpha$$

where

$$\ker(\text{ev}_\alpha) = (m_{\alpha,\mathbb{F}}(x)).$$

□

Definition 8.6.5. $m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}[x]$ in 8.6.4 is called the **minimal polynomial for α over $\mathbb{F}$**.

Definition 8.6.6. Let $\alpha \in k$ be algebraic over $\mathbb{F}$, and let $m_{\alpha,\mathbb{F}}(x)$ be as in 8.6.5. Then

$$\begin{aligned} \deg(\alpha) &= [\mathbb{F}(\alpha) : \mathbb{F}] \\ &= \deg\left(m_{\alpha,\mathbb{F}}(x)\right) \end{aligned}$$

is called the **degree of α**.

Proposition 8.6.7. *α algebraic $\Leftrightarrow [\mathbb{F}(\alpha) : \mathbb{F}] < \infty$.*

Proof sketch.

$$\ker(\text{ev}_\alpha) = (m_{\alpha,\mathbb{F}}(x)) \text{ or } = (0).$$

□

Corollary 8.6.8. *If for all $\alpha \in k$ we have $[\mathbb{F}(\alpha) : \mathbb{F}] < \infty \Rightarrow k/\mathbb{F}$ algebraic.*

Proof. Pick any $\alpha \in k$, then $\mathbb{F} \subset \mathbb{F}(\alpha) \subset k \rightsquigarrow [\mathbb{F}(\alpha) : \mathbb{F}] < \infty \underbrace{\Rightarrow}_{8.6.7} \alpha$ algebraic. Since $\alpha \in k$ was arbitrary, we find that k is an algebraic field extension. □

Definition 8.6.9. A field extension $k/\mathbb{F}$ is **finitely generated** if there are $\alpha_1, \ldots, \alpha_n \in k$ such that $k = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$.

Theorem 8.6.10. *A field extension $k/\mathbb{F}$ is **algebraic** and **finitely generated** $\Leftrightarrow [k : \mathbb{F}] < \infty$.*

Proof.

$$\mathbb{F} \subset \mathbb{F}(\alpha_1) \subset \underbrace{\mathbb{F}(\alpha_1, \alpha_2)}_{=\mathbb{F}(\alpha_1)\mathbb{F}(\alpha_2)} \subset \cdots \subset \mathbb{F}(\alpha_1, \ldots, \alpha_n) = k.$$

$$\underbrace{\Rightarrow}_{8.6.7} \underbrace{[\mathbb{F}(\alpha_1, \ldots, \alpha_i) : \mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})]}_{=\deg\left(m_{\alpha_i, \mathbb{F}_{i-1}}(x)\right)} < \infty$$

where

$$\mathbb{F}_{i-1} = \mathbb{F}(\alpha_1, \ldots, \alpha_{i-1}).$$

So k is finite dimensional over $\mathbb{F}$.

8.6.8 says that k is algebraic.

$$[k : \mathbb{F}] < \infty \Rightarrow k = \langle \alpha_1, \ldots, \alpha_n \rangle$$

as $\mathbb{F}$-vector space. This implies that

$$k = \mathbb{F}(\alpha_1, \ldots, \alpha_n). \tag{8.6}$$

□

Example 8.6.11.

$$\mathbb{Q} \underbrace{\subset}_{\deg\ 3} \mathbb{Q}(\sqrt[3]{2}) \underbrace{\subset}_{\deg\ 2} \mathbb{Q}(\sqrt[3]{2}, \xi\sqrt[3]{2})$$

so total degree 6, which implies that $\mathbb{Q}\left(\sqrt[3]{2}, \xi\sqrt[3]{2}\right)$ is *algebraic*! For example, $\sqrt[3]{2}+2\xi\sqrt[3]{2} \in \mathbb{Q}\left(\sqrt[3]{2}, \xi\sqrt[3]{2}\right)$ is then algebraic so is the *root* of some polynomial $m(x) \in \mathbb{Q}[x]$.

Chapter 9

Ninth lecture

- More on algebraic extensions
- Straighedge + Compass construction
- Splitting fields

9.1 Algebraic Extensions

Let $k/\mathbb{F}$ be a field-extension.

Remark 9.1.1. Note that we most often suppress $/\mathbb{F}$ in $k/\mathbb{F}$ and just write k.

- Recall that $\alpha \in k$ is *algebraic* (8.5.4) if there exists some $p(x) \in \mathbb{F}[x]$ such that $p(\alpha) = 0$.
- Otherwise $\alpha \in k$ is *transcendental* (8.5.5).

$$\mathbb{F}[x] \xmapsto{\text{ev}_\alpha} k$$

$$x \longmapsto \alpha$$

$$f(x) \longmapsto f(\alpha)$$

α *algebraic* $\Leftrightarrow m_{\alpha,\mathbb{F}}(x)$ *irreducible* and *monic*.

α **transcendental** $\Leftrightarrow m_{\alpha,\mathbb{F}}(x) = 0$. If α is algebraic then

$$\begin{aligned}\deg(\alpha) &= \deg(m_{\alpha,\mathbb{F}}(x)) \\ &= [\mathbb{F}(\alpha) : \mathbb{F}].\end{aligned}$$

Theorem 9.1.2 (14)**.** *Let* $\mathbb{L}/k$ *and* $k/\mathbb{F}$ *be* field extensions. Then

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : k][k : \mathbb{F}].$$

Proof. Note: Nothing to prove if one is infinite.

k has basis $\alpha_1, \ldots, \alpha_n$ over $\mathbb{F}$ (as an $\mathbb{F}$-vector space). $\mathbb{L}$ has basis $\beta_1, \ldots, \beta_m$ over k. This implies that $\mathbb{L}$ has basis

$$\{\alpha_i \beta_j\}_{j=1,\ldots,m}^{i=1,\ldots,n}$$

over $\mathbb{F}$. Prove $\{\alpha_i \beta_j\}$ **spans** $\mathbb{L}$ as an $\mathbb{F}$-vector space, and is an $\mathbb{F}$-linearly independent set. □

Theorem 9.1.3. *Let $k/\mathbb{F}$ be a field extension. Then*

$$[k : \mathbb{F}] \text{ finite} \Leftrightarrow k/\mathbb{F} \text{ finitely generated and algebraic.}$$

(see 8.6.10 for proof).

Corollary 9.1.4. *If α, β are algebraic over $\mathbb{F}$, then $\alpha + \beta$, $\alpha - \beta$,$\alpha \cdot \beta$ and*

$$\frac{\alpha}{\beta} \quad (\beta \neq 0)$$

are all algebraic.

9.1.4 in turn implies the following corollary.

Corollary 9.1.5 (19)**.** *Algebraic elements of k constitute a* subfield of k - the algebraic closure of $\mathbb{F}$ in k.

Proof. We prove 9.1.4.

We have $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{F}(\alpha, \beta)$. Now if $[\mathbb{F}(\alpha, \beta) : \mathbb{F}]$ is finite $\overset{9.1.3}{\Rightarrow}$ $\mathbb{F}(\alpha, \beta)$ **algebraic**.

Then we see that

$$\begin{aligned} [\mathbb{F}(\alpha) : \mathbb{F}] &= \deg(m_{\alpha,\mathbb{F}}(x)) < \infty \\ [\mathbb{F}(\alpha, \beta) : \mathbb{F}(\alpha)] &= \deg(m_{\beta,\mathbb{F}(\alpha)}(x)) \leq \deg(m_{\beta,\mathbb{F}}(x)) < \infty \\ \Rightarrow [\mathbb{F}(\alpha, \beta) : \mathbb{F}] &= [\mathbb{F}(\alpha, \beta) : \mathbb{F}(\alpha)][\mathbb{F}(\alpha) : \mathbb{F}] < \infty \end{aligned}$$

so since $\mathbb{F}(\alpha, \beta)$ finite, $\mathbb{F}(\alpha, \beta)$ is algebraic, hence every element in $\mathbb{F}(\alpha, \beta)$ is algebraic, and $\alpha + \beta, \alpha - \beta, \alpha\beta$ as well as

$$\frac{\alpha}{\beta} \qquad (\beta \neq 0)$$

are in $\mathbb{F}(\alpha, \beta)$, hence *algebraic*. □

Remark 9.1.6. Fix $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and note that

$$\begin{aligned} m_{\sqrt{2},\mathbb{Q}}(x) &= x^2 - 2 \\ m_{\sqrt{3},\mathbb{Q}}(x) &= x^2 - 3 \\ \Rightarrow \underbrace{\sqrt{2} + \sqrt{3}}_{=\gamma} &\text{ algebraic} \end{aligned}$$

then $1, \gamma, \gamma^2, \gamma^3, \gamma^4$ linearly independent

$$\Rightarrow [\mathbb{Q}(\gamma) : \mathbb{Q}] \geq 4$$
$$\mathbb{Q}(\gamma) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$\Rightarrow \mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

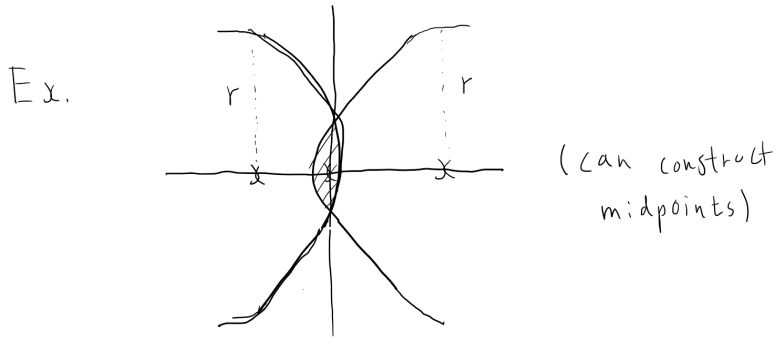
$$\Rightarrow 1, \gamma, \gamma^2, \gamma^3, \gamma^4 \text{ linearly independent}$$
$$\Rightarrow \gamma^4 + a_3\gamma^3 + a_2\gamma^2 + a_1\gamma + a_0 = 0$$
$$\Rightarrow m_{\gamma,\mathbb{Q}}(x) = x^4 + a_3x^3 + \ldots + a_1x + a_0.$$

9.2 Geometric constructions

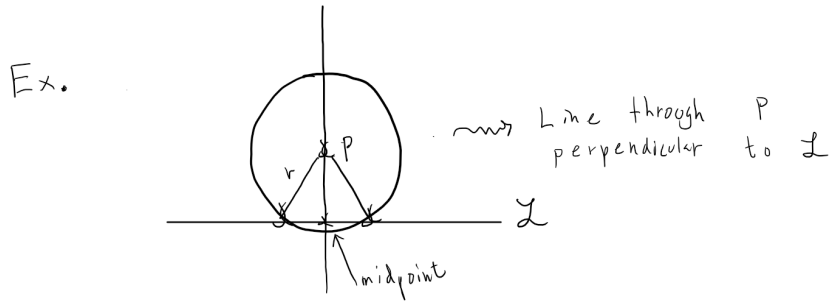
Definition 9.2.1 (Straightedge and Compass)**.**

Straightedge - Can draw line between 2 points.

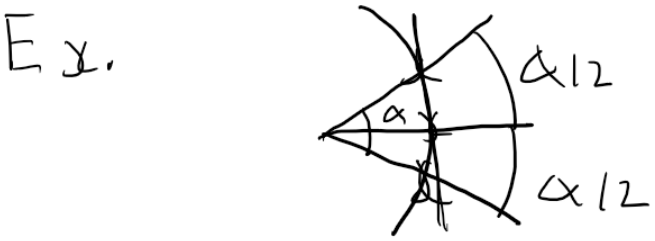
Compass - Can draw circle with center a given point and radius distance between two points.



Example 9.2.2.



Example 9.2.3.



Example 9.2.4.

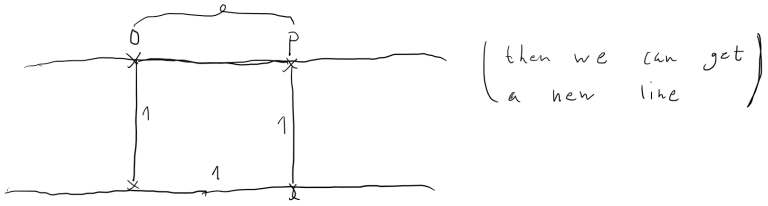
Question 9.2.5. ca 400 B.C.

(a) Trisect *any* angle.

(b) Double an arbitrary cube.

(c) Square a circle.

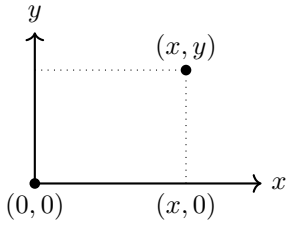
9.3 Constructible numbers



$\mathbb{L} = \{\text{all } \textit{lengths} \text{ that can be constructed from straightedge and compass operations}\}$

Lemma 9.3.1. $(x, y) \in \mathbb{R}^2$ ***constructible*** *point* $\Leftrightarrow x, y \in \mathbb{L}$.

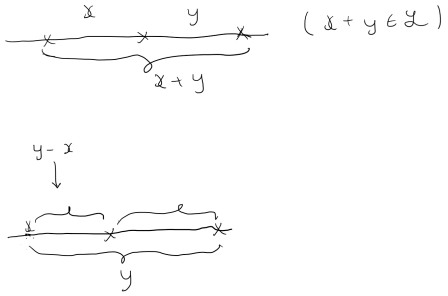
Proof.



$(x, y) \rightsquigarrow (x, 0), (0, y)$ lengths x & y.

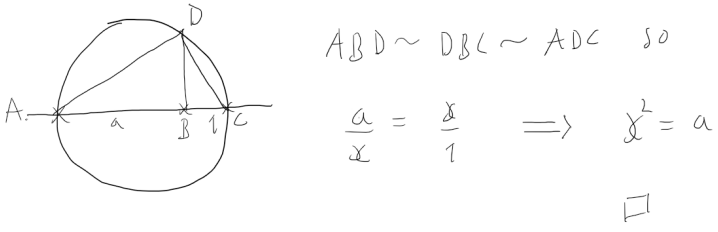
(This construction is the line through P perpendicular to $\mathbb{L}$ from example 9.2.3) □

Lemma 9.3.2. $\mathbb{L}$ *is a field.*



Proof. □

Lemma 9.3.3. *If* $\alpha \in \mathbb{L} \Rightarrow \sqrt{\alpha} \in \mathbb{L}$.



Proof. □

Question 9.3.4. ($\sim$ 400 B.C)

For which n can a **regular** n-polygon be *constructed*?

Greeks: $n = 3, 4, 5$.

Gauss (1796): $n = 17$.

Theorem 9.3.5 (Gauss-Wantzel, 1837)**.** *Possible* $\Leftrightarrow n = 2^k \cdot p$ (p *fermat prime*).

Definition 9.3.6. A **fermat prime** is a number on the form

$$2^{2^k} + 1 \qquad (k \geq 0)$$

that is also a prime.

Definition 9.3.7. Let $\tilde{\mathbb{L}}/\mathbb{Q}$ be the **field-extension** obtained by iteratively extracting square roots of positive real numbers in the field.

$$F_0 = \mathbb{Q}$$
$$F_i = F_{i-1}(\{\sqrt{a} \mid a \in F_{i-1}, a \geq 0\})$$

$$F_0 \subset F_1 \subset \ldots \subset \tilde{\mathbb{L}} = \bigcup_{i \geq 0} F_i \subset \mathbb{R}$$
$$\Leftrightarrow \tilde{\mathbb{L}} = \{\alpha \in \mathbb{R} \mid \exists \mathbb{Q} \subset \mathbb{Q}(\sqrt{a}_1) \subset \mathbb{Q}(\sqrt{a}_1)(\sqrt{a}_2) \subset \ldots \subset \mathbb{Q}(\sqrt{a}_1)\ldots(\sqrt{a}_n) \ni \alpha\}$$

Remark 9.3.8. $a \in \tilde{\mathbb{L}} \Rightarrow \sqrt{a} \in \tilde{\mathbb{L}}$ given $a \geq 0$.

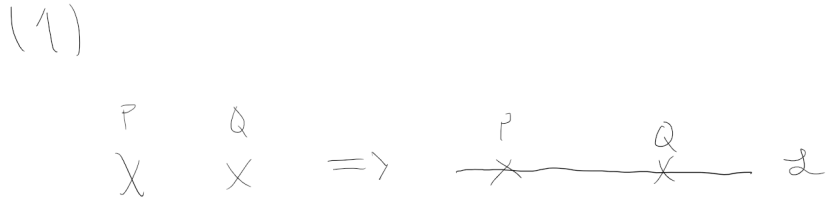
Theorem 9.3.9.

$$\mathbb{L} = \tilde{\mathbb{L}}$$

Proof. Have already seen

$$\tilde{\mathbb{L}} \subset \mathbb{L}.$$

For converse: Need to prove; given points with coordinates in $\tilde{\mathbb{L}}$, *any* construction of these give coordinates in $\tilde{\mathbb{L}}$.

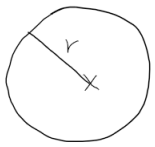


$$P = (x_1, y_1) \in \tilde{\mathbb{L}}^2$$
$$Q = (x_2, y_2) \in \tilde{\mathbb{L}}^2$$

Then the equation for $\mathbb{L}$ is $ax + by = c$. Solving for P and $Q \Rightarrow$ solution with $a, b, c \in \tilde{\mathbb{L}}$.

(2) point + distance

$(x_0, y_0) \in \tilde{\mathcal{L}}^2$, $r \in \tilde{\mathcal{L}} \Rightarrow$



$(x - x_0)^2 + (y - y_0)^2 = r^2$

has coefficients in $\tilde{\mathcal{L}}$

3. 2 lines $\Rightarrow$ intersection points

$$\begin{cases} ax + by = c \\ dx + ey = f \end{cases} \Rightarrow x, y \in \tilde{\mathbb{L}}$$

given that $a, b, c, d, e, f \in \tilde{\mathbb{L}}$.

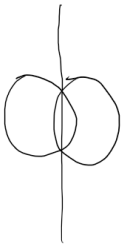
4. $$\begin{cases} \text{cons line} \\ \text{cons circle} \end{cases} \Rightarrow \leq \text{ 2 intersection points (solid quadratic equation in } \tilde{\mathbb{L}}).$$

5. 2 conic circles $\Rightarrow$ 1 common secant line

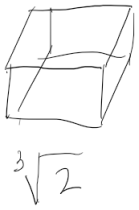
$$(x - x_i)^2 + (y - y_i)^2 = r_i^2 \qquad (\text{for } i \in \{1, 2\}).$$

equation 1 $-$ equation 2 has constructible coefficients.

□



Theorem 9.3.10. *(a),(b),(c) not constructible with straightedge and compass.*



(b).

$$\sqrt[3]{2} \notin \tilde{\mathbb{L}} = \mathbb{L}$$

$$\begin{aligned} \deg(\sqrt[3]{2}) &= \deg\left(m_{\sqrt[3]{2},\mathbb{Q}}(x)\right) \\ &= \deg(x^3 - 2) \\ &= 3 \\ &\neq 2^k \qquad (k \in \mathbb{N}). \end{aligned}$$

□

Lemma 9.3.11. *If $\alpha \in \tilde{\mathbb{L}} = \mathbb{L}$ then $\deg(\alpha) = 2^n$.*

Proof.

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{a_1}) \subset \mathbb{Q}(\sqrt{a_1})(\sqrt{a_2}) \subset \ldots \subset \underbrace{\mathbb{Q}(\sqrt{a_1})\ldots(\sqrt{a_n})}_{\mathbb{Q}(\alpha) \text{ subset of above}}$$

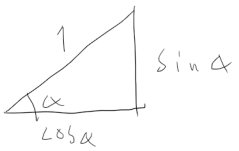
so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$.

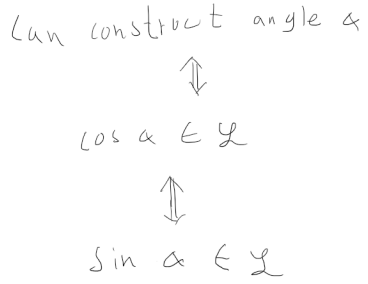
(c):

Need $\sqrt{\pi} \in \mathbb{L} \Leftrightarrow \pi \in \mathbb{L}$.

Theorem (Lindemann, 1887) gives us that π is **transcendental** $\Rightarrow$ π **not algebraic** so not in $\mathbb{L}$.

(a):





So given α such that $\cos\alpha \in \mathbb{L}$, is $\cos\left(\frac{\alpha}{3}\right) \in \mathbb{L}$?

We note that

$$\begin{aligned}
\cos(3\theta) &= \cos(\theta + 2\theta) \\
&= \cos(\theta)(\cos(2\theta)) - \sin(\theta)\sin(2\theta) \\
&= \cos(\theta)(\cos^2(\theta) - \sin^2(\theta)) - \sin(\theta)(2\sin(\theta)\cos(\theta)) \\
&= \cos^3(\theta) - \cos(\theta)\sin^2(\theta) - 2\sin^2(\theta)\cos(\theta) \\
&= \cos^2(\theta) - 3\cos(\theta)\sin^2(\theta) \\
&= \cos^3(\theta) - 3\cos(\theta)(1 - \cos^2(\theta)) \\
&= \cos^3(\theta) - 3\cos(\theta) + 3\cos^3(\theta) \\
&= 4\cos^3(\theta) - 3\cos(\theta).
\end{aligned}$$

We set $\theta = \frac{\alpha}{3}$ and get

$$\begin{aligned}
&\cos\alpha = 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3} \\
\Leftrightarrow\ &0 = 4\cos^3\left(\frac{\alpha}{3}\right) - 3\cos\left(\frac{\alpha}{3}\right) - \beta
\end{aligned}$$

where $\beta = \cos\alpha$. Finally we set $x = \cos\left(\frac{\alpha}{3}\right)$ and get $4x^3 - 3x - \beta = 0$. So given $\beta = \cos\alpha \in \mathbb{L} \cap [-1, 1]$ does $4x^3 - 3x - \beta$ have a root in $\mathbb{L}$? Let

$$\alpha = 90°, \beta = 0. \tag{9.1}$$

Then

$$4x^3 - 3x = x(2x - \sqrt{\cdots})(2x - \sqrt{\cdots}).$$

No for some α, e.g. $\alpha = 60°, \beta = \frac{1}{2}$ then

$$\begin{aligned}
&4x^3 - 3x - \frac{1}{2} = 0 \\
\Leftrightarrow\ &8x^3 - 6x - 1 = 0.
\end{aligned}$$

Note that if it was reducible over $\mathbb{Q}$ then it has a rational root. But by the rational root theorem, it root´s has to be $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$. I believe one finds that none of these are roots, hence $8x^3 - 6x - 1$ must be irreducible over $\mathbb{Q}$.

$$\begin{aligned} \deg_{\mathbb{Q}} \left(\cos \frac{\alpha}{3} \right) &= 3 \\ &\neq 2^k \\ \Rightarrow \cos \frac{\alpha}{3} &\notin \mathbb{L}. \end{aligned}$$

□

9.4 Splitting fields

Definition 9.4.1. Let $\mathbb{F}$ be a field. A polynomial $p(x) \in \mathbb{F}[x]$ **splits completely** if it factors in linear factors.

Definition 9.4.2. A **splitting field** of $p(x) \in \mathbb{F}[x]$ is a field extension $k/\mathbb{F}$ such that

(a) $p(x) \in k[x]$ splits completely

(b) $p(x) \in \mathbb{L}[x]$ does not split completely, if $\mathbb{L}$ is an *intermediate extension*, i.e. $\mathbb{F} \subset \mathbb{L} \subsetneq k$

$(a), (b)$ above are *equivalent* to:

(a') $p(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in k[x]$.

(b') $k = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$

Theorem 9.4.3. *Splitting fields always exists and are unique (up to non-unique isomorphism).*

Chapter 10

Tenth lecture

Let $\mathbb{F}$ be a field, and

$$p(x) = a_0 + a_1 x + \dots a_{n-1}x^{n-1} + a_n x^n \in \mathbb{F}[x] \qquad (n > 0)$$

Definition 10.0.1. $p(x)$ **splits completely** over $\mathbb{F}$ if there exists $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ such that

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

Theorem 10.0.2. *Let $\mathbb{F}$ and $p(x)$ as above. Then there $\exists$ **field extension** $\mathbb{E}/\mathbb{F}$ such that $p(x)$ **splits completely** over $\mathbb{E}$.*

Proof.

(1). If $p(x)$ splits completely over $\mathbb{F}$, then $\mathbb{E} = \mathbb{F}$.

(2). If $\deg(p(x)) = 1$ then $p(x) = x - a$ with $a \in \mathbb{F}$ so $\mathbb{E} = \mathbb{F}$.

Let $n \geq 2$ and suppose the theorem holds for all polynomials of degree $< n$, over all fields. Suppose

$$\deg(p(x)) = n. \tag{10.1}$$

If $p(x)$ does not split completely then it has an irreducible factor of degree > 1. Let's say

$$p(x) = p_1(x)q(x) \tag{10.2}$$

where $p_1(x)$ is irreducible of degree > 1. There exists a field extension $\mathbb{E}_1/\mathbb{F}$ such that $p_1(x)$ has a root α in $\mathbb{E}_1$, namely

$$\mathbb{E}_1 = \mathbb{F}[x]/(p_1(x))$$

over $\mathbb{E}_1$, where

$$\begin{aligned} x \bmod (p(x)) &= \pi(x) \\ &:= \alpha \quad (\pi \text{ being the canonical projection from } \mathbb{F}[x] \text{ to the quotient } \mathbb{F}[x]/(p(x))) \end{aligned}$$

$$\rightsquigarrow p_1(x) = (x-\alpha)p_2(x)$$

for some $p_2(x) \in \mathbb{E}_1[x]$. Therefore, over $\mathbb{E}_1$ we have

$$\begin{aligned} p(x) &= (x-\alpha)p_2(x)q(x) \\ &= (x-\alpha)r(x) \end{aligned}$$

where $\deg(r(x)) = n-1$. By inductive hypothesis there exists a field extension $\mathbb{E}/\mathbb{E}_1$ such that $r(x)$ splits completely over $\mathbb{E}$ so that

$$r(x) = (x-\alpha_2)\cdots(x-\alpha_n) \qquad (a_2,\ldots,\alpha_n \in \mathbb{E}). \tag{10.3}$$

But then $p(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n)$ over $\mathbb{E}$. □

Definition 10.0.3. Let $\mathbb{F}$ and p (shortening for $p(x)$) be as before. A **splitting field** for p over $\mathbb{F}$ is a field extension $\mathbb{E}/\mathbb{F}$ such that

1. p **splits completely** over $\mathbb{E}$
2. For any *proper* intermediate extension $\mathbb{E}_0$, i.e.

$$\mathbb{F} \subset \mathbb{E}_0 \subsetneq \mathbb{E}$$

p does **not** split completely over $\mathbb{E}_0$.

Theorem 10.0.4. *A splitting field **always** exists.*

Proof. Find an extension $\mathbb{E}_1/\mathbb{F}$ so that $p(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ over $\mathbb{E}_1$ (i.e. in $\mathbb{E}_1[x]$). Let

$$\mathbb{E} = \mathbb{F}(\alpha_1,\ldots,\alpha_n) \subset \mathbb{E}_1$$

Then $\mathbb{E}$ is the **minimal subfield** of $\mathbb{E}_1$ containing $\mathbb{F}$ and $\alpha_1,\ldots,\alpha_n \Rightarrow \mathbb{E} = \mathbb{F}(\alpha_1,\ldots,\alpha_n)$ is a splitting field. □

10.1 Uniqueness

Suppose $\sigma : \mathbb{F} \to \mathbb{F}_1$ is a field isomorphism. Then σ induces a ring isomorphism, also denoted σ with

$$\sigma : \mathbb{F}[x] \to \mathbb{F}_1[x]$$

explicitly by

$$\mathbb{F}[x] \ni a_0 + a_1x^1 + \ldots + a_nx^n \longmapsto \sigma(a_0) + \sigma(a_1)x^1 + \ldots + \sigma(a_n)x^n \in \mathbb{F}_1[x]$$

i.e. $p \mapsto \sigma p$ with σ "acting" on polynomials $p \in \mathbb{F}[x]$ as above.

$$p \text{ irreducible in } \mathbb{F}[x] \Leftrightarrow \sigma p \text{ irreducible in } \mathbb{F}_1[x].$$

Lemma 10.1.1. *Suppose $\sigma : \mathbb{F} \to \mathbb{F}_1$ is a field isomorphism and $p \in \mathbb{F}[x]$ is **irreducible**. Let*

$$\mathbb{E}/\mathbb{F}, \mathbb{E}_1/\mathbb{F}_1$$

be field extensions and let $\alpha \in \mathbb{E}$, $\alpha_1 \in \mathbb{E}_1$ be roots of p and σp respectively.

Then there $\exists!$ field isomorphism

$$\overline{\sigma} : \mathbb{F}(\alpha) \to \mathbb{F}_1(\alpha_1)$$

extending σ and sending α to α_1, that is

$$\begin{aligned} &\overline{\sigma}(f) = \sigma(f) \qquad (\forall f \in \mathbb{F}) \\ &\overline{\sigma}(\alpha) = \alpha_1 \end{aligned}$$

Proof. We claim there exists a **unique** field isomorphism

$$\eta : \mathbb{F}[x]/(p(x)) \to \mathbb{F}(a)$$

such that $\eta(x) = \alpha$ and similarly a unique isomorphism η_1 such that

$$\begin{array}{ccc} & \mathbb{F}_1[x]/(\sigma p(x)) \xrightarrow{\cong} \mathbb{F}_1(\alpha_1) & \\ \mathbb{F}[x]/(p) & \xrightarrow[\eta]{\cong} & \mathbb{F}(\alpha) \\ \Big\downarrow{\scriptstyle \sigma}\ {\scriptstyle \cong} & & \Big\downarrow{\scriptstyle \overline{\sigma}} \\ \mathbb{F}_1[x]/(\sigma p) & \xrightarrow[\eta_1]{\cong} & \mathbb{F}_1(\alpha_1) \end{array}$$

$\overline{\sigma}$ is induced from

$$\sigma : \mathbb{F}[x]/(p) \to \mathbb{F}_1[x]/(\sigma p).$$

Similarly define

$$\overline{\sigma} = \eta_1 \circ \sigma \circ \eta^{-1}$$

and isomorphism and uniqueness follows. □

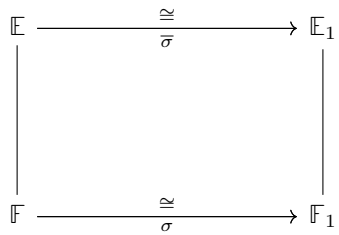
Theorem 10.1.2. *Let*

$$\sigma : \mathbb{F} \to \mathbb{F}_1$$

be an isomorphism of fields. Let $p \in \mathbb{F}[x]$ be a polynomial, and let $\mathbb{E}/\mathbb{F}$, $\mathbb{E}_1/\mathbb{F}_1$ be splitting fields for p and σp over $\mathbb{F}$ and $\mathbb{F}_1$ respectively. Then $\exists$ a field isomorphism

$$\overline{\sigma} : \mathbb{E} \to \mathbb{E}_1$$

extending σ (in particular, any two splitting fields of p over $\mathbb{F}$ are isomorphic).



Proof. If p **splits completely** over $\mathbb{F}$, in particular if p is linear, then $\mathbb{E} = \mathbb{F}$, $\mathbb{E}_1 = \mathbb{F}_1$, and there is nothing to prove.

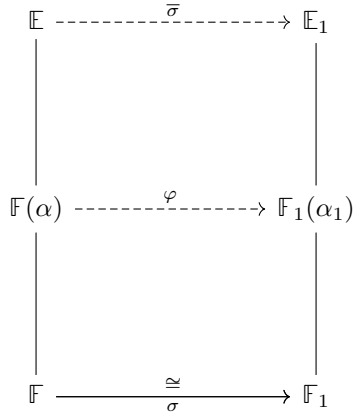
Let $n \geq 2$ and assume the theorem holds for any polynomial of *degree* less than n, over any field.

Let $p \in \mathbb{F}[x]$ be a polynomial of degree n.

We can assume p has an irreducible factor q of degree greater than 1.

Since $\mathbb{E}$ is a splitting field for p, q **splits completely** over $\mathbb{E}$. Let $\alpha \in \mathbb{E}$ be a root of q, similarly, let $\alpha_1 \in \mathbb{E}_1$ be a root of σq.

We have a diagram of fields:



By 10.1.1, there is a (unique) isomorphism

$$\varphi : \mathbb{F}(\alpha) \to \mathbb{F}_1(\alpha_1)$$

extending σ.

Moreover, over $\mathbb{F}(\alpha)$ we have

$$p = (x - \alpha)r(x)$$

where $r(x) \in \mathbb{F}(\alpha)[x]$ of degree $n - 1$ and

$$\sigma p = (x - \alpha_1)\sigma r(x)$$

where $\sigma r(x)$ is a polynomial over $\mathbb{F}_1(\alpha_1)[x]$ of degree $n - 1$.

We claim that $\mathbb{E}$ is a splitting field for $r(x)$ over $\mathbb{F}(\alpha)$. *p splits completely* over $\mathbb{E}$

$$\Rightarrow p(x) = (x - \alpha)r(x)$$

so that $r(x)$ *splits completely* over $\mathbb{E}$.

Moreover, if $r(x)$ splits completely over $\mathbb{E}_0$, where

$$\mathbb{F}(\alpha) \subset \mathbb{E}_0 \subset \mathbb{E}$$

then $p = (x - \alpha)r(x)$ splits completely over $\mathbb{E}_0 \underbrace{\Rightarrow}_{\text{by minimality}} \mathbb{E} = \mathbb{E}_0$.

Similarly, $\mathbb{E}_1$ is a splitting field for σp over $\mathbb{F}_1(\alpha_1)$.

Therefore, by the inductive hypothesis, there is a field isomorphism $\overline{\sigma} : \mathbb{E} \to \mathbb{E}_1$ extending φ, so $\overline{\sigma}$ extends σ. □

10.2 Algebraically closed fields

Definition 10.2.1. A field $\mathbb{F}$ is called **algebraically closed** if every polynomial over $\mathbb{F}$ of deg ≥ 1 has a root (in $\mathbb{F}$), and therefore splits completely.

Theorem 10.2.2. *$\mathbb{C}$ is algebraically closed.*

Definition 10.2.3. Let $\mathbb{F}$ be a field. A field extension

$$\overline{\mathbb{F}}/\mathbb{F}$$

is an **algebraic closure** of $\mathbb{F}$ if

(a) Every polynomial $p(x) \in \mathbb{F}[x]$ *splits completely* over $\overline{\mathbb{F}}$. That is, $p(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in \overline{\mathbb{F}}[x]$ if $\deg(p(x)) = n$, where $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{F}}$.

(b) All $\alpha \in \overline{\mathbb{F}}$ are *algebraic* in $\mathbb{F}$. That is, for all $\alpha \in \overline{\mathbb{F}}$ there exists a non-zero polynomial $p(x) \in \mathbb{F}[x]$ such that $p(\alpha) = 0$.

Lemma 10.2.4. *An algebraic closure (10.2.3) of $\mathbb{F}$ is algebraically closed (10.2.1).*

Proof. Let $\overline{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$. Let $p \in \overline{\mathbb{F}}[x]$. Let $\overline{\mathbb{F}}(\alpha)$ be an extension of $\overline{\mathbb{F}}$ generated by a *root* α of p. $\overline{\mathbb{F}}(\alpha)$ is an *algebraic* extension of $\overline{\mathbb{F}}$, and $\overline{\mathbb{F}}$ is an *algebraic* extension of $\mathbb{F} \Rightarrow \overline{\mathbb{F}}(\alpha)$ is an **algebraic** extension of $\mathbb{F} \Rightarrow \alpha$ is the *root* of some polynomial in $\mathbb{F}[x] \Rightarrow \alpha \in \overline{\mathbb{F}}$. □

Theorem 10.2.5.

1. *Every field has an algebraic closure.*
2. *Every two algebraic closures of* $\mathbb{F}$ *are isomorphic over* $\mathbb{F}$*.*

Proof. Existence:

Assuming $\mathbb{F}$ is *countable* then $\mathbb{F}[x]$ is also *countable*.

Let $f_1, f_2, \ldots$ be all polynomials of degree > 1 over $\mathbb{F}$. Construct a *sequence* of *field extensions*

$$\mathbb{F} = \mathbb{E}_0 \subset \mathbb{E}_1 \subset \mathbb{E}_2 \subset \ldots$$

where $\mathbb{E}_n$ is the splitting field for f_n over $\mathbb{E}_{n-1}$.

Let $\overline{\mathbb{F}} := \bigcup_{n \in \mathbb{N}} \mathbb{E}_n$.

$$\Rightarrow$$

(a) $\overline{\mathbb{F}}$ is a field (routine)

(b) Every element of $\overline{\mathbb{F}}$ over $\mathbb{F}$ is algebraic over $\mathbb{F}$.

(c) Every polynomial splits completely (9.4.1) over $\overline{\mathbb{F}}$.

-

□

Chapter 11

Eleventh lecture

11.1 Field extensions

(i)

$$\text{Galois Extensions (which are } \textbf{algebraic} \text{ field extensions)} = \begin{cases} \text{Seperable} \\ \text{Normal extensions} \end{cases}$$

(ii) **Transcendental** 8.5.5 (purely)

- Transcendental *degree*.

11.2 Separability

Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$ (henceforth p).

Definition 11.2.1. p is **seperable** if p has no *multiple* roots in the splitting field of p (that is, all roots are *distinct*).

Remark 11.2.2. This is equivalent to p *not* having a multiple root over *any* field extension $\mathbb{K}/\mathbb{F}$.

Indeed, if p has a multiple root in $\mathbb{E}$, then p has a multiple root in $\overline{\mathbb{E}}$, the algebraic closure of $\mathbb{E}$. But $\overline{\mathbb{E}}$ contains the splitting field of p over $\mathbb{F}$, which also contains a multiple root.

Example 11.2.3.

1. $x^2 - 2$ is seperable over $\mathbb{Q}$. This is because

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}) \qquad \left(\text{in } \mathbb{Q}(\sqrt{2})\right)$$

2. Let

$$\text{Frac}(\mathbb{F}_p[T]) = \mathbb{F}_p(t)$$

(an infinite field of characteristic p)

Note: $x^p = t$ does not have a solution. One can show that $x^p - t$ is an *irreducible* polynomial in $\mathbb{F}_p(t)[x]$.

Claim: This is **not** seperable.

Proof. Let $\mathbb{E}/\mathbb{F}_p(t)$ be a field extension where $p(x) = x^p - t$ has a root $\alpha \in \mathbb{E}$, that is, $\alpha^p = t$. Then in $\mathbb{E}$, we have

$$x^p - t = x^p - \alpha^p \tag{11.1}$$
$$= (x - \alpha)^p \tag{11.2}$$

because $\mathbb{E}$ must have characteristic p. □

Remark 11.2.4. The equality 11.2 is called the "freshmans dream".

Definition 11.2.5. Let $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ and define the **derivative** of $p(x)$ as

$$p'(x) := a_1 + 2a_2 x + \ldots + n a_n x^{n-1}.$$

Lemma 11.2.6.

(1) $(p(x) + q(x))' = p'(x) + q'(x)$.

(2) $(p(x)q(x))' = p'(x)q(x) + p(x)q'(x)$.

(3) $(p \circ q)' = (p' \circ q) \cdot q'$.

Theorem 11.2.7. *A polynomial* $p(x) \in \mathbb{F}[x]$ *is* seperable $\Leftrightarrow \gcd(p, p') = 1$.

Proof. Suppose $p(x)$ is *not* seperable. Then over a *splitting field* $\mathbb{E}$ of p we have $p = (x-a)^2 q(x)$ for $q(x) \in \mathbb{E}[x]$. But then $p' = 2(x-a)q(x) + (x-a)^2 q'(x) \Rightarrow (x-a) \mid p$ and $(x-a) \mid p'$ so that $(x-a) \mid \gcd(p, p') \Rightarrow \gcd(p, p') \neq 1$ in $\mathbb{E}[x]$. Does it follow that $\gcd(p, p') \neq 1$ in $\mathbb{F}[x]$?

Yes!: It is clear that $\gcd_{\mathbb{F}[x]}(p, p') \mid \gcd_{\mathbb{E}[x]}(p, p')$.

On the other hand, there exists $a(x), b(x) \in \mathbb{F}[x]$

such that (note that if $\mathbb{E}$ is a field then $\mathbb{E}[x]$ is a PID $\Rightarrow \mathbb{E}[x]$ is a *Bezout Domain*)

$$\begin{aligned} a \cdot p + b \cdot p' &= \gcd_{\mathbb{F}[x]}(p, p') \in \mathbb{E}[x] \\ \Leftrightarrow a \cdot (\gcd_{\mathbb{E}[x]}(p, p') q_1(x)) + b \cdot (\gcd_{\mathbb{E}[x]}(p, p') q_2(x)) &= \gcd_{\mathbb{F}[x]}(p, p') \\ \Leftrightarrow \gcd_{\mathbb{E}[x]}(p, p')(a \cdot q_1(x) + b \cdot q_2(x)) &= \gcd_{\mathbb{F}[x]}(p, p') \\ \Rightarrow \gcd_{\mathbb{E}[x]}(p, p') \mid \gcd_{\mathbb{F}[x]}(p, p') \\ \Rightarrow \gcd_{\mathbb{F}[x]}(p, p') &= \gcd_{\mathbb{E}[x]}(p, p'). \end{aligned}$$

Now, if $p(x)$ is *seperable* (11.2.1) then over a *splitting-field* we have

$$p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where $\alpha_1, \ldots, \alpha_n$ are all distinct. But then

$$p' = (x-\alpha_2)\cdots(x-\alpha_n) + \ldots + (x-\alpha_1)\cdots(x-\alpha_{n-1}).$$

Observe: None of the roots of p is a root of p'. It follows that if we had any non-trivial $q(x)$ such that $q(x) \mid p$ and $q(x) \mid p'$; then the prime-factorization of $q(x)$ would need to be composed of elements from the prime-factorization of $p \Rightarrow p, p'$ would share common roots, since

$$\begin{aligned} p(x) &= q(x)r_1(x) \qquad (r_1(x) \in \mathbb{E}[x]) \\ p'(x) &= q(x)r_2(x) \qquad (r_2(x) \in \mathbb{E}[x]) \\ \Rightarrow p(\alpha_i) &= p'(\alpha_i) \\ &= 0 \qquad \text{(for some } \alpha_i \text{ among the roots of } p) \end{aligned}$$

which is a contradiction $\Rightarrow \gcd_{\mathbb{E}[x]}(p, p') = 1 \Rightarrow \gcd_{\mathbb{F}[x]}(p, p') = 1$. □

Remark 11.2.8. Note that $\mathbb{F}[x], \mathbb{E}[x]$ are UFD:s. Hence if

$$\begin{aligned} \gcd_{\mathbb{F}[x]}(p, p') &= d(x) \\ \gcd_{\mathbb{E}[x]}(p, p') &= e(x) \end{aligned}$$

and we have the factorizations

$$\begin{aligned} p(x) &= up_1 \cdots p_n \qquad (p_1, \ldots, p_n \in \mathbb{F}[x], u \in \mathbb{F}) \\ p'(x) &= vq_1 \cdots q_m \qquad (q_1, \ldots, q_n \in \mathbb{F}[x], v \in \mathbb{F}) \end{aligned}$$

then we have that $d(x) = bd_1 \cdots d_k$ where d_i are irreducible polynomials in $\mathbb{F}[x]$ that are common to both the prime-factorization (note prime $\Leftrightarrow$ irreducible in UFD:s) of p and p', and b is a unit.

Now, similarly, we have

$$\gcd_{\mathbb{E}[x]}(p, p') = e(x) \in \mathbb{E}[x]$$

where $e(x) = te_1 \cdots e_\ell$ and e_i is an element both in the prime-factorization of p and p'. Now, assume that $e(x) \neq d(x)$, and assume furthermore that $d(x)$ has a prime-factor p_d common to both p and p' not in $e(x)$. Then we can get a new divisor

$$c(x) = e(x)p_d \text{ such that } c(x)|p \text{ and } c(x)|p'$$

hence $\deg(e(x)) < \deg(c(x)) \Rightarrow$ contradiction!

Inductively, we get that every prime-factor of $d(x)$ must be an element in the prime-factorization of $e(x)$, and therefore

$$\begin{aligned} e(x) &= d(x)q(x) \qquad (q(x) \in \mathbb{E}[x]) \\ \Rightarrow d(x) &\mid e(x). \end{aligned}$$

Corollary 11.2.9. *An irreducible polynomial p is seperable $\Leftrightarrow p' \neq 0$.*

Proof. If p is *irreducible* then

$$\gcd(p, p') = \begin{cases} p \\ 1 \end{cases}$$

where either $\deg(p') < \deg(p)$ or $p' = 0$.

If $\deg(p') < \deg(p)$ then $\gcd(p, p') = 1$. If $p' = 0$, then $\gcd(p, p') = p$.

□

Corollary 11.2.10. *If* $\text{char}(\mathbb{F}) = 0$ *then every irreducible polynomial p over $\mathbb{F}$ is* seperable.

On the other hand, $p(x) = x^p - t \in \mathbb{F}_p(t)[x]$ is *irreducible* and

$$\begin{aligned} p'(x) &= px^{p-1} \\ &= 0 \end{aligned}$$

so *not* seperable.

Definition 11.2.11. An algebraic field extension $\mathbb{E}/\mathbb{F}$ is **separable** if for every $\alpha \in \mathbb{E}$ the *minimal* polynomial of α is seperable (11.2.1).

Definition 11.2.12. A field $\mathbb{F}$ is **perfect** if every algebraic extension $\mathbb{E}/\mathbb{F}$ is *seperable* $\Leftrightarrow$ every *irreducible* polynomial over $\mathbb{F}$ is *seperable*.

We showed that every field of *characteristic* 0 is **perfect**. What about *characteristic* p?

Let $\mathbb{F}$ be a field of characteristic p.

Define:

$$\begin{aligned} \varphi_p : \mathbb{F} &\to \mathbb{F} \\ x &\mapsto x^p \end{aligned}$$

Note:

$$\begin{aligned} \varphi(xy) &= \varphi(x)\varphi(y) \\ \varphi(x+y) &= \varphi(x) + \varphi(y) \qquad \text{(see "freshmans dream")} \\ \varphi(1_{\mathbb{F}}) &= 1_{\mathbb{F}} \end{aligned}$$

$\Rightarrow \varphi$ is a field endomorphism of $\mathbb{F}$, hence injective (8.1.2).

Theorem 11.2.13. *A field $\mathbb{F}$ of* $\text{char}(\mathbb{F}) = p$ *is* ***perfect*** $\Leftrightarrow$ *φ_p, the frobenius endomorphism, is surjective (so is an isomorphism).*

Proof. Suppose $\varphi_p : \mathbb{F} \to \mathbb{F}$ is **surjective**. Let $p(x) \in \mathbb{F}[x]$ be a polynomial such that $p'(x) = 0$. We want to show that p is *not* irreducible.

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0. \\ p'(x) &= n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1 \\ &= 0 \\ \Rightarrow a_k &= 0 \qquad (\text{for } k \not| \, p) \end{aligned}$$

so that

$$\begin{aligned} p(x) &= a_0 + a_p x^p + \ldots + a_{ip}x^{ip} \\ &= b_0 + b_1 x^p + b_2 (x^2)^p + \ldots + b_k (x^k)^p \qquad (b_0, b_1, \ldots, b_k \in \mathbb{F}). \end{aligned}$$

Since φ_p is surjective we have

$$b_i = c_i^p \qquad (c_i \in \mathbb{F}) \tag{11.3}$$

for *all* b_i.

Hence

$$\begin{aligned} p(x) &= b_0 + b_1 (x^1)^p + \ldots + b_k (x^k)^p \\ &= c_0^p + c_1^p (x^1)^p + \ldots + c_k^p (x^k)^p \\ \Leftrightarrow p(x) &= (c_0)^p + (c_1 x)^p + \ldots + (c_k x^k)^p \\ &= (c_0 + c_1 x + \ldots + c_k x^k)^p \qquad (c_0 + c_1 x + \ldots + c_k x^k \in \mathbb{F}[x]) \end{aligned}$$

Therefore, $p(x)$ is not irreducible.

On the other hand, if φ_p is not surjective, one can find $\alpha \in \mathbb{F} \setminus \mathrm{im}(\varphi_p)$ and show that $x^p - \alpha$ is irreducible where $(x^p - a)' = 0$ so *not* seperable. □

Corollary 11.2.14. *A finite field is perfect. Because for finite* $\mathbb{F}$ *we have* φ_p *injective* $\Rightarrow$ *surjective.*

11.3 A couple of facts about seperable extensions

Definition 11.3.1. For any field extension $\mathbb{E}/\mathbb{F}$, the set of elements $\alpha \in \mathbb{E}$ such that $\mathbb{F}(\alpha)$ is *seperable* (11.2.11) over $\mathbb{F}$ is a subfield of $\mathbb{E}$. The *collection* of such elements is called the **seperable closure** of $\mathbb{E}$ in $\mathbb{F}$.

So any algebraic extension $\mathbb{E} \supset \mathbb{F}$ factors as

$$\mathbb{F} \subset \mathbb{F}^{\mathrm{sep}} \subset \mathbb{E}.$$

where $\mathbb{F}^{\mathrm{sep}}$ is seperable over $\mathbb{F}$ and $\mathbb{E}/\mathbb{F}^{\mathrm{seperable}}$ is *purely* **inseperable**.

Theorem 11.3.2. *A finite degree seperable extension* $\mathbb{E}/\mathbb{F}$ *is* ***simple*** *(8.3.5) for some* $\alpha \in \mathbb{E}$.

Example 11.3.3.

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$$

for some α.

11.3.1 Normality of extensions

Definition 11.3.4. An algebraic extension $\mathbb{E}/\mathbb{F}$ is **normal** if *every* irreducible polynomial over $\mathbb{F}$ that has a root in $\mathbb{E}$ *splits completely* (9.4.1) in $\mathbb{E}$.

This is *equivalent* to: $\mathbb{E}$ is the *splitting field* (9.4.2) of a collection of polynomials $\{f_\alpha\}_{\alpha\in I} \subset \mathbb{F}[x]$.

Example 11.3.5. $\mathbb{Q}(\sqrt{2})$ is *normal* over $\mathbb{Q}$ since it is the splitting field of $p(x) = x^2 - 2$.

Non-example:

$\mathbb{Q}(\sqrt[3]{2})$ is *not normal* over $\mathbb{Q}$. Not all roots of $x^3 - 2$ are in this field.

Definition 11.3.6. A **Galois extension** $\mathbb{E}/\mathbb{F}$ is one that is *both seperable* and *normal*.

Definition 11.3.7. The **Galois group** $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is the group of field *automorphisms* $\varphi : \mathbb{E} \to \mathbb{E}$ such that $\varphi|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$.

For Galois extensions we have

$$|\operatorname{Gal}(\mathbb{E}/\mathbb{F})| = \deg_{\mathbb{F}}(\mathbb{E}). \tag{11.4}$$

11.4 Finite fields

Theorem 11.4.1. *A finite field has p^n elements where p is a prime and $n \geq 1$. For every p, n there exists a finite field with p^n elements, which is unique, up to isomorphism.*

Proof. Let $\mathbb{F}$ be a *finite* field. Then $\mathrm{char}(\mathbb{F}) = p$ for p prime, so that $\mathbb{F}$ contains a copy of $\mathbb{F}_p$; $\mathbb{F}$ is a *finite vector space* over $\mathbb{F}_p$. Hence $|\mathbb{F}| = p^n$ where $[\mathbb{F} : \mathbb{F}_p] = n$.

Consider the polynomial

$$x^{p^n} - x \in \mathbb{F}_p[x].$$

Let $\mathbb{F}$ be the *splitting-field* of $x^{p^n} - x$ over $\mathbb{F}_p$ where $(x^{p^n} - x)' = -1$ so that $\gcd((x^{p^n} - 1), (x^{p^n} - 1)') = 1$. Hence $x^{p^n} - x$ is *seperable* over $\mathbb{F}_p$ by 11.2.7 $\Rightarrow$ it has p^n roots in $\mathbb{F}$ (see 9.4.2, 11.2.1).

We denote the roots of $x^{p^n} - x$ in $\mathbb{F}$ as $\alpha_1, \ldots, \alpha_{p^n} \in \mathbb{F}$. We notice that if α_i, α_j are roots then

$$\begin{aligned}(\alpha_i \cdot \alpha_j)^p &= \alpha_i^p \cdot \alpha_j^p \\ &= \alpha_i \cdot \alpha_j\end{aligned}$$

$$\left(\frac{\alpha_i}{\alpha_j}\right)^p = \frac{\alpha_i}{\alpha_j}$$

$$\begin{aligned}(\alpha_i \pm \alpha_j)^p &= \alpha_i^p \pm \alpha_j^p \\ &= \alpha_i \pm \alpha_j.\end{aligned}$$

It follows that $\{\alpha_1, \ldots, \alpha_{p^n}\} \subset \mathbb{F}$ is a subfield of $\mathbb{F}$ and that $x^{p^n} - x$ *splits completely* over $\{\alpha_1, \ldots, \alpha_{p^n}\}$ so that $\mathbb{F} = \{\alpha_1, \ldots, \alpha_{p^n}\}$ where $|\mathbb{F}| = p^n$.

□

Chapter 12

Twelfth lecture

12.1 Algebraic Geometry

Definition 12.1.1. An **algebraic set** is a set of solutions of polynomial equations.

Example 12.1.2.

$$x^2 + y^2 = 1 \qquad \text{(algebraic subset of the plane).}$$

- Interplay between *geometric* properties of *algebraic sets* and *algebraic* properties of *rings of functions*.

$$\left\{ \textit{Geometric} \text{ properties of } \textit{algebraic} \text{ sets} \right\} \longleftrightarrow \left\{ \textit{Algebraic} \text{ properties of } \textit{rings of functions} \right\}$$

- Let k be a field and $k[x_1, \ldots, x_n]$ be a polynomial ring ("ring of functions").
- $p(x_1, \ldots, x_n) \rightsquigarrow$ function $k^n \to k$
- Usually denote $k := \mathbb{A}$ and $\mathbb{A}^n := k^n$ ("n-dimensional affine space over k").

We have a function

$$\begin{aligned} k[x_1, \ldots, x_n] \times \mathbb{A}^n &\longrightarrow k \\ (p(x_1, \ldots, x_n), (a_1, \ldots, a_n)) &\longmapsto p(a_1, \ldots, a_n) \end{aligned}$$

- That is, for each $(a_1, \ldots, a_n) \in \mathbb{A}^n$ we get a ring-homomorphism

$$\mathrm{ev}_{(a_1, \ldots, a_n)} : k[x_1, \ldots, x_n] \longrightarrow k$$

  or rather, a k-algebra homomorphism.

- We have a bijection $\mathbb{A}^n \cong k\text{-alg}(k[x_1, \ldots, x_n], k)$.
- More generally: A polynomial function $\mathbb{A}^m \longrightarrow \mathbb{A}^n$ is a function of the form

$$(a_1, \ldots, a_m) \longmapsto (\varphi_1(a_1, \ldots, a_m), \ldots, \varphi_n(a_1, \ldots, a_m))$$

where $\varphi_1, \ldots, \varphi_n \in k[x_1, \ldots, x_m] \Rightarrow$ a k-algebra morphism $k[x_1, \ldots, x_m] \leftarrow k[x_1, \ldots, x_n] \Rightarrow$ a natural bijection

$$\text{Poly}(\mathbb{A}^m, \mathbb{A}^n) \cong \text{k-alg}(\underbrace{k[x_1, \ldots, x_n]}_{\mathbb{A}^n \to k}, \underbrace{k[x_1, \ldots, x_m]}_{\mathbb{A}^m \to k}) \qquad \text{(contravariant equivalence)}$$

Definition 12.1.3. ($\mathcal{Z}(-)$). Suppose $P \subset k[x_1, \ldots, x_n]$ is a subset. Define

$$\mathcal{Z}(P) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n \mid f(a_1, \ldots, a_n) = 0, \forall f \in P\}$$

$$\mathcal{Z} : \text{subsets of } k[x_1, \ldots, x_n] \longmapsto \text{subsets of } \mathbb{A}^n.$$

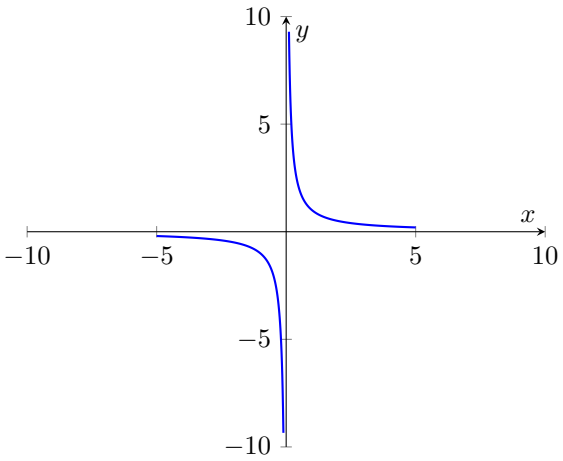
We say that $S \subset \mathbb{A}^n$ is **algebraic** if $S = \mathcal{Z}(P)$ for some $P \subset k[x_1, \ldots, x_n]$.

Example 12.1.4. Take base field as $k = \mathbb{R}$. A subset of $\mathbb{R}$ is *algebraic* (12.1.3) $\Leftrightarrow$ it is a *finite* set or *all of* $\mathbb{R}$ (works for any field k!).

Example 12.1.5.

$$\left\{ \left(x, \frac{1}{x} \right) \;\middle|\; x \in \mathbb{R}, x \neq 0 \right\}$$

is an *algebraic* subset of $\mathbb{R}^2 \Rightarrow$ set of solutions $xy - 1 = 0$.



Example 12.1.6. $\{(x, \sin(x)) \mid x \in \mathbb{R}\}$ is <u>not</u> an an algebraic subset of $\mathbb{R}^2$. Why? Because there does not exist a polynomial of 2 variables such that $p(x, y) = 0 \Leftrightarrow y = \sin(x)$.

Proof. For any polynomial p, the set of solutions of the equation $p(x, 0) = 0$ is *finite*, but $\sin(x) = 0$ has *infinitely* many solutions. □

12.2 Properties of $\mathcal{Z}(-)$

(1) If $P \subset Q \subset k[x_1, \ldots, x_n]$ then $\mathcal{Z}(P) \supset \mathcal{Z}(Q)$.

(2) If $P = \underbrace{\{f_1, \ldots, f_n\}}_{\text{finite}}$ then $\mathcal{Z}(f_1, \ldots, f_n) = \mathcal{Z}(f_1) \cap \cdots \cap \mathcal{Z}(f_n)$.

Definition 12.2.1. The *set of zeroes* of a *single* polynomial f, $\mathcal{Z}(f)$, is called a **hypersurface** in $\mathbb{A}^n$.

(3) For $p \subset k[x_1, \ldots, x_n]$ let $\langle p \rangle$ be the ideal of $k[x_1, \ldots, x_n]$ generated by p. Then $\mathcal{Z}(p) = \mathcal{Z}(\langle p \rangle)$.

Proof. Since $p \subset \langle p \rangle$, by (1) we have $\mathcal{Z}(p) \supset \mathcal{Z}(\langle p \rangle)$.

Exercise: prove that

$$\mathcal{Z}(p) \subset \mathcal{Z}(\langle p \rangle)$$

□

Remark 12.2.2. We can think of $\mathcal{Z}(-)$ as a function on ideals.

(4)

$$\mathcal{Z}(P) \cap \mathcal{Z}(Q) = \mathcal{Z}(P \cup Q) \qquad (P, Q \subset k[x_1, \ldots, x_n]).$$

More generally, if $P_\alpha \subset k[x_1, \ldots, x_n]$ where $\alpha \in I$ then $\bigcap_{\alpha \in I} \mathcal{Z}(P_\alpha) = \mathcal{Z}\Big(\bigcup_{\alpha \in I} P_\alpha\Big) \Rightarrow$ arbitrary intersection of algebraic sets is algebraic.

$$\mathcal{Z}(P + Q) = \mathcal{Z}(P \cup Q).$$

(5)

$$\mathcal{Z}(P) \cup \mathcal{Z}(Q) = \mathcal{Z}(P \cdot Q) \tag{12.1}$$

where $P \cdot Q = \{a_1 b_1 + \ldots + a_\ell b_\ell \mid a_i \in P, b_i \in Q\}$. Note that there always is an inclusion $P \cdot Q \subset P \cap Q$ but in general the two sets are not the same.

Proof of 12.1.

$$\begin{array}{ccc} & & P \cdot Q \subset P \cap Q \\ & \underbrace{\Rightarrow} & \mathcal{Z}(P) \cup \mathcal{Z}(Q) \subset \mathcal{Z}(P \cap Q) \\ P \cdot Q \subset P \cap Q \subset P \cup Q & & \\ & & \subset \mathcal{Z}(P \cdot Q). \end{array}$$

Let $(a_1, \ldots, a_n) \in \mathcal{Z}(P \cdot Q) \Rightarrow$ for every $p(x_1, \ldots, x_n) \in P$ and $q(x_1, \ldots, x_n) \in Q$ we have $p(x_1, \ldots, x_n) \cdot q(x_1, \ldots, x_n) = 0$.

Suppose $(a_1, \ldots, a_n) \notin Z(P) \Rightarrow$ then there exist $p \in P$ such that $p(a_1, \ldots, a_n) \neq 0$. But

$$p(a_1, \ldots, a_n) \cdot q(a_1, \ldots, a_n) = 0$$

for all $q \in Q$.

So $q(a_1, \ldots, a_n) = 0$ for all q. Hence $q(a_1, \ldots, a_n) = 0$ for all q, so $(a_1, \ldots, a_n) \in \mathcal{Z}(Q) \Rightarrow$ finite unions of algebraic sets are algebraic. □

(6)

$$\begin{aligned} \varnothing &= \mathcal{Z}(k[x_1, \ldots, x_n]) \\ \mathbb{A}^n &= \mathcal{Z}(0) \end{aligned}$$

so $\varnothing, \mathbb{A}^n$ are algebraic sets ((12.1.3)) $\Rightarrow$ there is a topology on $\mathbb{A}^n$ whose closed sets are precisely the algebraic sets (Zariski-topology). Although the Zariski-topology is usually defined on prime-ideals.

E.g. on $\mathbb{A}^1$ it is the finite complement topology (cofinite topology).

The **finite complement topology** (or **cofinite topology**) $\mathcal{T}$ on a set X is defined as

$$\mathcal{T} := \{A \subseteq X \mid A = \varnothing \text{ or } X \setminus A \text{ finite}\}$$

12.3 Recap

Suppose $I \subset k[x_1, \ldots, x_n]$ is a finitely generated ideal, say $I = (f_1, \ldots, f_n)$ where $f_i \in k[x_1, \ldots, x_n]$.

Then

$$\begin{aligned} \mathcal{Z}(I) &= \mathcal{Z}(f_1, \ldots, f_n) \\ &= \mathcal{Z}(f_1) \cap \ldots \cap \mathcal{Z}(f_n). \end{aligned}$$

What if I is not finitely generated? This *never* happens!

Henceforth, we by *ring* mean a *commutative ring with unity.*

Lemma 12.3.1. *Let R be a commutative ring with a 1. Then the following are equivalent:*

(a) Every ideal of R is finitely generated.

(b) For every ascending chain of ideals

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots \subset R$$

there exists an n_0 s.t.

$$I_{n_0} = I_{n_0+1} = \ldots = I_m \qquad (\forall m \geq n_0).$$

*R is called **Noetherian** if it satisfies this (see also 7.3.1).*

Theorem 12.3.2 (Hillbert basis theorem)**.** *If R is Noetherian then so is $R[x]$.*

Corollary 12.3.3. *$k[x_1, \ldots, x_n]$ is Noetherian.*

Contrapositive. Suppose $R[x]$ is not noetherian. We prove that neither is R.

Suppose $I \subset R[x]$ is not finitely generated. Construct a sequence of polynomials $f_1, \ldots, f_n \in R[x]$ inductively. f_1 is a polynomial of lowest degree in I (well-ordering of $\mathbb{N}$). Inductively, f_{n+1} is a polynomial of lowest degree in $I \setminus (f_1, \ldots, f_n)$.

Let d_n be the *degree* of f_n ($\deg(f_n) = d_n$). Then $d_1 \leq d_2 \leq \ldots$

Let a_n be the leading coefficient of f_n (i.e. the coefficient of x^{d_n}).

We claim: The sequence of ideals

$$(a_1) \subset (a_1, a_2) \subset \ldots \subset (a_1, \ldots, a_n) \subset \ldots \subset R$$

does not terminate.

Proof of the claim:

No 2 adjacent ideals are the same. Suppose by contradiction that $(a_1, \ldots, a_n) = (a_1, \ldots, a_{n+1})$. Then there exist $r_1, r_2, \ldots, r_n \in R$ such that $a_{n+1} = r_1 a_1 + \ldots + r_n a_n$.

Define $g(x) = r_1 f_1(x) x^{d_{n+1}-d_1} + \ldots + r_n f_n(x) x^{d_{n+1}-d_n}$.

$g(x) \in (f_1, \ldots, f_n)$ and

$$\begin{aligned} \deg(g(x)) &= \deg(f_{n+1}) \\ &= d_{n+1}. \end{aligned}$$

The leading coefficient of g is the same as the leading coefficient of $f_{n+1}(x) \Rightarrow \deg(f_{n+1}(x) - g(x)) < \deg(f_{n+1})$ and $\underbrace{f_{n+1}}_{\notin (f_1,\ldots,f_n)} - \underbrace{g(x)}_{\in (f_1,\ldots,f_n)} \in I \setminus (f_1, \ldots, f_n)$.

Contradiction to minimality of $\deg(f_{n+1})$. □

12.4 $\mathcal{I}(-)$

Definition 12.4.1. Let $S \subset \mathbb{A}^n$. Define

$$\mathcal{I}(S) = \{f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in S\}$$

Clearly, $\mathcal{I}(S)$ is an ideal of $k[x_1, \ldots, x_n]$.

$$\left\{ \begin{array}{c} \text{Ideals of} \\ \mathbb{K}[\alpha_1, \ldots, \alpha_n] \end{array} \right\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\rightleftarrows}} \left\{ \text{Subsets of } \mathbb{A}^n \right\}$$

Example 12.4.2. $(x^2) \subset k[x] \rightsquigarrow \mathcal{Z}(x^2) = \{0\} \rightsquigarrow \mathcal{I}(\mathcal{Z}(x^2)) = (x) \supsetneq (x^2)$.

Example 12.4.3. $(x^2 + 1) \subset \mathbb{R}[x] \rightsquigarrow \mathcal{Z}(x^2 + 1) = \varnothing$.

$\rightsquigarrow$

$\mathcal{I}(\mathcal{Z}(x^2 + 1)) = \mathbb{R}[x] \supsetneq (x^2 + 1)$

12.5 Some properties of $\mathcal{I}$ (and $\mathcal{Z}$)

1. If $S \subset T \subset \mathbb{A}^n$ then $\mathcal{I}(S) \supset \mathcal{I}(T)$ (contravariance, as for $\mathcal{Z}(-)$!)
2. For *all* $S \subset \mathbb{A}^n$ we have $\mathcal{Z}(\mathcal{I}(S)) \supset S$.

   For all $P \subset k[x_1, \ldots, x_n]$ we have $\mathcal{I}(\mathcal{Z}(P)) \supset P$.
3. $\mathcal{I}(\mathcal{Z}(\mathcal{I}(S))) = \mathcal{I}(S)$ and

   $\mathcal{Z}(\mathcal{I}(\mathcal{Z}(P))) = \mathcal{Z}(P)$.

12.6 Coordinate rings

Definition 12.6.1. Let $V \subset \mathbb{A}^n$ be an algebraic set. Then the k-algebra

$$k[V] := k[x_1, \ldots, x_n]/\mathcal{I}(V)$$

is the **ring of polynomial functions on V** (also known as **coordinate ring**).

Suppose V, W are algebraic (12.1.3) subsets of $\mathbb{A}^m, \mathbb{A}^n$ respectively ($V \subset \mathbb{A}^m$ & $W \subset \mathbb{A}^n$). A polynomial function $\varphi : V \to W$ is a collection of polynomials

$$\varphi_1(x_1, \ldots, x_m), \ldots, \varphi_n(x_1, \ldots, x_m)$$

such that if $(a_1, \ldots, a_m) \in V$ then

$$(\varphi_1(a_1, \ldots, a_m), \ldots, \varphi_n(a_1, \ldots, a_m)) \in W$$

Theorem 12.6.2. *There is a bijective correspondence between polynomial functions from V to W and k-algebra homomorphisms from $k[W]$ to $k[V]$.*

Chapter 13

Thirteenth lecture

Let k be a field, and let $\mathbb{A}^n = k^n$ be the n-dimensional affine space over k.

$$\left\{ \begin{array}{c} \text{Ideals of} \\ \mathbb{K}[x_1, \ldots, x_n] \end{array} \right\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\rightleftarrows}} \left\{ \text{Subsets of } \mathbb{A}^n \right\}$$

Example 13.0.1. Let $k = \mathbb{R}$, $n = 1$ and note $\mathbb{N} = \{0, 1, \ldots\} \subset \mathbb{R}$. We have $\mathcal{I}(\mathbb{N}) = \{0\}$ so that $\mathcal{Z}(\mathcal{I}(\mathbb{N})) = \mathbb{R}$.

Comment 13.0.2. Note that by property 6. in lecture 12, we have $\mathcal{Z}(0) = \mathbb{A}^n$. Also note that $\mathcal{I}(\mathbb{N}) = \{f \in \mathbb{R}[x] \mid f(n) = 0, \forall n \in \mathbb{N}\}$. A polynomial in one variable can only have *finitely* many zeroes, but a polynomial in $\mathcal{I}(\mathbb{N})$ would be forced to have *infinitely* many zeroes $\rightsquigarrow \mathcal{I}(\mathbb{N}) = \{0\}$.

Example 13.0.3. Let $S = \{(a_1, \ldots, a_n) \in \mathbb{A}^n\}$ be a **singleton**-set

$$\begin{aligned} \rightsquigarrow \mathcal{I}(S) &= \{f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0\} \\ &= \ker(k[x_1, \ldots, x_n] \xrightarrow{\text{ev}_{a_1, \ldots, a_n}} k) \\ &= a \qquad \text{(maximal ideal)} \\ &= (x_1 - a_1, \ldots, x_n - a_n) \qquad \text{(exercise!)}. \end{aligned}$$

$\mathcal{Z}(\mathcal{I}(a_1, \ldots, a_n)) = \{(a_1, \ldots, a_n)\}$.

Example 13.0.4. $(x^2 + 1) \subset \mathbb{R}[x]$ is *maximal* but $\mathcal{Z}(x^2 + 1) = \varnothing \rightsquigarrow \mathcal{I}(\mathcal{Z}(x^2 + 1)) = \mathbb{R}[x]$.

Remark 13.0.5. Remember that if $k = \mathbb{A}$ is *infinite* then $\mathcal{I}(\varnothing) = k[x_1, \ldots, x_n]$. Also note that $\mathbb{R}$ in 13.0.4 is not algebraically closed.

We have that $\mathcal{I}, \mathcal{Z}$ induces *bijection* between $\text{im}(\mathcal{I})$ and $\text{im}(\mathcal{Z})$. The image of $\mathcal{Z}(-)$ is *affine algebraic sets*. What is the image of $\mathcal{I}(-)$?

13.1 Radical ideals

Let R be a commutative ring with 1 and let $I \subset R$ be an ideal.

Definition 13.1.1. . The **radical** of the ideal I is the set

$$\sqrt{I} = \{r \in R \mid r^n \in I, \text{ for some } n \in \mathbb{N}_{>0}\}.$$

Lemma 13.1.2.

- $\sqrt{I}$ *is an ideal.*
- $I \subset \sqrt{I}$.
- $\sqrt{\sqrt{I}} = \sqrt{I}$

Proof. The least trivial step is to show that if $x, y \in \sqrt{I}$ then $x+y \in \sqrt{I}$. Suppose $x^m \in I$ and $y^n \in I$. Then

$$(x+y)^{m+n} = \sum_{j=1}^{m+n} \binom{m+n}{j} x^{(m+n)-j} \cdot y^j.$$

Either $j \geq n$ and then $y^j \in I$, or $j < n \rightsquigarrow m+n-j > m+n-n = m$ so that $x^{m+n-j} \in I \rightsquigarrow (x+y)^{m+n} \in \sqrt{I}$. □

Definition 13.1.3. . I is a **radical ideal** if $I = \sqrt{I}$.

Example 13.1.4.

- $(30) \subset \mathbb{Z}$ is a radical ideal
- $(12) \subset \mathbb{Z}$ is not a radical ideal, we have that $6^2 \in (12)$ but $6 \notin (12)$.
- Generally, $(n) \subset \mathbb{Z}$ is radical $\Leftrightarrow$ n is *square*-free or 0; that is, n has no *repeated prime factors* or is 0.

Proposition 13.1.5. *Suppose $\{\mathfrak{p}_\alpha \mid \alpha \in I\}$ is a collection of prime ideals in R. Then $\bigcap_{\alpha \in I} \mathfrak{p}_\alpha$ is radical.*

Proof. Suppose that $x^n \in \bigcap_{\alpha \in I} \mathfrak{p}_\alpha$. Then $x^n \in \mathfrak{p}_\alpha$ for all $\alpha \in I$. Then we find that $x^{n-1} \cdot x$ is such that either x or x^{n-1} is in $\mathfrak{p}_\alpha$ for all $\alpha \in I$. If $x \in \mathfrak{p}_\alpha$ for arbitrary α, we are done. If x^{n-1} is in $\mathfrak{p}_\alpha$ for some α, then clearly $x^{n-2} \cdot x$ is such that either x^{n-2} or x is in $\mathfrak{p}_\alpha$. Repeated application (note, in a finite number of steps, for fixed α) gives us that $x \in \mathfrak{p}_\alpha$ for arbitrary α. Hence $x \in \bigcap_{\alpha \in I} \mathfrak{p}_\alpha$. □

Proposition 13.1.6. *Let $I \subset R$ be an ideal. Then the following are equivalent:*

(1) $I = \sqrt{I}$

(2) I equals the intersection of some prime ideals.

(3) I equals the intersection of all the prime ideals containing I.

Proof. (2) $\Leftrightarrow$ (3):

(3) $\Rightarrow$ (2) is obvious. (2) $\Rightarrow$ (3) asserts that if I equals the intersection of *some* prime ideals, then I equals the intersection of *all prime ideals containing* I. So assume that $I = \bigcap_{\ell \in \mathcal{L}} \mathfrak{p}_\ell$ for *some* prime ideals $\mathfrak{p}_\ell$ and index set $\mathcal{L}$. Then clearly $I \subset \mathfrak{p}_\ell$ for all $\ell \in \mathcal{L}$. Now, let $\mathcal{L}'$ be the index set for *all* prime ideals $\mathfrak{p}_{\ell'}$ so that $I \subset \mathfrak{p}_{\ell'} \rightsquigarrow \bigcap_{\ell' \in \mathcal{L}'} \mathfrak{p}_{\ell'} \subseteq \bigcap_{\ell \in \mathcal{L}} \mathfrak{p}_\ell = I \subseteq \bigcap_{\ell' \in \mathcal{L}'} \mathfrak{p}_{\ell'} \Rightarrow I = \bigcap_{\ell' \in \mathcal{L}'} \mathfrak{p}_{\ell'}$.

For (2) $\Rightarrow$ (1), we can use the previous proposition, which gives us that $I = \bigcap_{\ell \in \mathcal{L}} \mathfrak{p}_\ell$ is radical, hence $I = \sqrt{I}$.

For (1) $\Rightarrow$ (3): In fact, we will show that $\sqrt{I} = \bigcap_{\alpha \in A} \mathfrak{p}_\alpha$ with where A is an index set for *all* prime-ideals $\mathfrak{p}_\alpha$ *containing* I (i.e. $I \subset \mathfrak{p}_\alpha$). The inclusion $\sqrt{I} \subset \bigcap_{\alpha \in A} \mathfrak{p}_\alpha$ follows from the fact that if $x \in \sqrt{I}$, so that $x^n \in I$ for some (positive) natural number n, then as in the proof of prop. 13.1.5 we find that x must be in $\mathfrak{p}_\alpha$ for all α.

For the inclusion $\bigcap_\alpha \mathfrak{p}_\alpha \subset \sqrt{I}$:

Suppose $x \notin \sqrt{I}$; we show there exists a prime ideal $\mathfrak{p}$ containing I s.t. $x \notin \mathfrak{p}$. Consider the set of ideals $\mathcal{O} := \{J \subset R \mid I \subset J, x^n \notin J, \forall n \in \mathbb{N}_{>0}\}$. We have that $I \in \mathcal{O}$ since $x \notin \sqrt{I}$. If $J_1 \subset J_2 \subset \ldots \subset J_\alpha \subset \ldots$ is an ascending chain in $\mathcal{O}$, then $J = \bigcup_\alpha J_\alpha$ is in $\mathcal{O}$ (so every chain in $\mathcal{O}$ has an upper bound). By Zorns lemma, there exists a maximal element (with respect to inclusion) $\mathfrak{p} \in \mathcal{O}$.

Claim: $\mathfrak{p}$ is prime.

Proof. Suppose $ab \in \mathfrak{p}$ but $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. Then $\mathfrak{p} + (a), \mathfrak{p} + (b) \notin \mathcal{O}$, by maximality. So for some $m, n \in \mathbb{N}_{>0}$ we have $x^m = p_1 + r_1 a$ and $x^n = p_2 + r_2 b$ for $p_1, p_2 \in \mathfrak{p}$ and $r_1, r_2 \in R$. But then

$$\begin{aligned} x^{m+n} &= x^m \cdot x^n \\ &= (p_1 + r_1 a) \cdot (p_2 + r_2 b) \\ &= p_1 p_2 + p_1(r_2 b) + (r_1 a) p_2 + r_1 r_2 ab \in \mathfrak{p} \end{aligned}$$

which is a contradiction to $\mathfrak{p} \in \mathcal{O}$, by definition of $\mathcal{O}$. □

Hence, we have found a prime ideal $\mathfrak{p}$ such that $I \subset \mathfrak{p}$ and so that $x^n \notin \mathfrak{p}$, for all $n \in \mathbb{N}_{>0}$. We have thus shown that $x \notin \sqrt{I} \Rightarrow \exists \mathfrak{p}$, $\mathfrak{p}$ prime, that includes I, so that $x \notin \mathfrak{p}$, hence $x \notin \bigcap_\alpha \mathfrak{p}_\alpha$. This is the contrapositive to what we wanted to show (i.e. $x \in \bigcap_\alpha \mathfrak{p}_\alpha \Rightarrow x \in \sqrt{I}$). □

Note: If $I \subsetneq R$ then $\sqrt{I} \subsetneq R$

Lemma 13.1.7. *Suppose $S \subset \mathbb{A}^n$, then $\mathcal{I}(S)$ is a radical ideal of $k[x_1, \ldots, x_n]$ (one needs to assume that k is algebraically closed, I believe).*

Proof. Suppose $f(x_1, \ldots, x_n)^m \in \mathcal{I}(S)$ so that $f(a_1, \ldots, a_n)^m = 0, \forall (a_1, \ldots, a_n) \in S \Rightarrow f(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in S \Rightarrow f(x_1, \ldots, x_n) \in \mathcal{I}(S)$. □

Comment 13.1.8. We have here used the fact that $f(a_1, \ldots, a_n) \in k$ and k is a field, hence has no zero-divisors $\rightsquigarrow f(a_1, \ldots, a_n) = 0$ if $f(a_1, \ldots, a_n)^m = 0$ (by repeated application, in a finite number of steps, of the fact that $f^j \cdot f = 0$ implies that f^j or f is 0, starting from $j = m$.).

13.2 Hillberts Nullstellensatz

Theorem 13.2.1. *(Hillberts Nullstellensatz). Let $J \subset k[x_1, \ldots, x_n]$ be an ideal. Then $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$, if k is algebraically closed.*

Consequences:

(2) $\mathrm{im}(\mathcal{I}) =$ radical ideals of $k[x_1, \ldots, x_n]$. Indeed, we saw that $\mathrm{im}(\mathcal{I}) \subset \{\text{radical ideals}\}$. Suppose that $J \subset k[x_1, \ldots, x_n]$ is radical. Then

$$\begin{aligned} \mathcal{I}(\mathcal{Z}(J)) &= \sqrt{J} \\ &= J \end{aligned}$$

so $J \in \mathrm{im}(\mathcal{I})$.

(2) If $J \subsetneq k[x_1, \ldots, x_n]$ is a proper ideal, then $\mathcal{Z}(J) \neq \emptyset$. Indeed, $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J} \subsetneq k[x_1, \ldots, x_n]$ but $\mathcal{I}(\emptyset) = k[x_1, \ldots, x_n]$ (The "weak" Nullstellensatz).

(2) Suppose $f_1, \ldots, f_k \in k[x_1, \ldots, x_n]$ so that $\mathcal{Z}(f_1) \cap \ldots \cap \mathcal{Z}(f_k) \neq \emptyset$. Then there exists $h_1, \ldots, h_k \in k[x_1, \ldots, x_n]$ so that

$$h_1(x_1, \ldots, x_n) f_1(x_1, \ldots, x_n) + \ldots + h_k(x_1, \ldots, x_n) f_k(x_1, \ldots, x_n) = 1.$$

(2) Every *maximal* ideal $\mathcal{M} \subset k[x_1, \ldots, x_n]$ has the form $\mathcal{M} = (x_1 - a_1, \ldots, x_n - a_n)$.

We prove the strong Nullstellensatz assuming "weak" Nullstellensatz (Rabinovich trick).

Proof. Let $J = (f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n))$ and $g \in \mathcal{I}(\mathcal{Z}(J))$. We want to prove that $g^\ell \in J$ for some $\ell \geq 1, \ell \in \mathbb{Z}^+$.

Claim: $g \in \mathcal{I}(\mathcal{Z}(J)) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0, \forall a \in \mathcal{Z}(J)\} \Leftrightarrow \mathcal{Z}(g) \supset \mathcal{Z}(f_1) \cap \ldots \cap \mathcal{Z}(f_k)$.

Note: $\mathcal{Z}(J) = \mathcal{Z}(f_1) \cap \ldots \cap \mathcal{Z}(f_k)$

Proof. If $\mathcal{Z}(g) \supset \mathcal{Z}(J) = \mathcal{Z}(f_1) \cap \ldots \cap \mathcal{Z}(f_k)$ then $\mathcal{I}(\mathcal{Z}(g)) \subset \mathcal{I}(\mathcal{Z}(J))$. Furthermore we have that $g \in \mathcal{I}(\mathcal{Z}(g)) \Rightarrow g \in \mathcal{I}(\mathcal{Z}(J))$, by properties of $\mathcal{I}(-)$ (12.4). On the other hand, if $g \in \mathcal{I}(\mathcal{Z}(J))$ then we have that

$$\begin{aligned} &\{g\} \subset \mathcal{I}(\mathcal{Z}(J)) \\ \Rightarrow \mathcal{Z}(g) \supset \mathcal{Z}(\mathcal{I}(\mathcal{Z}(J)) &= \mathcal{Z}(J) \\ &= \mathcal{Z}(f_1) \cap \ldots \cap \mathcal{Z}(f_k). \end{aligned}$$

□

Consider the following polynomials in $k[x_1, \ldots, x_{n+1}]$

$f_1(x_1,\dots,x_n),\dots,f_k(x_1,\dots,x_n),x_{n+1}g(x_1,\dots,x_n)-1$. The common set of zeroes of these polynomials are $\varnothing$. By the "weak" nullstellensatz (((2)) in "Consequences") we find that there exists $h_1(x_1,\dots,x_{n+1}),\dots,h_{k+1}(x_1,\dots,x_{n+1})\in k[x_1,\dots,x_{n+1}]$ so that

$$h_1(x_1,\dots,x_{n+1})f_1(x_1,\dots,x_n)+h_k(x_1,\dots,x_{n+1})f_k(x_1,\dots,x_n)+h_{k+1}(x_1,\dots,x_{n+1})(x_{n+1}g(x_1,\dots,x_n)-1)=1. \tag{13.1}$$

We make a substitution $x_{n+1}=\dfrac{1}{g(x_1,\dots,x_n)}$ in (13.1), and then see that in $\mathrm{Frac}(k[x_1,\dots,x_n])=k(x_1,\dots,x_n)$ we have the identity

$$h_1(x_1,\dots,\frac{1}{g})f_1(x_1,\dots,x_n)+\dots+h_k(x_1,\dots,\frac{1}{g})f_k(x_1,\dots,x_n)=1. \tag{13.2}$$

Note: (13.2) is an element of $k(x_1,\dots,x_n)$ since we have a sum of terms which are rational expressions of polynomials in $k[x_1,\dots,x_n]$.

Let ℓ be the highest power of x_{n+1} in $h_1,\dots,h_k$. Then $h_i(x_1,\dots,x_n,\frac{1}{g})\cdot g(x_1,\dots,x_n)^\ell=p_i(x_1,\dots,x_n)\in k[x_1,\dots,x_n]\rightsquigarrow$ multiplying both sides by $g(x_1,\dots,x_n)^\ell$ in (13.2) gives us

$$p_1(x_1,\dots,x_n)f_1(x_1,\dots,x_n)+\dots+p_k(x_1,\dots,x_n)f_k(x_1,\dots,x_n)=g(x_1,\dots,x_n)^\ell$$

which implies that $g(x_1,\dots,x_n)^\ell\in J\Rightarrow g(x_1,\dots,x_n)\in\sqrt{J}$.

This shows $\mathcal{I}(\mathcal{Z}(J))\subset\sqrt{J}$.

To show $\sqrt{J}\subset\mathcal{I}(\mathcal{Z}(J))$:

If $g\in\sqrt{J}\Rightarrow\exists\ell\geq 1,\ell\in\mathbb{Z}^+$ such that $g^\ell\in J$. It follows that $g^\ell(a)=0,\forall a\in Z(J)\Rightarrow g(a)=0,\forall a\in\mathcal{Z}(J)$ (see proof of 13.1.7) $\Rightarrow g\in\mathcal{I}(\mathcal{Z}(J))$ so that $\sqrt{J}\subset\mathcal{I}(\mathcal{Z}(J))\Rightarrow\sqrt{J}=\mathcal{I}(\mathcal{Z}(J))$. □

Let us now prove the "weak" Nullstellensatz. The "weak" Nullstellensatz says that if k is *algebraically closed*, then every maximal ideal $\mathcal{M}\subset k[x_1,\dots,x_n]$ is on the form $\mathcal{M}=(x_1-a_1,\dots,x_n-a_n)$.

Lemma 13.2.2. *(key lemma). Suppose k is algebraically closed and $\mathbb{E}/k$ is a field extension that is finitely generated as a k-algebra. Then $\mathbb{E}=k$.*

Proof of the "weak Nullstellensatz" assuming key lemma:

Proof. Suppose $\mathcal{M}\subset k[x_1,\dots,x_n]$ is maximal. Let $\mathbb{E}=k[x_1,\dots,x_n]/\mathcal{M}$. Note that the quotient is a field ($\mathcal{M}$ *maximal*), and it includes k ($\mathcal{M}$ can not include a unit $a\in k$ since then $a^{-1}a=1\in\mathcal{M}\Rightarrow\mathcal{M}=k[x_1,\dots,x_n]$, contradiction to the fact that $\mathcal{M}$ is maximal, hence *proper*). Also, we have that $k[x_1,\dots,x_n]$ is finitely generated as a k-algebra by $x_1,\dots,x_n$. Hence $\mathbb{E}=k[x_1,\dots,x_n]/\mathcal{M}$ is finitely generated by $x_1+\mathcal{M},\dots,x_n+\mathcal{M}\underbrace{\Rightarrow}_{\text{key lemma}}\mathbb{E}=k$.

We get a surjective homomorphism φ with kernel $\mathcal{M}$. This from the fact that we have a k-algebra isomorphism $\phi:k[x_1,\dots,x_n]/\mathcal{M}\to k$. Since $k[x_1,\dots,x_n]/\mathcal{M}$ is a finitely generated k-algebra, we also have a surjective k-algebra homomorphism $q:k[x_1,\dots,x_n]\twoheadrightarrow k[x_1,\dots,x_n]/\mathcal{M}$. Composing ϕ with q we get $\varphi=\phi\circ q$, which is clearly surjective. Furthermore, we note that $\varphi(p(x_1,\dots,x_n))=$

$q(p(x_1,\ldots,x_n)+\mathcal{M})$ so that $\mathcal{M}\subset ker(\varphi)$. We have that ϕ is injective, hence if $r(x_1,\ldots,x_n)\notin\mathcal{M}$ then $q(r(x_1,\ldots,x_n)+\mathcal{M})\neq 0\Rightarrow\varphi(r(x_1,\ldots,x_n))\neq 0$ which implies (we showed the contrapositive) that $r\in\ker(\varphi)\Rightarrow r\in\mathcal{M}\Rightarrow ker(\varphi)\subset\mathcal{M}\Rightarrow ker(\varphi)=\mathcal{M}$.

$$k[x_1,\ldots,x_n]\xrightarrow{\quad\varphi\quad}k$$

$$x_1\longmapsto a_1$$

$$\vdots\qquad\qquad\vdots$$

$$x_n\longmapsto a_n$$

If $m(x_1,\ldots,x_n)\in\mathcal{M}$ so that $m(x_1,\ldots,x_n)\in\ker(\varphi)=\mathcal{M}$ then $m(a_1,\ldots,a_n)=0\Rightarrow m\in I((a_1,\ldots,a_n))\underbrace{=}_{\text{example 13.0.3}}(x_1-a_1,\ldots,x_n-a_n)\Rightarrow\mathcal{M}\subset(x_1-a_1,\ldots,x_n-a_n)\underbrace{\Rightarrow}_{\text{maximality}}\mathcal{M}=(x_1-a_1,\ldots,x_n-a_n)$. We have used that $(x_1-a_1,\ldots,x_n-a_n)$ is a maximal ideal, hence a *proper* ideal. □

13.3 Sketch of proof of key lemma

To show that $\mathbb{E}=k$ it is enough to show that if $\mathbb{E}$ is finitely generated as a k-algebra, then $\mathbb{E}$ is *algebraic* over k. We can equivally show the contrapositive: If $\mathbb{E}$ is *not algebraic* over $k\Rightarrow\mathbb{E}$ is not finitely generated as a k-algebra.

Proof. If $\mathbb{E}$ is not algebraic then $\mathbb{E}$ contains a copy of $k(x)=\text{Frac}(k[x])$. Suppose $\mathbb{E}=k(x)$. Let´s prove that $\mathbb{E}$ is not finitely generated as a k-algebra.

Let $f_1(x),\ldots,f_m(x)\in k(x)$. We want to show that the algebra generated by $f_1(x),\ldots,f_m(x)$ is strictly smaller than $k(x)$. We can write $f_1(x)=\frac{p_1(x)}{q_1(x)},\ldots,f_m(x)=\frac{p_m(x)}{q_m(x)}$. Any polynomial expression in $\frac{p_i(x)}{q_i(x)}$ written as an *irreducible* fraction will have irreducible factors in the denominator that divide $q_1,\ldots,q_m$. Let $r(x)$ be an irreducible polynomial that is not a factor of $q_1,\ldots,q_m$. Then $\frac{1}{r(x)}\in k(x)$ is not in $k[f_1,\ldots,f_n]$. □

Excercise: Show that $\mathbb{Q}$ is not finitely generated as a $\mathbb{Z}$-algebra, that is, there does not exist a finite number of elements $\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\in\mathbb{Q}$ such that $\mathbb{Q}=\mathbb{Z}\left[\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right]$

Suggested solution: Assume to the contrary that $\mathbb{Z}\left[\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right]$. We can rewrite this as $\mathbb{Z}\left[\frac{1}{c}\right]$ where $c=\text{lcm}(q_1,\ldots,q_m)$. Take $\frac{1}{p}\in\mathbb{Q}$ for prime p that is not in the prime factorization of c. Then we must have $\frac{1}{p}=\frac{k}{c}\quad(k\in\mathbb{Z})\Leftrightarrow c=pk$, which is a contradiction, since then clearly p is a prime-factor in c. I believe this works. One could also show, I think, that $\frac{1}{2c}$ is not in $\mathbb{Z}\left[\frac{1}{c}\right]$ by the fact that then $\frac{1}{2c}=\frac{k}{c}\quad(k\in\mathbb{Z})\Leftrightarrow 2k=1$, which contradicts the fact that the only units in $\mathbb{Z}$ are $\{1,-1\}$, i.e. 2 is *not* a unit.

Source: https://math.stackexchange.com/questions/1076387/bbbq-is-not-a-finitely-generated-bbbz-module

Chapter 14

Fourteenth lecture

14.1 Localization

Recall: D integral domain $\rightsquigarrow \mathrm{Frac}(D) = \left\{\frac{x}{y}, x \in D, y \in D \setminus \{0\}\right\} = \underbrace{D \times (D \setminus \{0\})/\sim}_{x \longmapsto \frac{x}{1}}$ where

$$(x, y) \sim (x', y') \Leftrightarrow xy' = x'y.$$

$D \hookrightarrow \mathrm{Frac}(D)$ "smallest field" containing D.

Example 14.1.1. $\mathrm{Frac}(\mathbb{Z}) = \left\{\frac{x}{y}, x \in \mathbb{Z}, y \in \mathbb{Z} \setminus \{0\}\right\} = \mathbb{Q}$

This lecture: R arbitrary *unital, commutative* ring.

$S =$ set of denominators $R \to S^{-1}R$.

Also: M R-module $\rightsquigarrow M \to S^{-1}M$.

Localization of R in S.

14.2 Localization of rings

Definition 14.2.1. . $S \subset R$ is **multiplicative** if

1. $1 \in S$
2. $s, t \in S \Rightarrow st \in S$.

Example 14.2.2. D integral domain $\Rightarrow S = D \setminus \{0\}$.

Example 14.2.3. $\{1, f, f^2, f^3, \ldots\}$ for some $f \in R$.

Example 14.2.4. $P \subset R$ prime-ideal $\rightsquigarrow S = R \setminus \{P\}$ is multiplicative. This follows from the fact that since P is proper, $1 \notin P \Rightarrow 1 \in R \setminus \{P\}$. Furthermore, if $x, y \in R \setminus \{P\}$ then $xy \in R \setminus \{P\}$ since if $xy \in P$ then either $x \in P$ or $y \in P$, contrary to our assumption.

Example 14.2.5. Let $P_1, \ldots, P_n \subset R$ be prime ideals. Then $S = R \setminus (P_1 \cup \ldots \cup P_n)$. To show this, apply similar reasoning as in 14.2.4.

14.3 Construction of $S^{-1}R$

$S^{-1}R = (R \times S)/\sim$. To make $\sim$ transitive, we define $(r_1, s_1) \sim (r_2, s_2) \Leftrightarrow \exists s \in S : s(r_1 s_2 - r_2 s_1) = 0$. The $\exists$ part only needed when R not an integral domain (or $0 \in S$).

Claim: $\sim$ is an equivalence relation.

Proof.

reflexive: We want to show that $(r_1, s_1) \sim (r_1, s_1)$. Since $\exists 1 \in S$ it follows that $1 \cdot (r_1 s_1 - r_1 s_1) = 0$.

symmetric: If $(r_1, s_1) \sim (r_2, s_2) \Rightarrow \exists s \in S$ such that $s(r_1 s_2 - r_2 s_1) = 0 \Leftrightarrow s(r_1 s_2) = s(r_2 s_1) \Leftrightarrow s(r_2 s_1) - s(r_1 s_2) = s(r_2 s_1 - r_1 s_2) = 0$. We have used that $S \subset R$ so left-distributivity holds.

transitive: If $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$ then

- $\exists t_1 \in S \mid t_1(r_1 s_2 - r_2 s_1) = 0$
- $\exists t_2 \in S \mid t_2(r_2 s_3 - r_3 s_2) = 0$

Note that $s_1, s_2, s_3 \in S$. Furthermore, note that R is commutative. We find that $t_1 t_2 s_2 \in S$ (since S multiplicative so closed under multiplication) is such that

- $$\begin{aligned} t_1 t_2 s_2 (r_1 s_3) &= t_2 s_3 t_1 (r_1 s_2) \\ &= t_2 s_3 t_1 (r_2 s_1) \\ &= t_1 t_2 s_1 (r_2 s_3). \end{aligned}$$
- $$\begin{aligned} t_1 t_2 s_2 (r_3 s_1) &= t_1 t_2 s_1 (r_3 s_2) \\ &= t_1 s_1 t_2 (r_3 s_2) \\ &= t_1 s_1 t_2 (r_2 s_3) \\ &= t_1 t_2 s_1 (r_2 s_3). \end{aligned}$$

  Note: We have repeatedly used commutativity and associativity of R, together with the fact that $S \subset R$.

$\Rightarrow t_1 t_2 s_2 (r_1 s_3 - r_3 s_1) = 0 \Rightarrow (r_1, s_1) \sim (r_3, s_3)$. □

Notation: $\dfrac{r}{s} = [(r, s)]$.

Claim:

- $\dfrac{r_1}{s_1} + \dfrac{r_2}{s_2} = \dfrac{r_1 s_2 + r_2 s_1}{s_1 s_2}$

- $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 \cdot r_2}{s_1 \cdot s_2}$.
- $\frac{0}{1} = 0, \frac{1}{1} = 1$

Well-defined makes $S^{-1}R$ into a *commutative ring with unity.*

We get a ring homomorphism

$$R \xrightarrow{\pi} S^{-1}R$$

$$r \longmapsto \frac{r}{1}$$

14.4 Crucial observations

For all $s \in S$ we have that $\pi(s)$ is invertible. Note that $\left(\frac{s}{1}\right)^{-1} = \frac{1}{s} \in S^{-1}R$, so all elements $s \in S$ has an inverse in $S^{-1}R$.

Example 14.4.1. If D is an integral domain then $(D \setminus \{0\})^{-1}D = \mathrm{Frac}(D)$.

Example 14.4.2. $S = \{1, f, f^2, f^3, \ldots\}$ where $S^{-1}R$ is inverting f.

$R_f := S^{-1}R$ or $R\left[\frac{1}{f}\right] \cong R[z]/(zf - 1)$ (exc. 18 in [1]).

We have $z \mapsto \frac{1}{f}$ and $\frac{r}{f^n} \mapsto rz^n$.

Example 14.4.3. $S = R \setminus \{\mathfrak{p}\}$. $R_{\mathfrak{p}} := S^{-1}R$ "localizing at $\mathfrak{p}$" for prime ideal $\mathfrak{p}$.

Example 14.4.4. $\mathbb{Z}\left[\frac{1}{3}\right] = \left\{\frac{d}{3^n} \ : \ d \in \mathbb{Z}, n \geq 0\right\} \subset \mathbb{Q} \rightsquigarrow \mathbb{Z}_{(3)} = \left\{\frac{d}{e} \ : \ d, e \in \mathbb{Z}, 3 \not| \, e\right\} \subset \mathbb{Q}$.

Example 14.4.5. $R = k[x]$ then

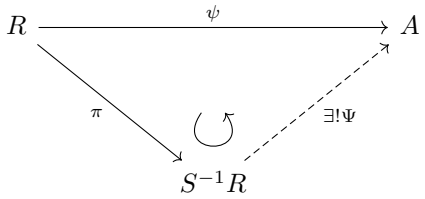
$$\begin{aligned} R_x &= R\left[\frac{1}{x}\right] \\ &= \left\{\frac{f(x)}{x^n}\right\} \\ &= \left\{\varphi(x) = \frac{f(x)}{g(x)}, \ g(x) \ \text{ allowed to have poles at } x = 0 \text{ but nowhere else}\right\}. \end{aligned}$$

$R_{(x)} = \left\{\varphi(x) = \frac{f(x)}{g(x)} \ : \ g(0) \neq 0\right\}$.

$R_{x(x-1)(x-\pi)}$ allow poles in $x = 0, x = 1$ and $x = \pi$.

14.5 Universal property of $S^{-1}R$

Theorem 14.5.1. *(Universal property of $S^{-1}R$). If $R \xrightarrow{\psi} A$ is a ring homomorphism such that $\psi(s)$ is invertible for all $s \in S$, then $\exists!$ ring homomorphism $\Psi : S^{-1}R \to A$ such that $\psi = \Psi \circ \pi$*



Note: Compare with $R \to R/I$, universal map which kills I.

Proof. (Uniqueness). Suppose Ψ exists.

- $$\begin{aligned}\Psi\left(\frac{r}{1}\right) &= \Psi(\pi(r)) \\ &= \psi(r).\end{aligned}$$

- $$\begin{aligned}\Psi\left(\frac{1}{s}\right) &= \Psi(\pi(s)^{-1}) \\ &= (\Psi(\pi(s)))^{-1} \\ &= (\psi(s))^{-1} \qquad (\text{since } \Psi(r/1) = \psi(r) \text{ for all } r \in R) \\ \Rightarrow \Psi\left(\frac{r}{s}\right) &= \Psi\left(\frac{r}{1} \cdot \frac{1}{s}\right) \\ &= \Psi\left(\frac{r}{1}\right) \cdot \Psi\left(\frac{1}{s}\right) \\ &= \psi(r) \cdot (\psi(s))^{-1}.\end{aligned}$$

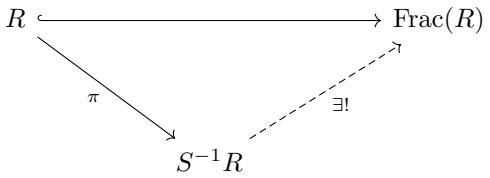
Hence uniquely determined by the ring homomorphism ψ.

□

Proof. (Existence). Show that $\Psi\left(\frac{r}{s}\right) = \psi(r) \cdot (\psi(s))^{-1}$ is well-defined and a ring-homomorphism. Let $\frac{r}{s} = \frac{r'}{s'} \Rightarrow \exists s'' \in S \ : \ s''(rs' - r's) = 0$. Prove that $\psi(r) \cdot (\psi(s))^{-1}) = \psi(r') \cdot (\psi(s'))^{-1}$ (some work needed).

□

It is not always true that $R \to S^{-1}R$ is *injective*. If R is an integral domain and $S \subset R \setminus \{0\}$ then



$\Rightarrow \pi$ is injective (and Ψ injective, where $S^{-1}R$ is an integral domain).

In general, corollary 15.37 in [1] gives $ker(R \to S^{-1}R) = \{r \in R \ : \ sr = 0, \text{for some } s \in S\}$.

Proof. $r \in ker(R \to S^{-1}R) \Rightarrow \exists s \in S$ such that $sr = 0 \Leftrightarrow s(r \cdot 1 - 0 \cdot 1) = 0 \Leftrightarrow (r, 1) \sim (0, 1) \Leftrightarrow \exists s \in S \ : \ sr = 0.$ □

Example 14.5.2.

$$\begin{aligned} R &= k[x, y]/(xy) \\ \rightsquigarrow R_x &= R\left[\frac{1}{x}\right] \\ &= k[x, y, z]/(xy, zx - 1) \\ &= k[x, y, z]/(y, zx - 1). \end{aligned}$$

$$\begin{aligned} xy &= 0 \\ \Rightarrow zxy &= 0 \\ &= y \end{aligned}$$

since $zx \equiv 1 + (xy, zx - 1)$. Furthermore, we have

$$\begin{aligned} k[x, y, z]/(y, zx - 1) &\cong k[x, z]/(zx - 1) \\ &= k\left[x, \frac{1}{x}\right] \\ &= k[x]_{(x)}. \end{aligned}$$

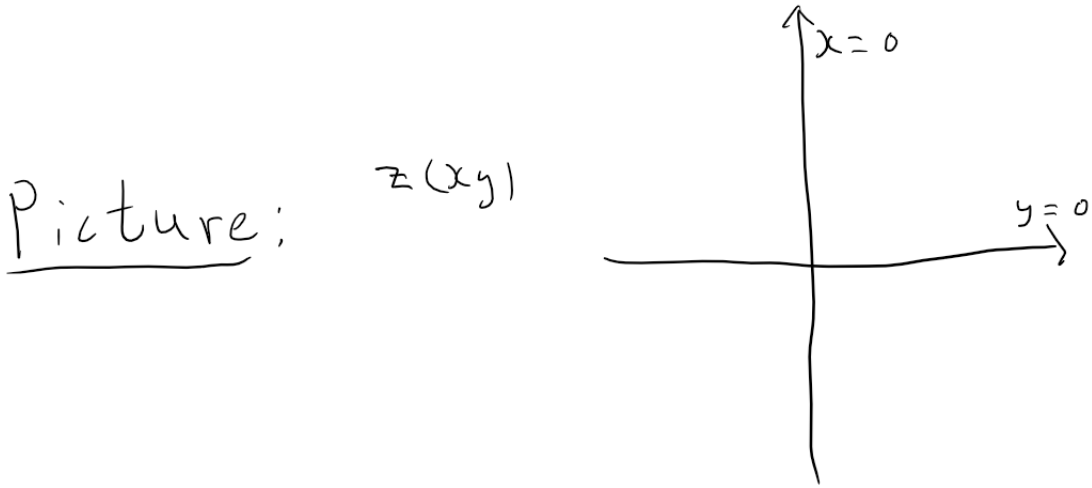


Figure 14.1: Example 14.5.2

Introducing $\dfrac{1}{x} \Leftrightarrow$ allowing poles along $x = 0$.

$k[V]\left[\frac{1}{x}\right]$ = functions on $V \setminus \{x = 0\}$. So $ker(R \to R_{(x)}) = (y)$.

14.6 Local Rings

Definition 14.6.1. . A unital commutative ring is a **local ring** if there exists a *unique maximal ideal* $\mathcal{M}$.

Proposition 14.6.2. *If R is* local *with maximal ideal $\mathcal{M}$ then*

$$\begin{aligned} R \setminus \mathcal{M} &= R^\times \\ &= \{r \in R \mid r \text{ invertible}\}. \end{aligned}$$

We have $R = M \coprod R^\times$.

Furthermore, if $R \setminus R^\times$ is an ideal, then R is local with maximal ideal $\mathcal{M} = R \setminus R^\times$.

Remark 14.6.3. $r \in R^\times \Leftrightarrow (r) = R$ so $I \subsetneq R \Leftrightarrow I \cap R^\times = \varnothing$.

Proof. If $r \notin R^\times$ then $(r) \subsetneq R \Rightarrow \exists \mathcal{M}'$ (maximal ideal) so that $(r) \subset \mathcal{M}'$ is *maximal* (Zorn:s lemma) $\Rightarrow R$ local gives $\mathcal{M} = \mathcal{M}' \Rightarrow r \in \mathcal{M} \Rightarrow R \setminus R^\times \subset \mathcal{M}$ and always true that $M \subset R \setminus R^\times \Rightarrow \mathcal{M} = R \setminus R^\times$. □

Fact: $\mathfrak{p} \subset R$ prime ideal, then $R_\mathfrak{p}$ is a *local ring* (14.6.1) with maximal ideal $\mathfrak{p}R_\mathfrak{p} := \pi(\mathfrak{p})R_\mathfrak{p}$.

Geometric picture: Let $k[U]$ coordinate ring = functions on U. Max ideals = points on U. $k[V]_\mathcal{M}$ = functions allowing poles except at points corresponding to $\mathcal{M}$. Local ring with unique maximal ideal: $\mathcal{M}k[V]_\mathcal{M}$. Functions defined on points corresponding to $\mathcal{M}$. R local with *maxmial ideal* $\mathcal{M}$.

We have ev : $R \to R/M$ = field and ev(r) = value of "function" r at point corresponding to $\mathcal{M}$.

14.7 Localization and Ideals

Let $f : A \to B$ be a ring homomorphism.

$$\left\{\text{Ideals of } I \subset A\right\} \underset{c}{\overset{e}{\rightleftarrows}} \left\{\text{Ideals of } J \subset B.\right\}$$

We have

$$\begin{aligned} I \longmapsto I^e &:= f(I)B \\ &= IB \end{aligned}$$

where IB is the ideal of B generated by $f(I)$ (**extension** of I), that is, $f(I)B = \langle f(I) \rangle \subset B$.

$J^c := f^{-1}(J) \longmapsto J$ (**contraction** of J).

Note: The preimage under a ring-homomorphism is an ideal.

Fact: $I \subset (I^e)^c$ and $J \supset (J^c)^e$.

Example 14.7.1. $f : R \to R/K$. $(I)^e = f(I)$ already an ideal and $(J^e)^c = J$.

$$\left\{\begin{matrix}\text{Ideals of } I \subset A \\ K \subset I\end{matrix}\right\} \underset{c}{\overset{e}{\longleftrightarrow}} \left\{\text{Ideals } J \subset A/K.\right\} \qquad \text{bijection!}$$

Example 14.7.2. $\pi : R \to S^{-1}R$.

Proposition 14.7.3 (15.3.8)**.**

(1)

$$\begin{aligned}(I^e)^c &= \mathrm{Sat}(I) \\ &= \{r \in R \ : \ \exists s \in S \text{ so that } sr \in I\}\end{aligned}$$

(2)

$$\left\{\begin{matrix}I \subset R \\ I = \mathrm{Sat}(I)\end{matrix}\right\} \underset{\text{bijective}}{\longleftrightarrow} \left\{J \subset S^{-1}R.\right\}$$

(3) $\mathfrak{p} = \mathrm{Sat}(\mathfrak{p}) \Leftrightarrow \mathfrak{p} \cap S = \varnothing$ *(where* $\mathfrak{p}$ *is prime).*

(4)

$$\left\{\begin{matrix}\mathfrak{p} \subset R \\ \mathfrak{p} \text{ prime}\end{matrix}\right\} \underset{\text{bijective}}{\longleftrightarrow} \left\{\begin{matrix}\mathfrak{q} \subset S^{-1}R \\ \text{prime ideal.}\end{matrix}\right\}$$

Example 14.7.4. $\mathbb{Z} \to \mathbb{Z}\left[\frac{1}{3}\right]$.

$I = (24) \mapsto I^e = (24) = (8) \mapsto (I^e)^c = (8)$.

$$\begin{aligned}\mathrm{Sat}(24) &= \{d \in \mathbb{Z} \ : \ \exists n \geq 0, (3^n)d \in (24)\} \\ &= (8).\end{aligned}$$

14.8 Localization of modules

Let M be an R-module and let $S \subset R$ be a *multiplicative* set. We have $S^{-1}M := (M \times S)/\sim$ where $(m_1, s_1) \sim (m_2, s_2) \Leftrightarrow \exists s \in S \mid s(m_1 \cdot s_2 - m_2 \cdot s_1) = 0$. We thus have equivalence-classes $m/s := [(m, s)]$.

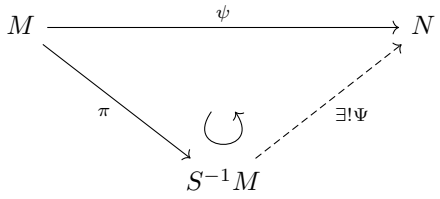
Fact: $S^{-1}M$ is an $S^{-1}R$-module, where $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{m_1 s_2 + m_2 s_1}{s_1 s_2}$ and $\frac{r}{s} \cdot \frac{m}{t} = \frac{rm}{st}$. We have a map

$$M \xrightarrow{\ \pi\ } S^{-1}M$$

$$m \longmapsto m/1$$

14.8.1 Universal Property

$\forall$ R-modules N and $\psi : M \to N$ such that $\forall s \in S \ s : N \to N$ (multiplication by S) is *bijective*, then $\Psi : S^{-1}M \to N$ **exists** and is *unique*. Hence the following diagram



Proposition 14.8.1 (15.41, key fact)**.** ∃ *canonical isomorphism of* $S^{-1}R$*-modules* $S^{-1}M$

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

$$m/s \longmapsto m \otimes 1/s$$

$$\sum \tfrac{r_i m_i}{s_i} \longmapsfrom \sum (m_i \otimes (r_i/s_i))$$

Proposition 14.8.2 (15.42.(6))**.** *Let* $S^{-1}R$ *be a* flat *R-module, given by*

$$\begin{aligned} &0 \to K \to M \to N \to 0 \\ \Rightarrow &0 \to \underbrace{K \otimes_R S^{-1}R}_{= S^{-1}K} \to \underbrace{M \otimes_R S^{-1}R}_{= S^{-1}M} \to \underbrace{N \otimes_R S^{-1}R}_{= S^{-1}N} \to 0. \end{aligned}$$

That is, $S^{-1}(-)$ *is an* ***exact*** *functor.*

Proposition 14.8.3 (15.47)**.** *Let* M *be an* R*-module, then the following are equivalent:*

(1) $M = 0$

(2)

$$\begin{aligned} M_{\mathfrak{p}} &:= (R - \mathfrak{p})^{-1}M \\ &= 0 \quad (\textit{where } \mathfrak{p} \textit{ is a } \text{prime } \textit{ideal in } R). \end{aligned}$$

(3) $M_{\mathfrak{m}} = 0$ (*where* $\mathfrak{m}$ *is a* maximal *ideal in* R).

Proposition 14.8.4. *Let* $\varphi : M \to N$ *be an* R*-module homomorphism. Then the following are equivalent:*

(1) φ *injective/surjective/bijective.*

(2) $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ *injective/surjective/bijective, where* $\mathfrak{p}$ *is a* prime ideal *in* R.

(3) $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ *injective/surjective/bijective, where* $\mathfrak{m}$ *is a* maximal ideal *in* R.

Chapter 15

Fifteenth lecture (bonus lecture, not on exam)

Suppose k is an algebraically closed field. Then there is a correspondence

$$\left\{\textbf{radical} \text{ ideals of } k[x_1,\ldots,x_n]\right\} \longleftrightarrow \left\{\textbf{algebraic} \text{ subsets of } \mathbb{A}^n\right\}$$

$$J \longmapsto \mathcal{Z}(J)$$

$$\mathcal{I}(S) \longmapsfrom S$$

Finitely generated k-algebras without nilpotents $k[S] = k[x_1,\ldots,x_n]/\mathcal{I}(S)$.

$$\text{Algebraic properties} \longleftrightarrow \text{Geometric properties.}$$

$$\text{Maximal ideals} \longleftrightarrow \text{Points.}$$

$$\underbrace{k\text{-algebra homomorphisms}}_{k[U],\ k[V]} \cong \text{polynomial functions(U,V).}$$

Ring = commutative ring with 1. Ring homomorphisms preserve 1.

Question 15.0.1. Is every ring R the **ring of functions** for some **geometric** object?

Answer: Yes, sort of.

Lemma 15.0.2. *Suppose R, S are finitely generated k-algebras and $f : R \to S$ is a k-algebra homomorphism, and $\mathcal{M} \subset S$ is a maximal ideal, then $f^{-1}(\mathcal{M}) \subset R$ is maximal (maximality preserved under pre-images).*

But for general ring-homomorphisms $f : R \to S$ we have that $f^{-1}(\mathfrak{p})$ is prime if $\mathfrak{p}$ is prime and $f^{-1}(\mathcal{M})$ is prime if $\mathcal{M}$ is maximal (every maximal ideal is a prime ideal).

Definition 15.0.3. Let R be a ring. The **spectrum** (also known as the "prime spectrum" or "$\mathcal{Z}$ariski spectrum" of a ring) of R is the set $\mathrm{Spec}(R)$ of *prime* ideals of R. T

The **maximal spectrum** of R is $\mathfrak{m}\,\mathrm{Spec}(R) = \{\text{maximal ideals}\}$.

There are functions

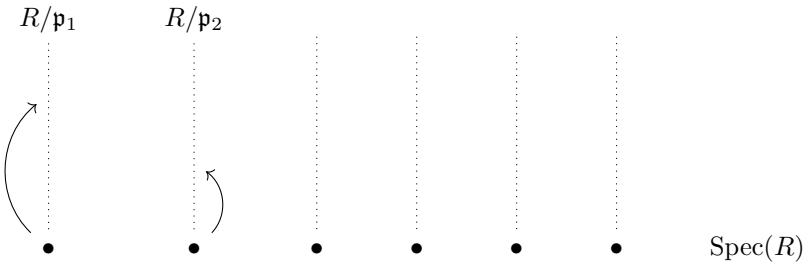
$$\text{Ideals of R} \longrightarrow \text{Subsets of Spec}(R)$$

$$J \longmapsto \mathcal{Z}(J) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid J \subset \mathfrak{p}\}$$

$$\mathcal{I}(S) = \bigcap_{\mathfrak{p} \in S} \mathfrak{p} \longmapsfrom S$$

Observations:

- $\mathcal{Z}(J_1) \cup \mathcal{Z}(J_2) = \mathcal{Z}(J_1 \cdot J_2)$.
- $\bigcap_{\alpha} \mathcal{Z}(J_\alpha) = \mathcal{Z}(+_\alpha J_\alpha)$.
- $\mathrm{Spec}(R) = \mathcal{Z}(0)$, $\varnothing = \mathcal{Z}(R) \Rightarrow$ subsets of $\mathrm{Spec}(R)$ of the form $\mathcal{Z}(J)$ form the **closed** sets in a topology on $\mathrm{Spec}(R)$. The "Zariski topology".
- Every element $x \in R$ defines a "function" $\mathfrak{p} \mapsto x + \mathfrak{p} = x \bmod \mathfrak{p}$ in $R/\mathfrak{p}$. We get $\mathrm{Spec}(R) \to \coprod_{\mathfrak{p} \in \mathrm{Spec}(R)} R/\mathfrak{p}$.



- $x(\mathfrak{p}) = x + \mathfrak{p}$
- $x(\mathfrak{p}) = 0 \Leftrightarrow x \in \mathfrak{p}$
- $x^{-1}(0) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid (x) \subset \mathfrak{p}\}$

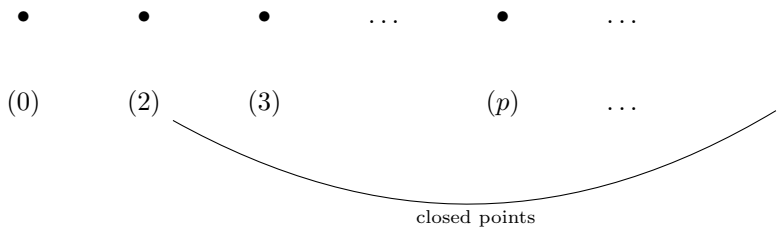
Example 15.0.4.

1. Let k be a field, then $\mathrm{Spec}(k) = \{(0)\}$ (one-point space).
2. $\mathbb{Z}$, then $\mathrm{Spec}(\mathbb{Z})$ consists of $(0), (2), (3) \ldots, (p), \ldots$. I.e. (0) and all prime ideals (p) for prime $p \in \mathbb{Z}$.

   $\mathcal{Z}(n) := \{(p) \in \mathrm{Spec}(\mathbb{Z}) \mid p \mid n\}$ (assuming $n \neq 0$).

$\mathcal{Z}(0) = \mathrm{Spec}(\mathbb{Z})$.

$\Rightarrow$ closed sets in $\mathrm{Spec}(\mathbb{Z})$ are the **finite** subsets and $\mathrm{Spec}(\mathbb{Z})$.



Example 15.0.5. $\overline{\{(0)\}} = \mathrm{Spec}(R)$. (0) is a **generic** point. Let R be a P.I.D., then $\{(0), (p_1), \ldots, (p_i), \ldots\}$ is a set of irreducible elements.

$k[x] \rightsquigarrow \mathrm{Spec}(k[x]) = \{\text{Monic irreducible } f(x) \in k[x]\} \cup \{(0)\}$.

If k is *algebraically closed* we have a bijection $\mathrm{Spec}(k[x]) \cong k \cup \{(0)\}$.

Example 15.0.6. $k[x, y]$ with k *algebraically closed.*

$$\begin{cases} (0) \\ (f(x,y)) & (f(x,y) \text{ irreducible in } k[x,y]) \\ \underbrace{(x-a, y-b)}_{\text{closed points}} & ((a,b) \in \mathbb{A}^2) \end{cases}$$

- $\mathfrak{m}\,\mathrm{Spec}(R) \subset \mathrm{Spec}(R)$
- $\mathfrak{m}\,\mathrm{Spec}(k[x,y]) \subset \mathrm{Spec}(k[x,y])$. Note that when k is algebraically closed, the maximal ideals of $k[x,y]$ is in bijective correspondence with points $(a,b) \in \mathbb{A}^2$ (that is, for every point we get a maximal ideal $\mathfrak{m}$, and for every ideal $\mathfrak{m}$ we get a corresponding point $(a,b) \in \mathbb{A}^2$).

A ring-homomorphism $f : R \to S$ induces a function $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ by $f^*(\mathfrak{p}) = f^{-1}(\mathfrak{p})$. In fact, it is a **continuous** function. We find that $\mathrm{Spec}(-)$ is a **contravariant** functor.

Rings $\to$ Topological spaces.

Comment 15.0.7. $\mathrm{Spec}(-) : \mathbf{CRing} \to \mathbf{AffSch}$, that is, a (contravariant) functor from the category of commutative rings, to the category of affine schemes. That is, it is the same as $\mathrm{Spec}(-) : \mathbf{CRing}^{\mathrm{op}} \to \mathbf{AffSch}$.

Example 15.0.8.

$$\mathbb{C}[x] \longrightarrow \mathbb{C}[x,y]$$

$$x \longmapsto x$$

$\rightsquigarrow i^* : \mathrm{Spec}(\mathbb{C}[x,y]) \to \mathrm{Spec}(\mathbb{C}[x])$ defined explicitly by $\mathfrak{p} \mapsto \mathfrak{p} \cap \mathbb{C}[x]$, where $(0) \mapsto (0)$. Furthermore, we have that $i^*(x-a, y-b) = (x-a)$.

- $(f(x,y)) \longmapsto \begin{cases} (0), \text{ if } f(x,y) \text{ depends on } y. \\ (f(x,-)), \text{ if } f(x,y) = f(x) \quad (\text{independent of } y). \end{cases}$

15.0.1 Open subsets of $\mathrm{Spec}(R)$

Let J be an ideal in a commutative ring R. Then $\mathrm{Spec}(R)_J := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid J \not\subset \mathfrak{p}\}$ are the **open** subsets of $\mathrm{Spec}(R)$.

- $\mathrm{Spec}(R)_{J_1} \cup \mathrm{Spec}(R)_{J_2} = \mathrm{Spec}(R)_{J_1+J_2}$
- $\mathrm{Spec}(R)_{J_1} \cap \mathrm{Spec}(R)_{J_2} = \mathrm{Spec}(R)_{J_1 \cdot J_2}$
- Principal open subsets of $\mathrm{Spec}(R)$:

  Sets of the form $\mathrm{Spec}(R)_{(f)} := \{(\mathfrak{p} \in \mathrm{Spec}(R) \mid f \notin \mathfrak{p}\} \quad (f \in R)$.

  These sets form a **basis** for the Zariski-topology on $\mathrm{Spec}(R)$.

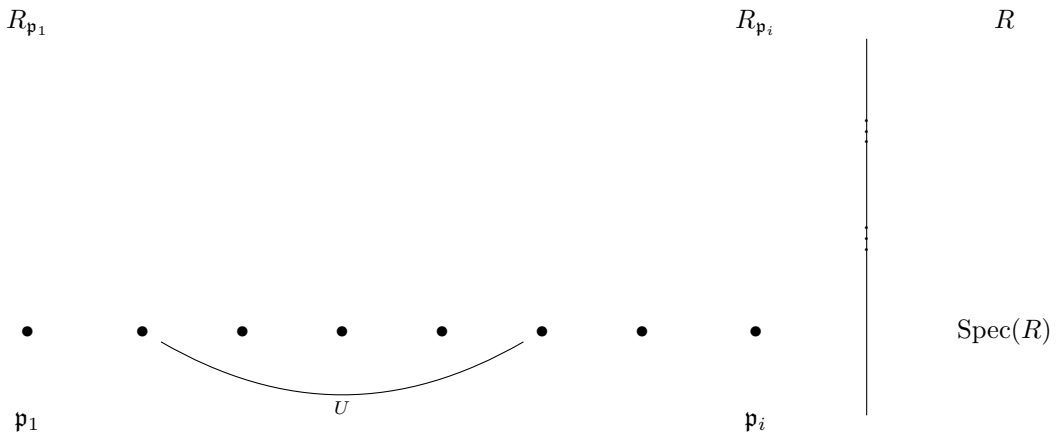
  Note: The intersection of basic open sets is again a basic open set since $\mathrm{Spec}(R)_{(f)} \cap \mathrm{Spec}(R)_{(g)} = \mathrm{Spec}(R)_{(f \cdot g)}$.

To a ring R, one associates the following "Space of rings"

$\coprod_{\mathfrak{p} \in \mathrm{Spec}(R)} R_{\mathfrak{p}}$ where $R_{\mathfrak{p}} = \{\frac{x}{y} \mid x, y \in R, y \in \mathfrak{p}\}$. Maps naturally into $\mathrm{Spec}(R)$.

We endow $\amalg R_{\mathfrak{p}}$ with a topology by defining a basis: For any basic set $\mathrm{Spec}(R)_{(f)}$, we have a homomorphism $\varphi_{\mathfrak{p}} : R_{(f)} \to R_{\mathfrak{p}}$, $\forall \mathfrak{p} \in \mathrm{Spec}(R)_{(f)}$.

The sets $\{\varphi_{\mathfrak{p}}(x) \mid \mathfrak{p} \in \mathrm{Spec}(R)\}$ form a basis for a topology on $\amalg_{\mathfrak{p} \in \mathrm{Spec}(R)}$



Scheme $\mathrm{Aff}(R)$.

Bibliography

[1] David Steven Dummit and Richard M. Foote. *Abstract algebra*. 3rd. Wiley; Sons, 2004.

Appendices

Appendix A

Exercise Session 1

- Recap: R ring. An R-module M is an abelian group with an action

$$R \times M \to M \quad \text{(with some axioms)}.$$

Example A.1.

(1) R is a module over itself

(2) An $\mathbb{F}$-module where $\mathbb{F}$ is a *field* is a *vector space*.

(3) *Any* abelian group is $\mathbb{Z}$-module.

For (1) we have that submodules = Ideals $I \subset R$.

For (2) we have that submodules = sub(vector)spaces.

For (3) we have that submodules = subgroups.

$\varphi : M \to N$ is an R-module homomorphism *if*

$$\varphi(r \cdot x) = r \cdot \varphi(x) \quad \text{(and } \varphi \text{ is a group homomorphism)}$$

In (3) $\mathbb{Z}$-module homomorphism are just group homomorphisms.

In (2) $\mathbb{F}$-module homomorphisms are $\mathbb{F}$-linear maps.

Note: R-module homomorphisms $R \to R \neq$ ring-homomorphisms.

Example A.2.

1. $R := \mathbb{F}[x]$.

   If we look at
   $$\varphi(f(x)) = f(x^2)$$
   then we have that
   $$\varphi(x) = x^2$$
   but
   $$x\varphi(1) = x \cdot 1.$$

$$M \cong \mathrm{Hom}_R(R, M)$$

as R-modules.

$$R \times \mathrm{Hom}_R(R, M) \to \mathrm{Hom}_R(R, M)$$

defined explicitly by

$$r \cdot \varphi(s) = \varphi(sr) \quad (\forall s \in R).$$

We define the map

$$\psi : M \to \mathrm{Hom}_R(R, M)$$

which is defined explicitly by the mapping

$$m \mapsto (r \mapsto rm).$$

R-linear:

$$\psi(rm)(s) = srm$$
$$r \cdot \psi(m)(s) = \psi(m)(sr) = srm.$$

We define the map

$$\theta : \mathrm{Hom}_R(R, M) \to M$$

by the explicit mapping

$$\varphi \to \varphi(1) \quad \text{(Evaluation at } \ 1)$$

for $\varphi \in \mathrm{Hom}_R(R, M)$.

We see that

$$\varphi : r \mapsto \varphi(r) = r \cdot \varphi(1)$$

since a map $\varphi \in \mathrm{Hom}_R(R, M)$ is R-linear, as $\mathrm{Hom}_R(R, M)$ is the group of R-module homomorphisms from R to M.

It follows that

$$\theta(r \cdot \varphi) = (r \cdot \varphi)(1) = \varphi(r) = r \cdot \varphi(1)$$

and that

$$r \cdot \theta(\varphi) = r \cdot \varphi(1)$$

so that θ is R-linear.

From this, we have that

$$\begin{cases} (\theta \circ \psi)(m) = \theta(r \mapsto rm) = m \\ (\psi \circ \theta)(\varphi) = \psi(\varphi(1)) = r \mapsto r\varphi(1) = r \mapsto \varphi(r) = \varphi \end{cases}$$

so that

$$\begin{cases} \theta \circ \psi = 1_M \\ \psi \circ \theta = 1_{\mathrm{Hom}_R(R,M)}. \end{cases}$$

Appendix B

Exercise Session 2

M is free if there *exists* $\mathcal{B} \subset M$ such that $\mathcal{B}$ generates M

$$m = \sum_{i=1}^{n} r_i b_i, \quad (\forall m \in M, r_i \in R, b_i \in \mathcal{B})$$

and $\mathcal{B}$ is linearly independent;

$$0 = \sum r_j b_j \Rightarrow r_j = 0$$

Infinite direct products of *free* modules need *not* be free.

Example B.1. Let

$$M := \prod_{i \in \mathbb{Z}^+} \mathbb{Z} = \{(a_n) \mid a_n \in \mathbb{Z}\} \quad (\text{M is } \textit{uncountable})$$

be considered as a $\mathbb{Z}$-module, and

$$N := \bigoplus_{i \in \mathbb{Z}^+} \mathbb{Z} \subset M$$

where N is countable.

Lemma B.2. *Let A be a free $\mathbb{Z}$-module $0 \neq a \in A$. Then*

$$\{k \in \mathbb{Z} \mid a = kb \text{ for some } b \in A\}$$

is finite.

Proof. Let $\mathcal{L} \subset A$ be a *basis*. Then

$$\exists!(r_i \in \mathbb{Z}, \ell_i \in \mathcal{L}) : a = \sum_{i=1}^{n} r_i \ell_i$$

$$\begin{aligned} &\rightsquigarrow a = kb \\ &\qquad = \sum_{i=1}^{m} k\tilde{r}_i \tilde{\ell}_i \\ &\Rightarrow k\tilde{r}_i = r_i \end{aligned}$$

$$\{k \in \mathbb{Z} \mid a = kb\} = \{k \in \mathbb{Z} \mid k \text{ divides } r_i \quad \forall i\}$$

If $(a_i) \in M$ then

$$\{k \in \mathbb{Z} \mid k|(a_i)\} \subset \{k \in \mathbb{Z} \mid k \text{ divides } a_j \text{ for some } j \in \mathbb{Z}^+\}$$

is **finite**. □

Assume M has a basis $\mathcal{B}$.

(a) N is countable. Has basis $\{e_i \mid i \in \mathbb{Z}^+\}$.

(b) **Claim**: There exists a set N_1, such that $N \subset N_1 \subset M$ and N_1 is generated by a countable subset $\mathcal{B}_1 \subset \mathcal{B}$.

Proof. For each i we can present e_i as a finite linear combination of elements of $\mathcal{B}$, as follows

$$e_i = \sum_j r_{ij} b_{ij}$$

Define $\mathcal{B}_1$ to be the set of all $\{b_{ij}\}$ that occur in the presentations of e_i in terms of elements of $\mathcal{B}$. $\mathcal{B}_1$ is a countable union of finite sets, and therefore is countable. Let $N_1 \subset M$ be the subset generated by $\mathcal{B}_1$

It follows from the construction that $N \subset N_1$. Furthermore, $\mathcal{B}_1$ is a subset of $\mathcal{B}$ and therefore is linearly independent. It follows that there is an isomorphism

$$N_1 = \bigoplus_{b_i \in \mathcal{B}_1} \mathbb{Z} \cdot b_i$$

and N_1 is countable. □

(c) Consider

$$\overline{M} := M/N_1.$$

Since N_1 is a submodule of M generated by a subset of our chosen basis $\mathcal{B}$, $\overline{M}$ is also free, with basis $\mathcal{B}_2 = \mathcal{B} \setminus \mathcal{B}_1$.

(d) Consider

$$\mathfrak{S} = \{(a_i \cdot i!) \mid (a_i) \in M\}$$

$\mathfrak{S}$ is clearly an uncountable set, and therefore there exists an element $s \in \mathfrak{S} \setminus \mathfrak{S} \cap N_1$. Let $\bar{s}$ be the image of s in $\overline{M}$.

Claim: $\bar{s} \in \overline{M}$ is a non-zero element that is divisible by every $k \in \mathbb{Z}$.

Proof.

$$\begin{aligned}
\bar{s} &= \overline{(a_i \cdot i!)} \\
&= \underbrace{(a_1 \cdot 1!, a_2 \cdot 2!, \ldots, a_{(k-1)} \cdot (k-1)!, 0, \ldots)}_{\in N \subset N_1} + (0, \ldots, 0, a_k \cdot k!, a_{(k+1)} \cdot (k+1)!, \ldots) \\
&= (0, \ldots, 0, a_k \cdot k!, a_{k+1} \cdot (k+1)!, \ldots) \qquad (k \mid (k+i)!)
\end{aligned}$$

is divisible by k. Contradicts lemma above; M can *not* be *free*. □

Appendix C

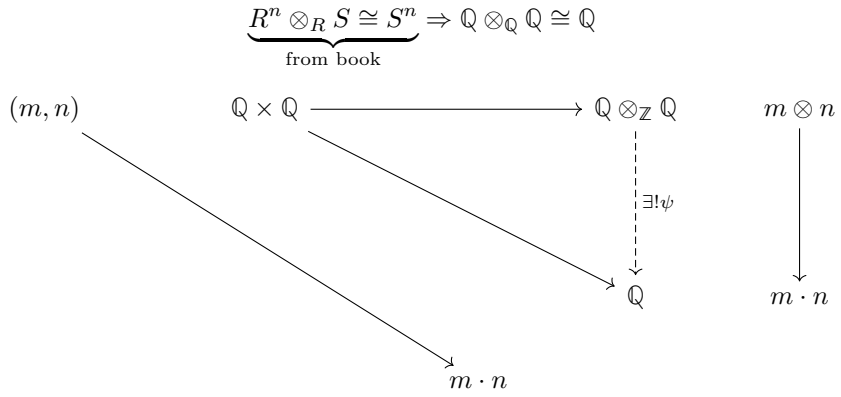
Exercise Session 3

10.4.4: Show that

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$$

as $\mathbb{Q}$-modules.

Claim C.1. Both isomorphic to $\mathbb{Q}$.



Show that ψ is a bijection.

Surjective: $m \in \mathbb{Q}$: $\psi(m \otimes 1) = m$.

Injective: Suppose that

$$\psi\Big(\sum_{\text{finite}} r_i \otimes s_i\Big) = \sum_i r_i s_i = 0$$

$$r_i = \frac{p_i}{q_i} \quad (p_i, q_i \in \mathbb{Z}).$$

Define

$$q = \operatorname{lcm}\{q_i\}_{i \in I}. \quad (I \text{ finite})$$

Then

$$q \cdot r_i \in \mathbb{Z} \quad (\forall i \in I).$$

$$\begin{aligned}
\sum_i r_i \otimes s_i &= \frac{1}{q}\sum_i (qr_i)\otimes s_i \\
&= \frac{1}{q}\sum_i (1 \otimes qr_i s_i) \\
&= \frac{1}{q}\left(1 \otimes q\sum_i \underbrace{r_i s_i}_{=\,0}\right) \\
&= \frac{1}{q}\underbrace{(1\otimes q\cdot 0)}_{=\,0} \\
&= \frac{1}{q}\cdot 0 \\
&= 0.
\end{aligned}$$

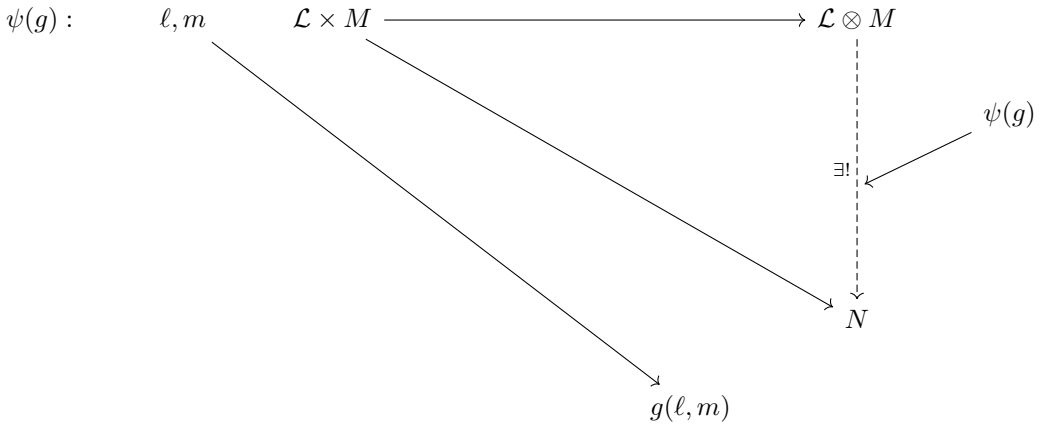
Theorem C.2 (Theorem 43)**.** *Let R be a commutative ring and let $\mathcal{L}, M, N$ be R-modules. Then*

$$\mathrm{Hom}_R(\mathcal{L}\otimes_R M, N) \cong \mathrm{Hom}_R(\mathcal{L}, \mathrm{Hom}_R(M,N)).$$

Proof.

$$\phi \to \cdots \to \psi \cdots \leftarrow$$

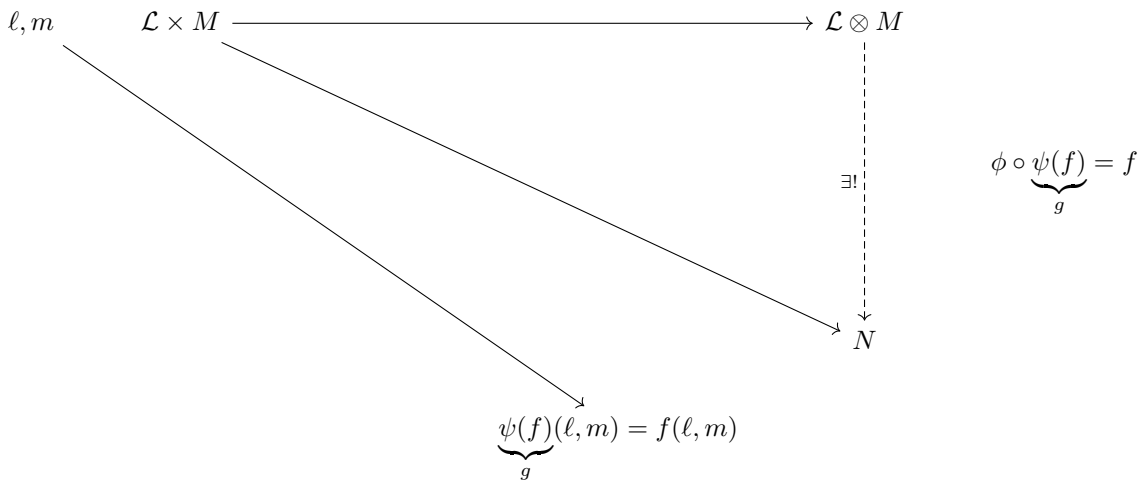
$$\phi(f)(\ell)(m) = f(\ell\otimes m) \quad \text{(check } R\text{-linear)}$$



$$\psi\circ\phi = \mathrm{id}$$

$$\phi\circ\psi = \mathrm{id}$$

$$\psi\circ\phi(f) = f \quad (?)$$

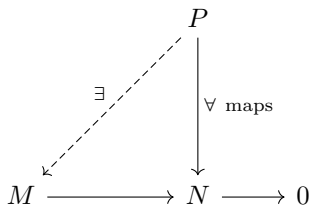


Because they both make the diagram commute (?). □

Appendix D

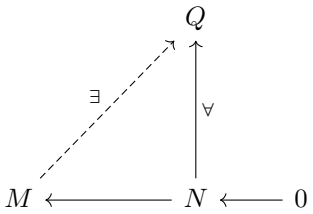
Exercise session 4

D.1 Projective modules



s.t. diagram commutes

D.2 Injective modules



such that diagram commutes

- P **projective** $\Leftrightarrow \exists$ free module $\mathcal{F}$ such that $\mathcal{F} \cong P \oplus K$.
- *Every* module is a quotient of a projective module.

Baer's Criterion (Prop. 36(1) in [1]):

Let Q be an R-module, then

$$Q \text{ injective } \Leftrightarrow \forall \text{left ideals } I \hookrightarrow R \text{ we have}$$

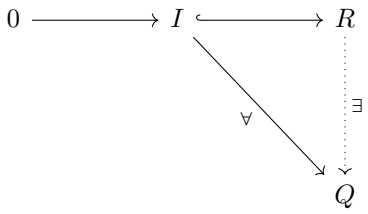


diagram commutes

Proof. See book. □

- *Every* module **embeds**[1] into an **injective** module (10.5.15 + 10.5.16 in [1] shows this).

Definition D.1. Let R be an integral domain. Then we have that an R-module M is **divisible** if

$$\forall r \in R \setminus \{0\} : rM = M$$

Lemma D.2. *Let R be an integral domain, and Q an R-module.*

(i) Q injective $\Rightarrow$ Q divisible.

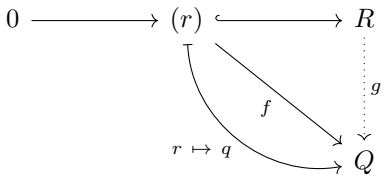
(ii) Suppose also that R is a P.I.D.. Then

$$Q \text{ divisible} \Rightarrow Q \text{ injective}$$

so that

$$Q \text{ injective} \Leftrightarrow Q \text{ divisible.}$$

Proof. (i). Suppose Q is injective, and $r \neq 0$.



(want to find $q' \in Q$ such that $rq' = q$)

$$rg(1) = g(r) = f(r) = q$$

Q is injective so g exists such that diagram commutes.

$$\text{Now } q = f(r) = g(r) = r \underbrace{g(1)}_{q'}$$

so Q is divisible.

(ii). Use the same diagram.

Note: In a P.I.D. all ideals are

$$(r) \hookrightarrow R.$$

Baer's criterion then gives the result (exercise). □

[1] Maybe clarify what embeds mean, in this context.

Example D.3. $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

Proof. $\mathbb{Q}/\mathbb{Z}$ is *divisible* so injective. □

Corollary D.4.

- *The only $\mathbb{Z}$-module which is injective and projective is* 0.
- *if R is an I.D. and $0 \neq M$ is an R-module which is injective and projective, then M is a* field.

Appendix E

Exercise session 5

$\mathrm{Hom}_R(P, -)$ exact $\Leftrightarrow$ P projective.

$\mathrm{Hom}_R(-, I)$ exact $\Leftrightarrow$ I injective.

$$A \xrightarrow{f} B \rightsquigarrow \mathrm{Hom}_R(B, I) \to \mathrm{Hom}_R(A, I)$$

10.5.16: Any R-module embeds in an injective R-module.

(a) show that M embeds into an injective $\mathbb{Z}$-module.

Idea: Find an injective $\mathbb{Z}$-module I such that the natural double duality homomorphism

$$M \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M, I), I)$$

is a monomorphism for all M.

Suppose that we have such an I. Let $\tilde{M} = \mathrm{Hom}_{\mathbb{Z}}(M, I)$.

There exists a free $\mathbb{Z}$-module that maps surjectively onto $\tilde{M}$:

$$\bigoplus_{\mathcal{S}} \mathbb{Z} \cong \mathcal{F} \twoheadrightarrow \tilde{M}$$

$$(\{m_s \in \tilde{M} \mid s \in \mathcal{S}\} \text{ generating set for } \tilde{M})$$

This surjective homomorphism induces an injective homomorphism

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}}(\tilde{M}, I) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{F}, I) &\cong \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{\mathcal{S}} \mathbb{Z}, I\right) \\ &\cong \prod_{\mathcal{S}} \underbrace{\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, I)}_{\cong I} \\ &\cong \prod_{\mathcal{S}} I. \end{aligned}$$

where

$$\prod_{\mathcal{S}} I$$

is injective, as a direct product of injective modules is injective (Excercise).

By our assumptions, we have a composition of injective homomorphisms, from M into an injective R-module

$$M \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\tilde{M}, I) \hookrightarrow \prod_{\mathcal{S}} I.$$

It remains to find an I with the required propery. This means find a divisible abelian group I with the property that for any abelian group M and $0 \neq m \in M$ there exists a homomorphism $f\colon M \to I$ such that $f(m) \neq 0$.

Claim E.1. : $\mathbb{Q}/\mathbb{Z}$ has the required property.

Proof. Let M be an abelian group and $0 \neq m \in M$. Let $\langle m \rangle$ be the subgroup of M generated by m. This is a cyclic group. Thus $\langle m \rangle \cong \mathbb{Z}$ or $\langle m \rangle \cong \mathbb{Z}/n$ for some integer $n > 1$. In any case there exists a homomorphism $\alpha\colon \langle m \rangle \to \mathbb{Q}/\mathbb{Z}$ such that $\alpha(m) \neq 0$. Here we used the fact that $\mathbb{Q}/\mathbb{Z}$ contains a subgroup isomorphic to $\mathbb{Z}/n$ for every n. Since $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, the map α can be extended to a homomorphism $\tilde{\alpha}\colon M \to \mathbb{Q}/\mathbb{Z}$ such that $\tilde{\alpha}(m) \neq 0$. □

Appendix F

Exercise Session 6

3 definitions:

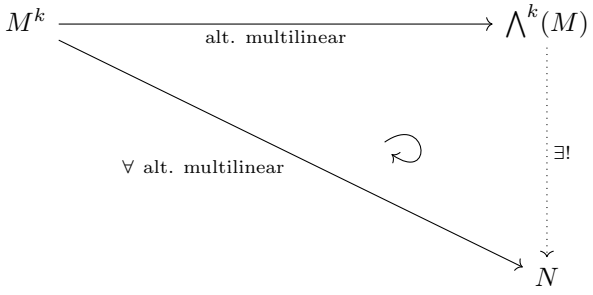
$T^k(M) = \underbrace{M \otimes \cdots \otimes M}_{k \text{ times}}$.

Definition F.1. $\bigwedge^0(M) = \frac{T^0(M)}{A^2(M)T^0(M)}$ $\qquad (A^2(M) = \langle m \otimes m, m \in M \rangle)$

Definition F.2. $\bigwedge^k(M) = \frac{T^k(M)}{\langle m_1 \otimes \cdots \otimes m_k,\ m_i = m_j,\ i \neq j \rangle}$

Definition F.3. Universal Property:

$$(m_1, \ldots, m_k) \longmapsto m_1 \wedge \cdots \wedge m_k$$



Let $M = V$ vector-space. $v_1, \ldots, v_k \in V$ and $v_1 \wedge \cdots \wedge v_k \in \bigwedge^k(V)$ is 0 if $v_1, \ldots, v_k$ is *linearly dependent*.

Exercise 11.5.8:

Let R be an integral domain and view $F = \mathrm{Frac}(R)$ as an R-module. Then

1. $\bigwedge^2(F) = 0$
2. Let $I \hookrightarrow F$ be an R-submodule. Show that $\bigwedge^k(I)$ is *torsion* (7.1.3) for all $k \geq 2$.

3. Exhibit R, F, I such that $\bigwedge^i(I) \neq 0$ for all $i \geq 0$.

(1):

$$\frac{a}{b} \otimes \frac{c}{d} \qquad (a, b, c, d \in R \setminus \{0\}).$$

$$\begin{aligned} \frac{a}{b} \wedge \frac{c}{d} &= \frac{ad}{bd} \wedge \frac{cb}{bd} \\ &= adbc\Big(\frac{1}{bd} \wedge \frac{1}{bd}\Big) \\ &= 0 \qquad (\text{since } \ \in A^2). \end{aligned}$$

(2):

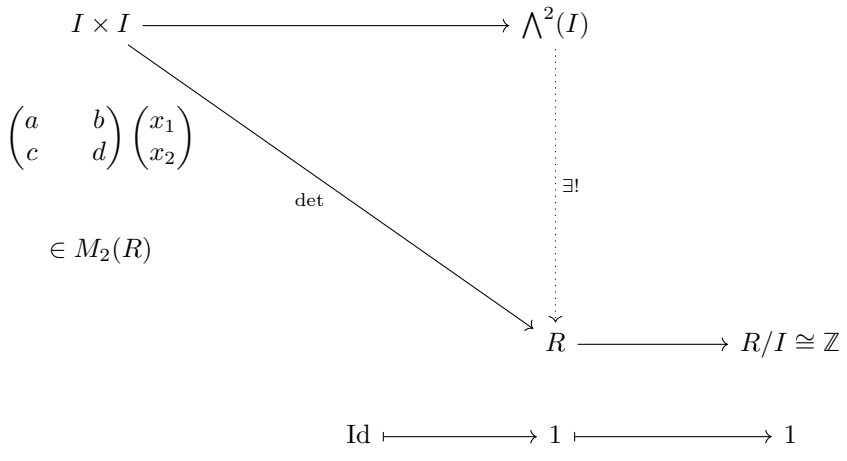
$$\begin{aligned} a_1a_2(b_1 \cdots b_k)\Big(\frac{a_1}{b_1} \wedge \frac{a_2}{b_2} \wedge \cdots \wedge \frac{a_k}{b_k}\Big) &= a_1a_2 \wedge a_1a_2 \wedge \cdots \wedge a_k \\ &= 0. \end{aligned}$$

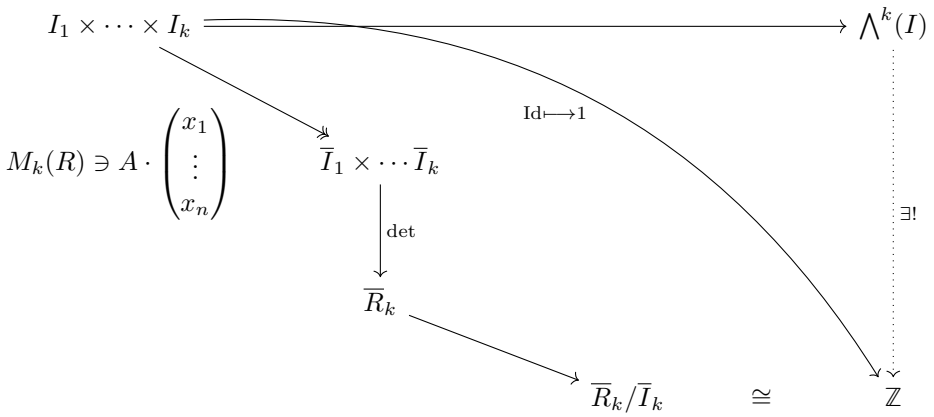
where $a_1, \ldots, a_k \in I$ and $b_1, \ldots, b_k \in R \setminus \{0\} \Rightarrow$ every element is *torsion*.

(3):

Let $R = \mathbb{Z}[x_i \mid i \in \mathbb{N}]$, $I = (x_i \mid i \in \mathbb{N})$ and $\overline{R}_k = R/(x_j | j > k) \cong \mathbb{Z}[x_1, \ldots, x_k]$ where

$$\overline{I}_k = \text{Image of } I \text{ in } \overline{R}_k$$





$$\exists \bigwedge^k(I) \xrightarrow{\neq 0} \mathbb{Z} \qquad x_1 \wedge \cdots \wedge x_n \mapsto 1$$
$$\Rightarrow \bigwedge^k(I) \neq 0.$$

Appendix G

Exercise Session 7

Setup: Let R be an integral domain, and let M be an R-module.

Definition G.1.

$$\mathrm{rk}_R(M) := \max(\{k \in \mathbb{N} \mid \exists k \text{ } R\text{-linearly independent elements in } M\}.)$$

12.1.20

Let R be an ID, let M be an R-module and let $F = \mathrm{Frac}(R)$. We want to show that

$$\mathrm{rk}_R(M) = \dim_F(M \otimes_R F).$$

Idea:

1. $\mathrm{rk}_R(M) \leq \dim_F(M \otimes_R F)$
2. $\mathrm{rk}_R(M) \geq \dim_F(M \otimes_R F)$.

Proof. Say $m_1, \ldots, m_k$ are R-linearly independent. Take $m_1 \otimes 1, \ldots, m_k \otimes 1$ and look at the map $M \to M \otimes_R F$ defined by $m \mapsto m \otimes 1$.

Suppose

$$\begin{aligned} \frac{r_1}{s_1}(m_1 \otimes 1) + \ldots + \frac{r_k}{s_k}(m_k \otimes 1) &= 0 \\ \Rightarrow \underbrace{(r_1 s_2 \cdots s_n m_1 + \ldots + r_k s_1 \cdots s_{k-1} m_k)}_{\text{may not be zero, so new approach}} \otimes 1 &= 0. \end{aligned}$$

New approach: Show that $\ker(M \to M \otimes_R F) = \mathrm{Tor}(M)$.

For the direction $\mathrm{Tor}(M) \subset \ker(M \to M \otimes_R F)$:

Assume $m \in \text{Tor}(M)$. Then there exists $r \in R \setminus \{0\}$ such that $rm = 0$. Hence we have that

$$\begin{aligned} m \mapsto m \otimes 1 &= m \otimes \frac{r}{r} \\ &= m \cdot r \otimes \frac{1}{r} \\ &= r \cdot m \otimes \frac{1}{r} = 0 \otimes \frac{1}{r} \\ &= 0 \end{aligned}$$

where we have used that R is an ID, so R is commutative, hence we can give M the "standard" bimodule-structure (R, R) defined by $r \cdot m = m \cdot r$

together with the fact that we have

$$m \otimes rr' = mr \otimes r' \tag{G.1}$$

for the tensor-product $M \otimes_R F$.

Consider: Define an R-module (**Localization**)

$$(R \setminus \{0\})^{-1}M := \{(r, m) \in R \setminus \{0\} \times M\}$$

where (r, m) is an equivalence class defined by the fact that $(r_1, m_1) \sim (r_2, m_2)$ if $\exists s \neq 0 \in R$ such that

$$s(r_2 m_1 - r_1 m_2) = 0.$$

We have

$$\frac{r_1}{m_1} = \frac{r_2}{m_2} \Leftrightarrow \frac{r_2 m_1 - r_1 m_2}{m_1 m_2} = 0 \Leftrightarrow \frac{s(r_2 m_1 - r_1 m_2)}{s m_1 m_2} = 0.$$

If we define

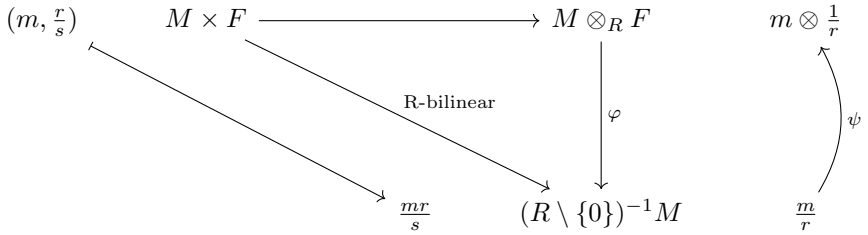
$$\overline{(r_1, m_1)} + \overline{(r_2, m_2)} := \overline{(r_1 r_2, r_2 m_1 + r_1 m_2)}$$

we get an R-module structure (did not check now, but I believe there is an exercise earlier in D & F that shows this).

Now, we look at the map $M \to (R \setminus \{0\})^{-1}M$ defined by $m \mapsto \frac{m}{1}$.

Lemma G.2. $M \otimes_R F \cong (R \setminus \{0\})^{-1}M$.

Proof.



Prove that

$$\varphi \circ \psi = \mathrm{Id}_{M \otimes_R F}$$
$$\psi \circ \varphi = \mathrm{Id}_{(R\setminus\{0\})^{-1}M}\,.$$

□

Next, we look at the map

$$M \to (R \setminus \{0\})^{-1}M \to M \otimes_R F. \tag{G.2}$$

Here we get that

$$M \ni m \mapsto \frac{m}{1} \in R \setminus \{0\}).$$

This we identify as $\overline{(1, m)}$. Now, we have that if

$$\overline{(1, m)} = \overline{(1, 0)} \Rightarrow \exists s \in R \setminus \{0\} \text{ such that } s(1 \cdot m - 0) = 0$$

so that $m \in \mathrm{Tor}(M)$.

Now, if we take ψ as the map

$$R \setminus \{0\} \ni \frac{m}{r} \mapsto m \otimes_R \frac{1}{r}$$

we get that $\dfrac{m}{1}$ and $\dfrac{0}{1}$ gets mapped to the same element in the tensor-product, and since $\frac{0}{1}$ gets mapped to 0, we see that

$$m \mapsto \overline{(1, m)} \mapsto m \otimes 1 = 0$$

so that $m \in \ker(M \to M \otimes_R F)$ under the map $m \mapsto m \otimes 1$. Hence

$$\ker(M \to M \otimes_R F) \subset \mathrm{Tor}(M).$$

Note here that we used the fact that $(R \setminus \{0\})^{-1}M \cong M \otimes_R F$ so that only $\frac{0}{1}$ which we identify as $\overline{(1,0)}$ gets sent to 0, hence if m is sent to 0 under the map from M to the tensor-product, via the isomorphism to the localization, we see that m must be a torsion-element.

Hence we find that

$$\ker(M \to M \otimes_R F) = \mathrm{Tor}(M).$$

Now, we know that $m_1, \ldots, m_k$ are not elements in the torsion-module $\mathrm{Tor}(M)$. We note that

$$r_1(s_2 \cdots s_k)m_1 + \ldots r_k(s_1 \cdots s_{k-1}m_k \otimes 1 = 0$$

implies that

$$r_1(s_2 \cdots s_k)m_1 + \ldots r_k(s_1 \cdots s_{k-1})m_k \in \mathrm{Tor}(M).$$

but this means that there exists a non-zero $r \in R$ such that

$$r(r_1(s_2 \cdots s_k)m_1 + \ldots r_k(s_1 \cdots s_{k-1}m_k)) = rr_1(r_1(s_2 \cdots s_k)m_1 + \ldots rr_k(s_1 \cdots s_{k-1}m_k) = 0$$

which implies that

$$rr_1(s_1 \cdots s_k) = \ldots = rr_k(s_2 \cdots s_{k-1}) = 0$$

where since R is an ID and $s_i \neq 0$, we must have that $rr_i = 0$ for all i. Now, by assumption, r is non-zero, hence $r_i = 0, \forall i \in \{1, \ldots, k\}$, that is

$$r_1 = \cdots = r_k = 0$$

so that

$$\frac{r_1}{s_1} = \cdots \frac{r_k}{s_k} = 0$$

hence

$$\frac{r_1}{s_1}(m_1 \otimes 1) + \ldots + \frac{r_k}{s_k}(m_k \otimes 1) = 0 \Rightarrow \frac{r_1}{s_1} = \cdots = \frac{r_k}{s_k} = 0$$

Unsure how to conclude.

Now, for (ii), suppose that

$$m_1 \otimes \frac{r_1}{s_1}, \ldots, m_k \otimes \frac{r_k}{s_k}$$

are linearly independent over $M \otimes_R F$, we want to show that it follows that $m_1, \ldots, m_k$ are linearly independent:

If

$$\sum r_i m_i = 0 \Rightarrow \left(\sum r_i m_i\right) \otimes 1 = 0 \Rightarrow \sum r_i m_i \otimes 1 = 0 \Rightarrow \sum r_i (m_i \otimes 1) = 0$$

which due to the assumed linear independence of $m_1 \otimes \frac{r_1}{s_1}, \ldots, m_k \otimes \frac{r_k}{s_k}$ shows that

$$r_1 = \ldots = r_k = 0.$$

□

Appendix H

Exercise Session 8

$p \in R[x]$ **irreducible** if $p = p_1 p_2$ then p_1 or p_2 in R.

Lemma H.1 (Gauss)**.** *R is UFD and $F = \mathrm{Frac}(R)$, $p \in R[x]$ then*

$$p \text{ reducible in } F[x] \Rightarrow p \text{ reducible in } R[x]$$

Remark H.2. Usually used with $R = \mathbb{Z}$ and $F = \mathbb{Q}$ (see prop. 9.3.5 in [**1**]).

Eisensteins Criterion:

Let R be an ID and let $f \in R[x]$ be **monic**,

$$f = x^n + \ldots + a_1 x + a_0.$$

If $\exists$ prime-ideal $P \subset R$ such that

(i) $a_{n-1}, \ldots, a_1, a_0 \in P$

(ii) $a_0 \notin P^2$

$\Rightarrow f$ is **irreducible**.

Remark H.3. Usually $R = \mathbb{Z}$ and $P = (p)$ for prime $p \in \mathbb{Z}$.

13.2.7:

(i) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

(ii) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$

(iii) Find some **irreducible** f with $f(\sqrt{2} + \sqrt{3}) = 0$.

Proof. (i) $\supset$ is clear.

For $\subset$: We have

$$(\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6}$$

$$\begin{aligned}(\sqrt{2}+\sqrt{3})^3 &= \sum_{k=0}^{3}\binom{3}{k}(\sqrt{2})^{3-k}\cdot(\sqrt{3})^k \\ &= 2\sqrt{2} + 3\cdot 2\cdot\sqrt{3} + \sqrt{2}\cdot 3\cdot 3 + 3\sqrt{3} \\ &= 11\sqrt{2} + 9\sqrt{3}.\end{aligned}$$

Hence

$$\frac{(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})}{2} = \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

so that also

$$\sqrt{2}+\sqrt{3}-\sqrt{2} = \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

□

Proof.

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})]\underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{=2}.$$

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1 \text{ or } 2$$

depending on whether $x^2 - 3$ is **reducible** or **irreducible** in $\mathbb{Q}(\sqrt{2})$.

We have

$$x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x] \textbf{ reducible} \Leftrightarrow \exists \text{ root of } x^2 - 3 \in \mathbb{Q}(\sqrt{2}).$$

So

$$(a + b\sqrt{2})^2 - 3 = 0$$

If $2ab\sqrt{2} = 0$ then $a = 0$ or $b = 0$.

Either way we get $a^2 - 3 = 0$ or $2b^2 - 3 = 0$ which has no **rational** solution.

We find that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ so that

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2.$$

and all in all we have

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$$
$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4.$$

□

(iii)

$$(\sqrt{2}+\sqrt{3})^4 = (5+2\sqrt{6})^2 = 49+20\sqrt{6}$$

$$(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 = 0$$

so consider

$$m(x) = x^4 - 10x^2 + 1.$$

Index