Rings and modules
(course notes, Fall 2021)

Zsolt Patakfalvi

with the collaboration of Marta Pieropan, Roberto Svaldi and Maciej Zdanowicz

Friday 17$^{\text{th}}$ December, 2021

Contents

Chapter 1

Color codes

We box certain parts of the material that has special meaning. We would like to stress that *boxes do NOT mean highlighting*. They just mean special type of material.

Part of the material that generalizes linear algebra material by pattern substitution

This is a part where linear algebra statements, definitions and proofs are generalized in an obvious way, that is, more or less by simple word replacement. For example statements about vector spaces are generalized by replacing every occurrence of "vector space" by "module". We take the liberty to go over this part of the material quicker in the lectures, only talking through the lecture notes, instead of writing down thoroughly each bit of it again.

Review of material learned in another course

We have learned this in another course, and we include it in these notes only for review.

Material very similar of what we learned in "Anneaux et corps"

Similarly to the case of material reminiscent to "Linear algebra", we take the liberty to go over this part of the material quicker in the lectures, only talking through the lecture notes, instead of writing down thoroughly each bit of it again.

Material very similar of what we learned in "Théorie des groupes"

Similarly to the case of material reminiscent to "Linear algebra" and "Theorie des groupes", we take the liberty to go over this part of the material quicker in the lectures, only talking through the lecture notes, instead of writing down thoroughly each bit of it again.

Material not on the exam but strongly suggested if you are seriously interested in algebra

This part of the material will not be asked in the exam, and will not be covered in class. At the same time there will be video uploaded about it on the Moodle page of the course. It is highly suggested to understand this material if you are seriously interested in algebra, say you are thinking about continuing taking algebra courses and maybe even do a PhD in something algebra related.

Chapter 2

Definitions and first properties of rings and modules

2.1 Rings

Review of material learned in another course

Recall the definition of a ring.

Definition 2.1.1. A ring R is a 5-tuple $(R, +, 0, \cdot, 1)$ satisfying the following conditions:

(1) $(R, +)$ additive group, and 0 is the additive unit,

(2) $\cdot$ is a binary operation which is associative, it is right and left distributive, and 1 is a multiplicative unit,

(3) $1 \neq 0$

A ring R is commutative if $\cdot$ is a commutative operation.

Example 2.1.2. Here are some examples of rings.

(1) the ring of integers $\mathbb{Z}$, fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, more generally, any field k.

(2) k-algebra: k-vector space V together with a k-bilinear map $\cdot : V \times V \to V$ (which is associative) and an element 1_V such that $1_V \cdot v = v \cdot 1_V = v$, $\forall v \in V$. Hence, $(V, +, 0, \cdot, 1_V)$ is a ring. [Exercise: $k \cdot 1_V$ is an embedded copy of k included in the center of V].
Examples: (commutative) polynomial rings: $k[x_1, \ldots, x_n]$ and $k[x_i]_{i \in \mathbb{N}}$,

(3) non commutative k-algebra: $M_n(k) = \{n \times n \text{ matrices with coefficients in } k\}$. Then $(M_n(k), +, 0, \cdot, Id)$ is a non-commutative k-algebra.

(4) ring of endomorphisms of a k-vector space W, $(\mathrm{End}_k(W), +, \circ, 0, \mathrm{id})$,

(5) let $\{Y_i\}_{i \in I}$ be a collection of elements and let k be a field. Let V be the k-vector space generated by all the (non-commutative) monomials in the Y_i – that is, a basis for V is given by all the words you can write using the Y_i, where we denote the empty word by 1_V. Then, it is easy to verify that there is a bilinear map $\cdot : V \times V \to V$ induced by the concatenation of words in the Y_i.
The free non-commutative algebra $k\langle Y_i \rangle_{i \in I}$ on k generated by $\{Y_i\}_{i \in I}$ is the

algebra structure on V induced by the operation $\cdot$, where the multiplicative identity is 1_V. [Caveat: non-commutativity is reflected by the fact that the concatenation of words is non commutative, e.g., $Y_1Y_2 \neq Y_2Y_1$; otherwise, we would just be producing a polynomial algebra with generators the Y_i].

(6) The group algebra of a finite group G over a field k is the k-algebra $R = k[G] := \left\{ \sum_{g\in G} \lambda_g g | \lambda_g \in k \right\}$. To explain the ring operations on R let us look at a specific example of $G = C_3 = \{e, g, g^2\}$ and $k = \mathbb{Q}$. Then every element of R can be written as $\lambda_e e + \lambda_g g + \lambda_{g^2} g^2$, for example $2e + 3g + 1/2g^2$. Addition happens coordinate-wise. For example:

$$(2e + 3g + 1/2g^2) + (1/3e + 4g + 2g^2) = 7/3e + 7g + 5/2g^2$$

and multiplication happens distributively:

$$\begin{aligned}&(2e + 3g + 1/2g^2)(1/3e + 4g + 2g^2)\\ &= (2/3 + 3\cdot 2 + 1/2\cdot 4)e + (2\cdot 4 + 3\cdot 1/3 + 1/2\cdot 2)g + (2\cdot 2 + 3\cdot 4 + 1/2\cdot 1/3)g^2\\ &= 26/3e + 10g + 97/6g^2.\end{aligned}$$

We note that when G is non-commutative, so is $k[G]$.

(7) Another frequently investigated non-commutative ring is the ring of differential operators $\mathcal{D}_x$ in 1 variable x over the field k. This is the subring of $\mathrm{End}_k(k[x])$ (meaning k-linear vector space endomorphisms), that are differential operators. For the details we refer to the corresponding "Anneaux et corps" exercises (in 2021 these were exc. 8 on sheet 3 and exc. 7 on sheet 4).

Here, let us only exhibit a basis and explain the multiplication of basis elements, assuming that $\mathrm{char}\, k = 0$. So, a basis as a k-vector space is

$$x^i \left(\frac{\partial}{\partial x}\right)^j$$

($\frac{\partial}{\partial x}$ is just a formal symbol here, it has nothing to do with taking limits). To understand multiplication, we should think about the above elements as operations on $k[x]$:

$$\frac{\partial}{\partial x} x(f) = \frac{\partial}{\partial x}(xf) = f + x\frac{\partial}{\partial x}(f) = \left(1 + x\frac{\partial}{\partial x}\right)(f).$$

So, $\frac{\partial}{\partial x} x = 1 + x\frac{\partial}{\partial x}$. This relation determines multiplication completely.

It can be shown that $\mathcal{D}_x \cong k\langle x, y\rangle \Big/ (yx - xy - 1)$, where $k\langle x, y\rangle$ is the free non-commutative k-algebra on the elements x, y introduced a few points above. We leave this as a homework.

In any case, $\mathcal{D}_x$ is the only non-commutative example we had with infinite dimension over the base-field.

Recall: ring homomorphisms, subrings, ideals, principal ideals, quotient rings. Properties of commutative rings:

- R is a domain $\Leftrightarrow$ R contains no zero divisors ("anneaux integre"),

- principal ideal domain (PID) $\Leftrightarrow$ domain + all ideals principal ("anneaux principal"),
- UFD ("anneaux factoriel") $\Leftrightarrow$ domain + every non-zero element $x \in R$ can be written as a product of irreducible elements $p_i \in R$ and a unit $u \in R$ and this is unique up to reordering the terms and up to multiplying each irreducible element by a unit.

2.2 MODULES

Part of the material that generalizes linear algebra material by pattern substitution

Definition 2.2.1. R is a ring, an abelian group $(M, +)$ is a *left R-module* if there is an operation $\cdot : R \times M \to M$ that satisfies the usual axioms of vector spaces:

(1) $1 \cdot m = m$,

(2) $\cdot$ is distributive and associative:

(i) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$,
(ii) $r(m_1 + m_2) = r \cdot m_1 + r \cdot m_2$,
(iii) $(rs) \cdot m = r \cdot (s \cdot m)$.

Instead of requiring the existence of $\cdot : R \times M \to M$ with the above properties, equivalently we can also require that there is a homomorphism of rings $R \to \mathrm{End}_{\text{ab-gp}}(M, +)$.

The definition of *right R-module* is the same as above, except instead of condition (2|(iii)) we require that $(rs)m = s(rm)$. In particular, in this situation we also write the multiplication on the on the other side: $m(rs) = (mr)s$.

Notation: left module ${}_RM$, right module M_R. If we only say R-module it means a left R-module.

Definition 2.2.2.

(1) Let M and N two R-modules, then an additive homomorphism $\phi : (M, +) \to (N, +)$ is an *R-module homomorphism*, if $\forall r \in R$, $\phi(rm) = r\phi(m)$.

(2) ϕ is called an *isomorphism* if it is bijective.

(3) $M \subseteq N$ is a *submodule* of an R-module N if it is an additive subgroup and $\forall r \in R$, $r \cdot M \subseteq M$. Sometimes, being a submodule is denoted by $M \leq_R N$.

(4) If $M \subseteq N$ is a submodule, then the *quotient module* N/M is the quotient group $\{ M+n \mid n \in N \}$ as an additive group, with multiplication $r(n+M) = rn+M$.

[Exercise: Check that the quotient N/M is a well defined R-module. *Hint*: use the fact that $\forall r \in R$, $r(n + m) = rn + rm$ and $rm \in M$.]

Notation 2.2.3. We fix certain notations for the entire notes:

(1) R denotes always a base-ring over which we work,

(2) when we just write "module", it means an "R-module", and similarly "submodule" and "quotient module" mean "sub R-module" and "quotient R-module",

(3) M and N always denote R-modules (or just modules, using the language of the previous point), and

(4) k is always an arbitrary field.

Example 2.2.4.

(1) if $R = \mathbb{Z}$, then the above notions mean group homomorphisms, subgroups and quotient groups of abelian groups

(2) if R is a field, then the notions of Definition 2.2.2 become linear transformations, sub-spaces, quotient spaces

(3) ${}_RR$ is the R-left module on R. Submodule of ${}_RR$ = left-ideal.

(4) $R \oplus \cdots \oplus R = \left((r_1, \ldots, r_d) \;\middle|\; r_i \in R \right)$ is an R-module (operations coordinatewise).

(5) If M is an R-module and $m \in M$, then

$$Rm := \left\{ rm \in M \;\middle|\; r \in R \right\}$$

is a left submodule of R (generated by m). If $M = Rm$ (for some $m \in M$), then M is a *cyclic module*.

(6) Having cyclic modules, we can see how modules behave differently compared to vector spaces, despite of the formal similarities between the definition of the two. For example the one dimensional vectorspace over a field has only the two trivial sub-spaces: itself and the zero subspace. However, one dimensional free modules can have many non-trivial subspaces. For example for $R = k[x]$ (where k is a field), Rf is a non-trivial subspace, or equivalently we have $0 \neq Rf \subsetneq R$, whenever f is non-zero and not invertible.

(7) Using the examples of the previous point we get really interesting modules, for example $M = {}^{R}\!/_{Rx}$ for $R = k[x]$. These examples differ fundamentally from vector spaces, as $x \in R$ acts on it by the $0 \in \mathrm{End}_{\text{ab-gb}}(M, +)$.

(8) Similarly to cyclic modules, if $m_1, \ldots, m_d \in M$, then

$$\sum_{i=1}^{d} Rm_i := \left\{ \sum_{i=1}^{d} r_i m_i \;\middle|\; r_i \in R \right\} \subseteq M$$

is the left submodule of M generated by $m_1, \ldots, m_d$. M is finitely generated, if $M = \sum_{i=1}^{d} Rm_i$ for some finitely many m_i.

(9) concrete example: take $R = k[x, y]$. Consider the R-module, $R \oplus R/R(x, 0) + R(0, y)$.

[Exercise: is it isomorphic to ${}_RR$?]

(10) Let R be a ring. If M, N are left R-modules, $\mathrm{Hom}_R(M, N)$ is a *left* R-module with module structure $R \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$ given by

$$(r, \varphi) \mapsto \big(r\varphi : M \to N \text{ defined by } (r\varphi)(m) := r\varphi(m)\big).$$

(11) It is not part of the material of the exam, but we mention for the interested reader that the representations of a finite group G over a field k are in one-to-one correspondence with finite dimensional modules over M over $k[G]$. A representation of G is simply a group homomorphism $\rho : G \to \mathrm{GL}(V)$. Then there is a natural homomorphism $\alpha : k[G] \to \mathrm{End}(V)$, defined by

$$\alpha\left(\sum_{g\in G} \lambda_g g\right) = \sum_{g\in G} \lambda_g \rho(g).$$

The fact that α is a homomorphism follows from ρ being a homomorphism (homework: wok out the details). This endows V with a $k[G]$-module structure. We leave it as a non-obligatory homework to show that the assignment $\rho \mapsto \alpha$ yields a bijection as claimed above.

Part of the material that generalizes linear algebra material by pattern substitution

Definition 2.2.5. As in the case of groups, if $\phi : M \to N$ is a homomorphism of R-modules, we define

$$\ker(\phi) = \{\ m \in M \mid \phi(m) = 0\ \},$$

and

$$\mathrm{im}(\phi) = \{\ \phi(m) \mid m \in M\ \}$$

Proposition 2.2.6. *Using the notations of the above definition,* $\ker\phi \subseteq M$, *and* $\mathrm{im}\,\phi \subseteq N$ *are* R*-submodules.*

Proof. We know from group theory that $\ker\phi$ and $\mathrm{im}\,\phi$ are additive subgroups. So, we just have to show for each $r \in R$ that $r(\ker\phi) \subseteq \ker\phi$:

$$\forall m \in M \ :\ m \in \ker\phi \Longrightarrow \phi(m) = 0 \Longrightarrow \phi(rm) = r\phi(m) = 0 \Longrightarrow rm \in \ker\phi$$

and that $r(\mathrm{im}\,\phi) \subseteq \mathrm{im}\,\phi$:

$$\forall \phi(m) \in \mathrm{im}\,\phi \ :\ r\phi(m) = \phi(rm) \in \mathrm{im}\,\phi$$

□

Material very similar of what we learned in "Théorie des groupes"

Definition 2.2.7. A sequence

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \ldots \xrightarrow{f_{n-1}} M_n$$

of R-modules is exact, if for all integers $1 \le i \le n-2$, $\mathrm{im}\, f_i = \ker f_{i+1}$.

A short exact sequence is an exact sequence of the type

$$0 \longrightarrow M \longrightarrow N \longrightarrow K \longrightarrow 0\ .$$

Remark 2.2.8. For a short exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow K \longrightarrow 0\ ,$$

then $K \cong N/M$. To see this use the next proposition.

Proposition 2.2.9 (First isomorphism theorem)**.** *Let $\phi : M \to N$ be an R-homomorphism. Then ${}^{M}/_{\ker \phi} \cong \operatorname{im} \phi$.*

Proof. As for Proposition 2.2.6 we know from group theory that there is an additive isomorphism $\xi : {}^{M}/_{\ker \phi} \to \operatorname{im} \phi$ given by $\xi(x + \ker \phi) = \phi(x)$. Then we check that this is also a module homomorphism, that is, for every $r \in R$ and every $m \in M$ we have

$$\xi\big(r(x + \ker \phi)\big) \underset{\uparrow}{=} \xi(rx + \ker \phi) \underset{\uparrow}{=} \phi(rx) \underset{\uparrow}{=} r\phi(x) \underset{\uparrow}{=} r\big(\xi(r + \ker \phi)\big).$$

definition of multiplication on ${}^{M}/_{\ker \phi}$	definition of ξ	ϕ is an R-module homomorphism	definition of ξ

□

Remark 2.2.10 (Universal property of the quotient). Let $M \subset N$ be an R-submodule. The quotient module N/M satisfies the following universal property: for every R-module Q specifying a homomorphism of R-modules $\overline{\phi}\colon N/M \to Q$ is equivalent to giving a homomorphism $\phi\colon N \to Q$ such that $\phi_{|M} = 0$.

Proposition 2.2.11. *$\phi : M \to N$ a homomorphism of R-modules, and $K \leq_R N$, then*

$$\phi^{-1}(K) := \{\ m \in M \mid \phi(m) \in K\ \}$$

is also an R-submodule. In the same setup, if $L \leq_R M$, then

$$\phi(L) := \{\ \phi(l) \mid l \in L\ \}$$

is also an R-submodule. Similarly, if $K, L \leq_R M$, then $K \cap L \leq_R M$.

Proof. Homework, similar to Proposition 2.2.6. □

Proposition 2.2.12. *$N \subseteq M$ a sub R-module, then there is a bijective correspondence*

$$\{\ N \leq_R H \leq_R M\ \} \leftrightarrow \{\ L \mid L \leq_R M/N\ \}$$

Proof. Consider the natural homomorphism $\phi : M \to M/N$ given by $m \mapsto m + N$. Proposition 2.2.11 gives the $\leftarrow$ direction. For the other direction, for H we associate $\phi(H)$. Homework is to check that this is bijective. □

Proposition 2.2.13 (Second isomorphism theorem)**.** *Let H and N be submodules of M. Then ${}^{H+N}/_{N} \cong {}^{H}/_{H \cap N}$.*

Proof. Consider the composition of the natural homomorphisms $H \hookrightarrow H + N \to (H + N)/N$. The kernel is $H \cap N$, and image is surjective, since $[h + n] = [h]$ in $(H + N)/N$ for every $h \in H$ and $n \in N$. □

Proposition 2.2.14 (Third isomorphism theorem)**.** *If $L \subseteq N$ are submodules of M. Then ${}^{M}/_{N} \cong {}^{M}/_{L}\Big/{}^{N}/_{L}$, such that the isomorphism sends $m + N$ to $(m + L) + {}^{N}/_{L}$.*

Proof. Denote by ξ the composition $M \to {}^{M}/_{L} \to {}^{M}/_{L}\Big/{}^{N}/_{L}$. By definition ξ is surjective and $\ker \xi = N$. Use then the first isomorphism theorem, that is, Proposition 2.2.9. □

Part of the material that generalizes linear algebra material by pattern substitution

Definition 2.2.15. Given a family of R-modules $\{M_i\}_{i\in I}$, we define the direct product

$$\prod_{i\in I} M_i := \{\ (m_i)_{i\in I} \mid m_i \in M_i\ \}$$

and the direct sum

$$\bigoplus_{i\in I} M_i := \{\ (m_i)_{i\in I} \ \big|\ m_i \in M_i, \quad m_i = 0 \text{ for all but finitely many indices } i \in I\ \},$$

both with the obvious coordinatewise operations. We also define the natural homomorphisms

$$\mathrm{pr}_i : \prod_{i\in I} M_i \twoheadrightarrow M_i \qquad \iota_i : M_i \hookrightarrow \bigoplus_{i\in I} M_i$$

by

$$\mathrm{pr}_i\Big((m_i)_{i\in I}\Big) = m_i, \qquad \text{and} \qquad \iota_i(m) = (0,\dots,0,\underset{\substack{\uparrow\\ i\text{-th}}}{m},0,\dots,0)$$

Remark 2.2.16. If I is a finite set, then the inclusion $\bigoplus_{i\in I} M_i \subseteq \prod_{i\in I} M_i$ is an equality.

Proposition 2.2.17 (Universal properties of products and direct sums)**.** *Let $\{M_i\}_{i\in I}$ be a family of R-modules. The product $\prod_{i\in I} M_i$ and the direct sum $\bigoplus_{i\in I} M_i$ satisfy the following universal properties:*

- *given an R-module Q and a collection $\phi_i : Q \to M_i$ of R-module homomorphisms for every $i \in I$, there exists a unique homomorphism $\phi : Q \to \prod_{i\in I} M_i$ such that for every $i \in I$ we have $\mathrm{pr}_i \circ \phi = \phi_i$.*
- *given an R-module Q and a collection $\xi_i : M_i \to Q$ of R-module homomorphisms for every $i \in I$, there exists a unique homomorphism $\xi : \bigoplus_{i\in I} M_i \to Q$ such that for every $i \in I$ we have $\xi \circ \iota_i = \xi_i$.*

Proof. The map ϕ and ξ are defined by

$$\phi(q) = \big(\phi_i(q)\big)_{i\geq 0} \qquad \text{and} \qquad \xi\Big((m_i)_{i\in I}\Big) = \sum_{i\in I, m_i\neq 0} \xi_i(m_i).$$

It follows by their definition that ϕ and ξ are R-module homomorphims and they satisfy the above universal properties. □

Lemma 2.2.18. *If $m \in M$ is an element of an R-module, then there is a unique R-module homomorphism $\phi_m : R \to M$ such that $\phi_m(1) = m$.*

Proof. *Unicity:* If ϕ_m exists, then for any $r \in R$ we have

$$\phi_m(r) \underset{\substack{\uparrow\\ \text{point (1) of Definition 2.2.2}}}{=} r\phi_m(1) \underset{\substack{\uparrow\\ \text{by assumption}}}{=} rm,$$

which says that ϕ_m is uniquely determined.

Existence: Define ϕ_m by $\phi_m(r) = rm$ for every $r \in R$. We have to verify that it is an R-module homomorphism. That is, it is additive because for every $r, s \in R$ we have

$$\phi_m(r+s) = (r+s)m \underset{\uparrow}{=} rm + sm\phi_m(r) + \phi_m(s),$$

point (2|(i)) of Definition 2.2.1

and additionally it is compatible with scalar product, because for every $r, s \in R$ we have

$$r\phi_m(s) = r(sm) \underset{\uparrow}{=} (rs)m = \phi_m(rs).$$

point (2|(iii)) of Definition 2.2.1

□

Example 2.2.19. If $m_1, \dots, m_d \in M$ are finitely many elements, then by applying point Proposition 2.2.17 of Proposition 2.2.17 to $R^{\oplus d}$, as well as Lemma 2.2.18 to each m_i we obtain a homomorphism $\phi : R^{\oplus d} \to M$ such that

$$\phi\big((r_1, \dots, r_d)\big) = \sum_{i=1}^{r} r_i m_i \in M$$

In particular, $\operatorname{im}\phi$ is the submodule of M generated by $m_1, \dots, m_d$.

Definition 2.2.20. An R-module M is *free* if $M \cong \oplus_{i\in I} R$ for some index set I. A subset of M is a basis if it corresponds via an isomorphism as above to the elements

$$e_i = (0, \dots, 0, \underset{\uparrow}{1}, 0, \dots, 0) \in \bigoplus_{i\in I} R.$$

i-th

The *rank* of a free module is defined by the cardinality of I involved in the above isomorphis. It was shown in "Anneaux et corps" that this is independent of the choice of the basis.

Proposition 2.2.21 (Universal property of free modules)**.** *Let M be an R-module. The following are equivalent:*

(1) M is free with basis $\{m_i\}_{i\in I}$;

(2) There exists a generator set $(m_i)_{i\in I}$ of M such that for every finite subset $\{i_1, \dots, i_t\} \subseteq I$ of distinct indices and for every $r_1, \dots, r_t \in R$ we have

$$\sum_{j=1}^{t} r_j m_{i_j} = 0 \implies r_1 = \cdots = r_t = 0 \tag{2.21.a}$$

Proof. *(1) $\implies$ (2):* Via the isomorphism $M \cong \bigoplus_{i\in I} R$, we may assume that $M = \bigoplus_{i\in I} R$, and $m_i = e_i$. Then we have $\sum_{j=1}^{t} r_j e_{i_j}$ is the vector where we have zeros everywhere except in the i_j-th position, where we have an r_j. As i_j are different indices, we obtain directly that this sum is zero if and only if all the r_j are zero.

(2) $\implies$ (1): The universal property of direct sum gives a unique R-module homomorpism $\phi : \bigoplus_{i\in I} R \to M$ such that $\phi \circ \iota_i(1) = m_i$. We have:

- ϕ is surjective as $(m_i)_{i\in I}$ is assumed to be a generator, and
- ϕ is injective, because this is exactly what is stated by f (2.21.a).

□

Chapter 3

Chain conditions

3.1 Basics

Material very similar of what we learned in "Anneaux et corps"

Definition 3.1.1. Let R be a ring. A module M over a ring R is *Noetherian* if it does not have infinite strictly increasing chains of submodules. i.e., there does not exist $\{ M_i \leq_R M \mid i \in \mathbb{N} \}$ such that

$$M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_i \subsetneq M_{i+1} \subsetneq \dots$$

A ring R is Noetherian if it is Noetherian as a module over itself.

A module M over a ring R is *Artinian* if it does not have infinite strictly decreasing chains of submodules. i.e., there does not exist $\{ M_i \leq_R M \mid i \in \mathbb{N} \}$ such that

$$M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_i \supsetneq M_{i+1} \supsetneq \dots$$

A ring R is Artinian if it is Artinian as a module over itself.

Example 3.1.2.

(1) Finite abelian groups are both Noetherian and Artinian as $\mathbb{Z}$-modules.

(2) Fields are both Noetherian and Artinian.

(3) The ring $\mathbb{Z}$ is Noetherian but not Artinian. Noetherian because if

$$I_1 \subseteq I_2 \subset I_3 \subseteq \dots$$

is an increasing chain of ideals, then the ideal $\bigcup_{i \geq 1} I_i$ is principal, hence generated by an element $n \in \mathbb{Z}$. Then there exists $i \geq 1$ such that $n \in I_i$, then $I_i = I_j$ for all $j \geq i$. Not Artinian because the sequence

$$(2) \supsetneq (2^2) \supsetneq (2^3) \supsetneq (2^4) \supsetneq \dots$$

is an infinite strictly decreasing sequence of submodules.

(4) $k[x]$ is Noetherian as we have learned in "Anneaux et corps", but it is not Artinian by a similar chain as in the previous example:

$$(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \dots$$

End of 1. class, on 23.09.2021.

(5) Over $R = k[x]$, on the other hands there are plenty of Artinian modules. For example $M = {}^{R}/_{Rx^2}$ Artinian as it has finitely many submodules. Indeed, by Proposition 2.2.12 its submodules correspond to the submodules of R containing Rx^2. This are the same as ideals of R containing x^2. As R is a PID such ideal is of the form (f). Furthermore, such an ideal contains x^2 if and only if $f|x^2$. So, up to multiplication by a unit, there are three such f's: 1, x, or x^2. That is, M has three submodules.

(6) $k[x_1, x_2, \dots] = \bigcup_{i\geq 1} k[x_1, \dots, x_i]$ (k is any field) is not Noetherian nor Artinian. Indeed $(x_1) \subsetneq (x_1, x_2) \subsetneq \dots$ is an infinite increasing sequence of ideals (and hence submodules), and $(x_1) \subsetneq (x_1^2) \subsetneq \dots$ is an infinite strictly decreasing sequence of ideals.

(7) The $\mathbb{Z}$-module $M = \{x \in \mathbb{Q}/\mathbb{Z} : \exists n \geq 0, p^n x = 0\}$ for a fixed prime $p \in \mathbb{Z}$ is Artinian but not Noetherian. Below we explain this, but first note that the preimage in $\mathbb{Q}$ of M via the quotient homomorphism $\mathbb{Q} \twoheadrightarrow {}^{\mathbb{Q}}/_{\mathbb{Z}}$ is

$$\left\{ y \in \mathbb{Q} \;\middle|\; \exists n \in \mathbb{N} : p^n y \in \mathbb{Z} \right\} = \left\{ \frac{a}{p^n} \in \mathbb{Q} \;\middle|\; (a,p) = 1,\ n \in \mathbb{N} \right\}$$

Second, note that all submodules of M are cyclic of the form $\mathbb{Z} \cdot \left[\frac{1}{p^m}\right]$ for some$m \geq 0$. This is because if $\left[\frac{a}{p^n}\right]$ belongs to a submodule $M' \subseteq M$ with $p \nmid a$, then there exist $\alpha, \beta \in \mathbb{Z}$ such that $1 = \alpha a + \beta p^n$, and hence $\left[\frac{1}{p^n}\right] = \left[\frac{\alpha a}{p^n}\right] \in \mathbb{Z}\left[\frac{a}{p^n}\right]$. So, there are three types of submodules of M:

- M itself,
- finite cyclic submodules,
- the zero module

In particular, any decreasing sequence is either constant or it has one term which is finite, and hence contains only finitely many further submodules. Moreover, the sequence $< \frac{1}{p} > \subsetneq < \frac{1}{p^2} > \subsetneq < \frac{1}{p^3} > \dots$ is infinite strictly increasing, as

$$\left[\frac{1}{p^n}\right] \in \mathbb{Z} \cdot \left[\frac{1}{p^{n-1}}\right] \iff \exists a \in \mathbb{Z} \ : \ \frac{1}{p^n} - \frac{a}{p^{n-1}} \in \mathbb{Z} \iff a \in \mathbb{Z} \ : \ \frac{1-ap}{p^n} \in \mathbb{Z}$$

where the right-most condition is false whenever $n \geq 1$, as $p \nmid 1 - ap$.
Exercise: is $\mathbb{Q}/\mathbb{Z}$ an Artinian $\mathbb{Z}$-module?

Material very similar of what we learned in "Anneaux et corps"

Lemma 3.1.3. *If M is a Noetherian (resp. Artinian) module then so are all its factor and submodules modules.*

Proof. Let M be Noetherian, and N a submodule. For the quotient module case, we use the correspondence theorem, that is, if

$$M_1 \subsetneq M_2 \subsetneq M_2 \subsetneq \dots.$$

is an infinitely increasing chain of submodules of M/N, then so is

$$\phi^{-1}(M_1) \subsetneq \phi^{-1}(M_2) \subsetneq \dots.$$

where $\phi : M \to M/N$ is the usual homomorphism. However, the latter cannot exist

by the Noetherian assumption on M. The Artinian case for quotients is shown the same way, only replacing increasing by decreasing.

For the submodule case we just note that all submodules of N are also submodules of M, so every increasing (resp. decreasing case) chain of submodules of N is also a similar chain in M.

□

In fact, the converse of Lemma 3.1.3 also holds. For this we first need the following lemma:

Lemma 3.1.4. *If $N \subseteq M$ is a submodule of a module over R, and $K \subseteq L \subseteq M$ are two submodules such that $K \cap N = L \cap N$ and $\phi(K) = \phi(L)$, where $\phi : M \to {}^{M}\!/_{N}$ is the quotient map, then $K = L$.*

Proof. Assume the contrary, and take $m \in L \setminus K$. As $\phi(m) \in \phi(L) = \phi(K)$, there is an $x \in K$ such that $\phi(x) = \phi(m)$. As $\phi(x-m) = \phi(x) - \phi(m) = 0$, we have $x - m \in \ker \phi = N$. However, $x - m$ is also contained in L. Hence, $x - m \in L \cap N = K \cap L$. Therefore $m = x - (x - m) \in K$, which is a contradiction. □

Remark 3.1.5. Lemma 3.1.4 fails already for 2 dimensional vector spaces over a field $k \neq \mathbb{F}_2$ if we do not assume that $K \subseteq L$. For example: $M = k^2$, $N = k \cdot (1,0)$, $K = k \cdot (1,1)$, $L \cdot (1,x)$, where $x \in k \setminus \{0,1\}$.

Proposition 3.1.6. *If $N \subseteq M$ is a submodule of a module over R such that both N and ${}^{M}\!/_{N}$ are Noetherian (resp. Artinian), then M is also Noetherian (resp. Artinian).*

Proof. We show the Noetherian statement only, as the proof of the Artinian one is literally the same by just inverting the containments. Let

$$M_1 \subseteq M_2 \subseteq \dots$$

be an ascending chain, and let $\phi : M \to {}^{M}\!/_{N}$ be the quotient homomorphism. As N and ${}^{M}\!/_{N}$ are Noetherian, the ascending chains formed out of $N \cap M_i$ and by $\phi(M_i)$ stabilize for $i \gg 0$. However, then Lemma 3.1.4 shows that M_i stabilizes too. □

Corollary 3.1.7. *M finitely generated module over a Noetherian (resp. Artinian) ring R, then M is Noetherian (resp. Artinian).*

Proof. Again, we show the proof only in the Noetherian case, as it is similar in the Artinian case. As M is finitely generated, $M = \sum_{i=1}^{d} Rm_i$. We show the statement by induction on d. For $d = 1$, M is the quotient of R, and hence it is Noetherian by Lemma 3.1.3. Hence, we are left to show the induction statement. That is we assume that $d > 1$ and that we know the statement for d replaced by $d-1$. Set then $N := \sum_{i=1}^{d-1} Rm_i$, in which case ${}^{M}\!/_{N}$ is generated by $[m_d]$. Hence, by the induction hypothesis both N and ${}^{M}\!/_{N}$ are Noetherian. Then, it follows that M is Noetherian by Proposition 3.1.6. □

Example 3.1.8. Consider $R := k[\varepsilon] = {}^{k[x]}\!/_{(x^2)}$. Ideals of R correspond to ideals of $k[x]$ containing (x^2), via Proposition 2.2.12. As $k[x]$ is a PID these are ideals of the form (f) such that $f | x^2$. Hence $f = (1)$, $f = (x)$ or $f = (x^2)$. This shows that R is both Artinian and Noetherian. Hence, finitely generated modules over R are both Artinian and Noetherian.

Example 3.1.2 shows that having an infinitely generated submodule ($(x_1, x_2, \dots)$ for example in point (6)) is an obstruction to being Noetherian. Indeed, in this case we can construct an infinitely ascending chain of submodules out of the infinitely many generators. What if all submodules are finitely generated?

Material very similar of what we learned in "Anneaux et corps"

Proposition 3.1.9. *Let M be an R-module. Then, M is Noetherian if and only if all its submodules are finitely generated.*

Proof. $\boxed{\Longrightarrow:}$ If M Noetherian, then all its submodules are Noetherian: if $N \leq_R M$, then an increasing chain of submodules of N is also an increasing chain of submodules of M, and hence it stabilizes.

So, it suffices to show that if M is Noetherian then M is finitely generated. Assume, by contradiction, that M is Noetherian but not finitely generated. Since M is not finitely generated, we can choose elements $m_1 \in M$, and $m_i \in M \setminus \sum_{j=1}^{i-1} Rm_j$ for all $i \geq 2$. Then $M_i := \sum_{j=1}^{i} Rm_j$ is a strictly increasing chain of submodules. This contradicts the fact that M is Noetherian (note that we used the axiom of choice!).

$\boxed{\Longleftarrow:}$ Assume that there is an infinite strictly ascending chain:

$$M_1 \subsetneq M_2 \subsetneq M_2 \subsetneq \dots.$$

Then $N := \bigcup_{i \geq 1} M_i$ is a submodule of M (may check this in words). Hence, by assumption, N is generated by finitely many elements $m_1, \dots, m_s$. However, then there is a finite index, say r, such that $m_1, \dots, m_s \in M_r$. But then $M_i = N$ for every $r \leq i$, which contradicts the assumption on our chosen chain. □

3.2 Jordan-Hölder theorem

Definition 3.2.1. A simple module over a ring R is a non-zero module M such that for every submodule $N \subseteq M$ we have $N = 0$ or $N = M$.

Definition 3.2.2. Let M be an R-module. A *composition series* is a finite chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{t-1} \subsetneq M_t = M$$

Such that for each $1 \leq i \leq t$, the submodule M_{i-1} is maximal among the proper submodules of M_i (such submodules we call maximal from now).

Remark 3.2.3. In Definition 3.2.2, the condition that M_{i-1} is maximal in M_i is equivalent to any of the following conditions:

(1) M_i/M_{i-1} is a simple module, by Proposition 2.2.12,

(2) M_i is minimal among the modules that contain M_{i-1} but that are not equal to M_{i-1}.

Remark 3.2.4. Let M be an R-module which is both Noetherian and Artinian, then it has a composition series. Indeed, one can start by taking maximal submodules iteratedly starting with M. The maximal submodules exist by Noetherianity and the process terminates by Artinianity.

In fact, the same argument, shows that each chain of submodules in this case can be refined to a composition series.

To give an explicit example, take the $R = k[x]$-modules, $M = k[x]/(x^2)$. This is both Aritinian and Noetherian, as it has finitely many submodules by point (5) of Example 3.1.2. Hence it admits a composition series as well. More explicitly

$$(0) \subsetneq (x)M \subsetneq M$$

is a composition series (see exercise 1 for the definition of IM, where $I \subseteq R$ is an ideal), as we have the R-module isomorphisms

$$(x)M \cong {}^{M}\!/_{(x)M} \cong {}^{k[x]}\!/_{(x)}.$$

Lemma 3.2.5. *If N and L are maximal submodules of M, then $N \cap L$ is a maximal submodule in both N and L.*

$$M/N \cong L/N \cap L \qquad \text{and} \qquad M/L \cong N/N \cap L. \tag{2.5.a}$$

Proof. As N and L are maximal submodules, M/N and M/L are simple modules. Hence, if we prove (2.5.a), we would have that $L/N \cap L$ and $N/N \cap L$ would also be simple, and then the maximality of $N \cap L$ in both N and L would follow.

Hence, we are left to show (2.5.a). Note first that as $N \neq L$, the submodule $N + L$ of M is strictly bigger than both N and L. As N and L are maximal submodules, it follows that $N + L = M$. Using then the isomorphism theorem (2.2.13), it follows that

$$M/N \cong N + L/N \cong L/N \cap L$$

and

$$M/L \cong N + L/L \cong N/N \cap L$$

This concludes our proof. □

Lemma 3.2.6. *Let $L \subsetneq K \subseteq M \supsetneq N$ be submodules of a module M over a ring R. Assume that N is maximal in M and that L is maximal in K. Then $K \cap N/L \cap N$ is either 0 or simple.*

Proof.

$$K \cap N/L \cap N \underset{\boxed{K \supseteq L}}{=} K \cap N/L \cap (K \cap N) \underset{\boxed{\text{Proposition 2.2.13}}}{\cong} (K \cap N) + L/L \hookrightarrow K/L. \quad \boxed{\text{simple by assumption}}$$

□

Theorem 3.2.7. JORDAN-HÖLDER THEOREM: *If*

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{r-1} \subsetneq M_r = M \tag{2.7.b}$$

and

$$0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{s-1} \subsetneq N_s = M \tag{2.7.c}$$

are two composition series, then $r = s$ and the collection of quotients

$$\left(M_{i-1}/M_i \;\middle|\; i = 1, \dots r \right) \qquad \text{and} \qquad \left(N_{i-1}/N_i \;\middle|\; i = 1, \dots s \right)$$

for the two chain agrees up to permutation and isomorphism.

Proof. We show the statement by induction on r. If $r = 0$, then $M = 0$ and there is nothing to prove. So, assume that $r > 0$ and we know the statement for r replaced by $r - 1$. If $M_{r-1} = N_{s-1}$, then we are ready by applying the induction hypothesis to M_{r-1}.

So, we may assume that $M_{r-1} \neq N_{s-1}$. Take now a composition series

$$0 = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_{t-1} \subsetneq L_t = M_{r-1} \cap N_{s-1}. \tag{2.7.d}$$

One can see that such series exists by applying Lemma 3.2.6 to $M_{i-1} \subsetneq M_i \subseteq M \supsetneq N_{s-1}$.

Appending M_{r-1} to the end of the composition series (2.7.d) and taking away M from the series (2.7.b), we obtain two composition series of M_{r-1}. By our induction hypothesis, applied to M_{r-1}, we see that $t = r-2$, and that the following collection of quotients agree up to permutation and isomorphisms:

$$\left(M_{i-1}/M_i \;\middle|\; i = 1, \dots r-1 \right) \qquad \text{and} \qquad \left(L_1/L_0, \dots, L_{r-2}/L_{r-3}, M_{r-1}/M_{r-1} \cap N_{s-1} \right). \tag{2.7.e}$$

Applying now the induction to the series obtained by appending N_s to (2.7.d), and to the series by removing M from the series (2.7.c). we obtain that $s = r$, and that the following collection of quotients agree up to permutation and isomorphisms:

$$\left(N_{i-1}/N_i \;\middle|\; i = 1, \dots r-1 \right) \qquad \text{and} \qquad \left(L_1/L_0, \dots, L_{r-2}/L_{r-3}, N_{r-1}/M_{r-1} \cap N_{s-1} \right). \tag{2.7.f}$$

Putting (2.7.e), (2.7.f) and Lemma 3.2.5 together concludes then that the quotients of the $M_\bullet$ and the $N_\bullet$ chain are isomorphic up to permutation. □

Definition 3.2.8. Let R be a ring. Over R, if M is a module that has a composition series, then we define the length $\operatorname{length}_R M$ of M by the integer n for which M has a composition series $0 = M_0 \subseteq \dots M_n = M$. By Theorem 3.2.7 this number is uniquely determined.

Example 3.2.9. Set $R := k[\varepsilon]$ and $M := R^{\oplus s}$, which is both Artinian and Noetherian. Then, a composition series can be obtained by

$$0 \subseteq R \cdot (\varepsilon, \underbrace{0, \dots, 0}_{s-1 \text{ coordinates}}) \subseteq R \oplus 0^{\oplus(s-1)} \subseteq R \oplus R(\varepsilon, \underbrace{0, \dots, 0}_{s-2 \text{ coordinates}}) \subseteq \dots \subseteq R^{\oplus(s-1)} \oplus R \cdot \varepsilon \subseteq R^{\oplus s}$$

The quotients of successive terms in this composition series are all isomorphic to the R-module $N := R/(\varepsilon)$. Hence, the same holds for all composition series, and $\operatorname{length}_R M = 2s$.

End of 2. class, on 27.09.2021.

3.3 Hilbert's basis theorem

The reason why it is hard to give examples of non-Noetherian rings is the following famous theorem saying intuitively that by finitely generated techniques one cannot produce a non-Noetherian ring.

Theorem 3.3.1. Hilbert's basis theorem: *If R is a commutative Noetherian rings, then so is $R[x]$.*

Proof. Let $I \subseteq R[x]$ and ideal.
We need to show: I is finitely generated.
Let us define

$$I_{\text{init}} := \left\{ a \in R \;\middle|\; \exists n \geq 0,\ a_0, \dots, a_n \in R,\ \sum_{i=0}^{n} a_i x^i \in I,\ a_n = a \right\}.$$

Claim. *I_{init} is an ideal in R.*

Proof. If $p(x) = \sum_{i=0}^{n} a_i x^i \in I$ and $q(x) = \sum_{i=0}^{n'} a'_i x^i \in I$, and $n \geq n'$, then $p(x) - x^{n-n'} q(x) \in I$ and has initial coefficient $a_n - a'_{n'}$. Moreover, for every $r \in R$, $rp(x) \in I$

and has initial coefficient ra_n. This shows that I_{init} satisfies both the additive and the multiplicative criterion of being an ideal, and hence concludes our claim. □

By the Noetherianity assumption on R, I_{init} is finitely generated, say by $b_1, \dots, b_s$. For each i choose $p_i(x) \in I$ with initial term b_i. By multiplying with some power of x we may further assume that for each i, $\deg p_i(x) = N$ for some fixed integer N. Consider now

$$J := \{\ f(x) \in I \mid \deg f(x) < N\ \} \subseteq \{\ f(x) \in R[x] \mid \deg f(x) < N\ \}.$$

The R-module on the right is finitely generated (generated by $1, x, x^2, \dots, x^{N-1}$), hence Noetherian by Corollary 3.1.7, hence J is also a finitely generated R-module. Choose generators $q_1(x), \dots, q_r(x)$ of J.

Claim. $I = \big(p_1(x), \dots, p_s(x), q_1(x), \dots q_r(x)\big)$.

Proof. Take $f(x) \in I$. We prove by induction on $\deg f(x)$ that

$$f(x) \in \big(p_1(x), \dots, p_s(x), q_1(x), \dots q_r(x)\big).$$

This follows by definition of $q_i(x)$ if $\deg f(x) < N$. For the induction step, assume that $\deg f(x) \geq N$ and that we know the statement for degrees smaller than $\deg f(x)$. Let b be the initial coefficient of $f(x)$. Then there are $c_i \in R$, such that $b = \sum_{i=1}^{s} c_i b_i$ and hence $\sum_{i=1}^{s} c_i x^{\deg f - N} p_i(x)$ has the same initial coefficient as $f(x)$. Therefore

$$g(x) = f(x) - \sum_{i=1}^{s} c_i x^{\deg f - N} p_i(x) \in I$$

and furthermore $\deg g(x) < \deg f(x)$. Hence, by induction we may write

$$g(x) = \sum_{i=1}^{s} a_i(x) p_i(x) + \sum_{i=1}^{r} b_i(x) q_i(x)$$

for some $a_i(x), b_i(x) \in R[x]$. However, then

$$f(x) = \sum_{i=1}^{s} \Big(c_i x^{\deg f - N} + a_i(x)\Big) p_i(x) + \sum_{i=1}^{r} b_i(x) q_i(x).$$

□

□

Recall that if $R \subset S$ is an inclusion of commutative rings, we say that S is a finitely generated R algebra if there exists elements $s_1, \dots, s_n \in S$ such that

$$S = R[s_1, \dots, s_n] := \{\ f(s_1, \dots, s_n) \mid f \in R[x_1, \dots, x_n]\ \},$$

where $f(s_1, \dots, s_n)$ denotes the evaluation of the polynomial f by substituting the s_i to the variables.

The following corollary is an immediate consequence of Hilbert's basis theorem.

Corollary 3.3.2. *Let R be a Noetherian ring.*

(1) For any $n \in \mathbb{N}$, $R[x_1, \ldots, x_n]$ is Noetherian.

(2) If $R \subset S$ is a finitely generated commutative R-algebra, then S is Noetherian.

Chapter 4

The fundamental theorem of finitely generated modules over a PID

4.1 Initial considerations

Let M be a finitely generated module over a left Noetherian ring R.

Question 4.1.1. Can we classify M as above?

Since M is finitely generated, there is a surjection $\epsilon : R^{\oplus s} \twoheadrightarrow M$ of R-modules (the one given in Example 2.2.19). By Corollary 3.1.7, $R^{\oplus s}$ is a Noetherian R-module. Hence by Proposition 3.1.9, $\ker \epsilon$ is a finitely generated R-module. Hence, there is another surjection of R-modules $\eta : R^{\oplus t} \to \ker \epsilon \subseteq R^{\oplus s}$, which can be written as a slight abuse of notation as the following exact sequence:

$$R^{\oplus t} \xrightarrow{\eta} R^{\oplus s} \xrightarrow{\epsilon} M \longrightarrow 0 \tag{1.1.a}$$

This is called a *presentation* of M.

Example 4.1.2. Let M be the ideal $(x, y) \subseteq k[x, y] =: R$. Then we have

$$\begin{aligned} R \oplus R &\xrightarrow{\epsilon} M \\ (r_1, r_2) &\longmapsto r_1 x + r_2 y \end{aligned} \quad .$$

How can we then describe $\ker \epsilon$? We have

$$(r_1, r_2) \in \ker \epsilon \Leftrightarrow r_1 x + r_2 y = 0 \Leftrightarrow r_1 x = -r_2 y$$

Using that R is a UFD, we have that $x | r_2$ and $y | r_1$, hence we may write $r_1 = y d_1$ and $r_2 = x d_2$, for which the previous equation becomes $d_1 yx = -d_2 xy$. Hence, using that R is a domain we obtain that $d_1 = -d_2$. Hence

$$(r_1, r_2) \in \ker \epsilon \Leftrightarrow (r_1, r_2) = d_1(y, -x).$$

Therefore, a presentation is of M is given by

$$\begin{aligned} R &\xrightarrow{\eta} R \oplus R \xrightarrow{\epsilon} M \\ r &\longmapsto r(y, , -x) \end{aligned} \quad .$$

So, here we have $t = 1$ and $s = 2$.

Going back to the general context, let us assume that we have a presentation as in (1.1.a) of a module M over a ring R. The first important thing to notice is that M is determined up to isomorphism uniquely by $\ker\epsilon$. Indeed, $M \cong R^{\oplus s}/\ker\epsilon$. However, since $\ker\epsilon = \operatorname{im}\eta$, it is also determined by $\operatorname{im}\eta$, and then also by the map η itself.

Another important thing to note is that if we take a $\phi \in \mathrm{Aut}_R(R^{\oplus t})$ and $\xi \in \mathrm{Aut}_R(R^{\oplus s})$, then $\xi\circ\eta\circ\phi$ and η determine isomorphic modules. Indeed,

$$R^{\oplus s}/\operatorname{im}(\xi\circ\eta\circ\phi) \underset{\boxed{\text{given by } \xi}}{\overset{\cong}{\uparrow}} R^{\oplus s}/\operatorname{im}(\eta\circ\phi) \cong R^{\oplus s}/\operatorname{im}(\eta),$$

where we used that both ξ and ϕ are isomorphisms. In particular, if we want to understand M up to isomorphism, then it is enough to understand η up to pre- and post-composing by ϕ and ξ.:

To classify finitely generated modules over R it is enough to classify R-module homomorphisms $\eta : R^{\oplus t} \to R^{\oplus s}$ up to pre- and post-composition by $\phi \in \mathrm{Aut}_R(R^{\oplus t})$ and $\xi \in \mathrm{Aut}_R(R^{\oplus s})$.

The above translation of the classification problem of finite generated modules over R is particularly useful, as all the R-module homomorphisms and all their compositions in this translation can be understood as matrices and as matrix multiplications. In the remainder of Section 4.1 we explain this.

There is a bijection

$$\boxed{\mathrm{Hom}_R\left(R^{\oplus t}, R^{\oplus s}\right)} \longleftrightarrow \boxed{\{s\times t \text{ matrices with coefficients in } R\}} \tag{1.2.b}$$

given exactly as in the case of finite dimensional vector spaces over a field k. That is, if $e_i \in R^t$ denotes the i-th standard basis vector, and if a_i denotes the i-th coordinate of any $a \in R^s$, then (1.2.b) in the rightwards direction is given by

$$\phi \mapsto \Big(\big(\phi(e_j)\big)_i\Big)_{i,j=1}^{s,t},$$

and in the leftwards direction

$$\left((a_1,\dots,a_t) \mapsto \left(\sum_{j=1}^t r_{1j}a_j, \sum_{j=1}^t r_{2j}a_j, \dots, \sum_{j=1}^t r_{sj}a_j\right)\right) \mapsfrom \big(r_{ij}\big)_{i=1,j=1}^{s,t}.$$

There are two important features of the correspondence that we have just constructed.

Proposition 4.1.3. *(1) In the correspondence (1.2.b), composition on the left side corresponds to matrix multiplication on the right side.*

(2) Under this correspondence, when $s = t$, automorphisms of R^s correspond to $s\times s$ matrices whose determinant is a unit in R.

Proof. (1) This works the same as over fields. So, for example in the rightwards direction if $\xi \in \mathrm{Hom}_R\left(R^{\oplus r}, R^{\oplus t}\right)$ and $\phi \in \mathrm{Hom}_R\left(R^{\oplus t}, R^{\oplus s}\right)$, then we have

$$\phi\circ\xi \mapsto \Big(\big((\phi\circ\xi)(e_j)\big)_i\Big)_{i,j=1}^{s,r},$$

where is exactly equal to the usual sum in the definition of matrix multiplication by the following computation:

$$\big((\phi\circ\xi)(e_j)\big)_i = \big(\phi(\xi(e_j))\big)_i = \left(\phi\Big(\sum_l \big(\big(\xi(e_j)\big)_l\big)e_l\Big)\right)_i \underset{\boxed{\text{as } \phi \text{ is a module homomorphism, it is additive and commutes with multiplication by ring elements}}}{\overset{=}{\uparrow}} \sum_l \big(\xi(e_j)\big)_l \cdot \big(\phi(e_l)\big)_i$$

We leave the other direction to the reader (again it works just like over fields, and it is quite straightforward, it is basically just about reading the last displayed equation in the backwards direction).

(2) We claim that a matrix is invertible if and only if its determinant is an invertible element of R. In backwards direction this is shown by the fact that the determinant is multiplicative, or with other words the determinant gives a multiplicative semi-group homomorphism $\mathrm{Mat}(s \times s, R) \to R$ (again, whatever proof you have seen over fields, over rings it works the same way). In the forward direction this is shown by Cramer's formula giving an inverse when the determinant is invertible.

□

According to Proposition 4.1.3, the above translation of the classification problem in terms of matrices this translates to understanding $s \times t$ matrices up to multiplication on both sides by invertible matrices. To summarize, we obtained that:

To classify finitely generated modules over R it is enough to classify $s \times t$ matrices up to multiplication by invertible matrices on both sides.

(s: number of rows; t: number of columns)

4.2 SMITH'S NORMAL FORM

For the remainder of Chapter 4, we assume that R is a PID.

Part of the material that generalizes linear algebra material by pattern substitution

Recall PID's are UFD's, and in particular irreducibles are the same as primes in R, and greatest commond divisors in R can be defined as explained in Proposition 4.2.1.

Proposition 4.2.1. *For $a, b \in R$, define c to be a generator of the ideal (a, b) (which exists by the PID assumption, and it is the greatest common divisor $\gcd(a, b)$ of a and b, as defined in Def. 2.7.2 of the "Anneaux et corps" notes). Then, we may write $a\sigma + b\tau = c$, $a = \alpha c$ and $b = \beta c$ for some $\alpha, \beta, \tau, \sigma \in R$. Then, the matrix*

$$\begin{pmatrix} \sigma & \tau \\ -\beta & \alpha \end{pmatrix}$$

is invertible.

Proof. $\alpha\sigma + \beta\tau = 1$, so the determinant is invertible and the inverse is given simply by

$$\begin{pmatrix} \alpha & -\tau \\ \beta & \sigma \end{pmatrix}.$$

□

Smith's normal form is the algorithm of reducing an arbitrary $s \times t$ matrix over R to the diagonal form by repeatedly multiplying by invertible matrices on both sides.

Hence, let $R = (r_{ij})$ be an $s \times t$ matrix. We will show that R is equivalent to a

diagonal matrix of the form

$$\left(\begin{array}{cccc|c} f_1 & 0 & 0 & 0 & \\ 0 & f_2 & 0 & 0 & 0_{s-r,r} \\ 0 & 0 & \ddots & 0 & \\ 0 & 0 & 0 & f_r & \\ \hline \multicolumn{4}{c|}{0_{r,t-r}} & 0_{s-r,t-r} \end{array}\right),$$

where $0_{m,n}$ indicates the 0 matrix of size $m \times n$. Our proof will be by induction on (t, s), the dimensions of the matrix, considered with the lexicographic order. The case of a 1×1 matrix is trivially true.

To begin with, we are free to swap columns (resp. rows) of R, as that corresponds to multiplying on the right (resp. on the left) by an invertible $t \times t$ matrix. Hence, we may assume that $r_{11} \neq 0$.

So, choose the largest l such that our matrix has the form

$$\begin{bmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & d_{l-1} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & r_{ll} & \dots & r_{lt} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & r_{sl} & \dots & r_{st} \end{bmatrix} \tag{2.1.a}$$

By multiplying with the adequate matrices we may swap both columns and rows. In particular, we may assume that $r_{ll} \neq 0$. Then by multiplying either on the left by a block matrix whose $l - j$ submatrix is of the form as the matrix of Proposition 4.2.1, and the rest is the identity matrix, or by multiplying the transpose of such a matrix, we may replace r_{ll} by the generator of (r_{ll}, r_{jl}) or of (r_{ll}, r_{lj}) (for some $j > l$). If r_{ll} does not divide r_{jl} (resp. r_{lj}) this way the ideal (r_{ll}) becomes strictly larger. As a PID is Noetherian, this process has to terminate. Then by multiplying with matrices that have an $-r_{jl}/r_{ll}$ (resp. $-r_{lj}/r_{ll}$) entry at an adequate place and they are the identity everywhere else, we may subtract r_{jl}/r_{ll} times (resp. r_{lj}/r_{ll} times) the l-th row (resp. column) to obtain 0 in the l-th row/column everywhere outside the diagonal. Then we may increase the value of l and we have proven by induction the following result.

Theorem 4.2.2. *Let R be a PID. Then for any $s \times t$ matrix M with coefficients in R, there exist an invertible $t \times t$ matrix A, an invertible $s \times s$ matrix B, and $f_1, \dots, f_r \in R$ such that*

$$BMA = \left(\begin{array}{cccc|c} f_1 & 0 & 0 & 0 & \\ 0 & f_2 & 0 & 0 & 0_{s-r,r} \\ 0 & 0 & \ddots & 0 & \\ 0 & 0 & 0 & f_r & \\ \hline \multicolumn{4}{c|}{0_{r,t-r}} & 0_{s-r,t-r} \end{array}\right).$$

4.3 Statement of the fundamental theorem

Theorem 4.3.1 (Fundamental theorem ver. 1.0)**.** *Suppose that R is a PID and M is a finitely generated module over R. Then*

$$M \cong \bigoplus_{i=1}^{s} R/Rf_i \tag{3.1.a}$$

for some $f_i \in R$.

Proof. By the considerations of Section 4.1, M has a presentation $R^{\oplus t} \to R^{\oplus s}$ given by a matrix $(r_{ij})_{i=1,j=1}^{s,t}$. Also by considerations of Section 4.1, the Smith normal form of this matrix presents the same module up to an isomorphism. Hence, we may assume that r_{ij} is diagonal. However, having diagonal presentation with elements $f_1, \dots, f_{\min\{r,s\}} \in R$ in the diagonal corresponds to an isomorphism

$$M \cong \left(\bigoplus_{i=1}^{\min\{r,s\}} R/Rf_i \right) \oplus R^{\oplus(s-\min\{r,s\})}.$$

If $s \neq \min\{r,s\}$, take $f_{\min\{r,s\}+1} = \cdots = f_s = 0$. □

Review of material learned in another course

Since R is a PID in the above theorem, it is also a unique factorization domain. Therefore we may write the prime decomposition

$$f_i = \prod_{j=1}^{r} p_j^{l_{i,j}}$$

where $p_1, \dots, p_r$ is a finite collection of primes, and $l_{i,j} \geq 0$ are integers.

We note that the greatest common divisor of f_i and $f_{i'}$, denoted by $\gcd(f_i, f_{i'})$, can be defined both as

$$\prod_{j=1}^{r} p_j^{\min\{l_{i,j}, l_{i',j}\}},$$

and as a generator of the ideal $(f_i, f_{i'})$ (in any case, $\gcd(f_i, f_{i'})$ is defined only up to multiplication by a unit). We say, f_i and $f_{i'}$ are coprime, if $\gcd(f_i, f_{i'}) = 1$.

Lemma 4.3.2 (Chinese remainder theorem for UFD's)**.** *If $q_i \in R$ $(i = 1, \dots, s)$ are finitely many pairwise coprime elements in a UFD then*

$$R/(\textstyle\prod_{i=1}^{s} q_i) \cong \displaystyle\bigoplus_{i=1}^{s} R/(q_i)$$

and additionally this isomorphism is an isomorphism of R-modules.

Proof. Consider the natural homomorphism

$$\phi : R \to \bigoplus_{i=1}^{s} R/(q_i)$$

The kernel is $\bigcap_{i=1}^{s}(q_i)$, which is equal to $(\prod_{i=1}^{s} q_i)$ by the coprimality assumption. We need: ϕ is surjective. Since $\gcd(q_i, q_j) = 1$, there are $a, b \in R$, such that $aq_i + bq_j = 1$. Then $r_{ij} := aq_i$ is an element of R is such that it is 0 mod q_i and 1 mod q_j. Then

for fixed j, $\prod_{i\neq j} r_{ij}$ is such that it is 1 mod q_j and 0 mod q_i for every $i \neq j$. This shows that ϕ is surjective.

To see that ϕ is also an isomorphism of R-modules, as it is bijective, we only have to check that ϕ is an R-module homomorphism. This follows diretly from the fact that so is the quotient homomorphism $R \to {}^{R}/_{(q_i)}$. □

Now getting back to understanding ${}^{R}/_{(f_i)}$ by the prime decomposition $f_i = \prod p_{i,j}^{l_{i,j}}$, we see that

$$ {}^{R}/_{(f_i)} = \prod_j {}^{R}/_{\left(p_j^{l_{i,j}}\right)} $$

Therefore, we can modify our main theorem.

Theorem 4.3.3 (Fundamental theorem ver. 2.0)**.** *Suppose that R is a PID and M is a finitely generated module over R. Then we have an isomorphism*

$$ M \cong R^{\oplus m_0} \oplus \left(\bigoplus_{i=1,l=1}^{s,r} \left({}^{R}/_{(p_i^l)} \right)^{\oplus m_{i,l}} \right) $$

for some integers $m_0, s, r \geq 0$, $m_{i,j} \geq 0$ and different primes $p_i \in R$.

Question 4.3.4. Is this unique?

Answer 4.3.5. Yes, up to obvious reordering. See what follows.

Definition 4.3.6. A module M over R is *torsion*, if

$$ \mathrm{Ann}(M) = \{\ r \in R \mid \forall m \in M :\ rm = 0\ \} \neq 0. $$

An element $m \in M$ is called *torsion* if

$$ \mathrm{Ann}(m) = \{\ r \in R \mid rm = 0\ \} \neq 0. $$

A module (resp. element) is called *r-torsion* (where $r \in R$), if $r \in \mathrm{Ann}(M)$ (resp. $r \in \mathrm{Ann}(m)$).

Lemma 4.3.7. *If R is a commutative domain (resp. R is commutation), torsion (resp. r-torsion) elements form a submodule* $\mathrm{Tors}(M)$ *(resp.* $\mathrm{Tors}_r(M)$*).*

Proof. Let us prove the statement for r-torsion elements, and we leave the case of arbitrary torsion to the reader. For that, take $m, n \in \mathrm{Tors}_r(M)$ and $s \in R$. Then,

$$ r(m+n) = rm + rn = 0 \implies m + n \in \mathrm{Tors}_r(M) $$

and

$$ rsm \underset{\uparrow}{=} srm = s \cdot 0 = 0 \implies sm \in \mathrm{Tors}_r(M) $$

R is commutative

□

Theorem 4.3.8 (Fundamental theorem ver. 3.0)**.** *Suppose that R is a PID and M is a finitely generated module over R. Then*

$$ M \cong R^{\oplus m_0} \oplus \left(\bigoplus_{i=1,l=1}^{s,r} \left({}^{R}/_{(p_i^l)} \right)^{\oplus m_{i,l}} \right) $$

for some integers $m_0, s, r \geq 0$, $m_{i,j} \geq 0$ and different primes $p_i \in R$, which are unique up to reordering the indices i, if we assume that $p_i \nmid p_j$ for all $i \neq j$, and that we cannot decrease s and r

Proof. We just have to count each type of factors.

FREE FACTORS. Then $R^{\oplus m_0} \cong {}^{M}\!/_{\mathrm{Tors}(M)}$, so the isomorphism class of $R^{\oplus m_0}$ is uniquely determined. Hence m_0 is unique, because the rank of a free module is unique (since an invertible matrix over a ring has to be a square matrix by the Smith normal form for example.).

FACTORS OF THE FORM ${}^{R}\!/_{(p^l)}$ FOR SOME FIXED PRIME p AND INTEGER $l > 0$. First, note that if $q \in R$ is a prime, then

$$\mathrm{Tors}_{q^j}\left({}^{R}\!/_{(p^l)}\right) = \begin{cases} 0 & \text{if } q \text{ is not associated to } p \text{ (i.e., not unit times } p) \\ \left(p^{l-j}\right)\Big/\left(p^l\right) \cong {}^{R}\!/_{(p^j)} & \text{if } q \text{ is associated to } p \text{ and } l \geq j \\ {}^{R}\!/_{(p^l)} & \text{if } q \text{ is associated to } p \text{ and } l < j \end{cases} \tag{3.8.b}$$

Indeed, for any $x \in R$ we have that

$$[x] \in \mathrm{Tors}_{q^j}\left({}^{R}\!/_{(p^l)}\right) \Leftrightarrow q^j x \in \left(p^l\right) \Leftrightarrow p^l | q^j x. \tag{3.8.c}$$

If $\gcd(q,p) = 1$, then this means that $p^l | x$, and hence $[x] = 0$. This gives the first case. On the other hand, if $\gcd(q,p) \neq 1$, then q is associated to p and hence the divisibility in (3.8.c) is equivalent to $p^{l-j}|x$ if $l \geq j$, and it gives no constraint if $l < j$. This gives the second and the third cases of (3.8.c)

Having showed (3.8.b),, we obtain

$$\mathrm{Tors}_{p_i^j} M \cong \bigoplus_{l=1}^{j-1} \left({}^{R}\!/_{(p_i^l)}\right)^{\oplus m_{i,l}} \oplus \left({}^{R}\!/_{\left(p_i^j\right)}\right)^{\oplus \sum_{l=j}^{r} m_{i,l}}$$

Note now that for $l < j$ we have

$$p_i^{j-1} \cdot \left({}^{R}\!/_{(p_i^l)}\right) = 0$$

and

$$p_i^{j-1} \cdot \left({}^{R}\!/_{\left(p_i^j\right)}\right) \cong \left(p_i^{j-1}\right)\Big/\left(p_i^j\right) \cong {}^{R}\!/_{(p_i)}.$$

Therefore,

$$m_{i,l} = \dim {}_{R}\!/_{(p_i)}\left(p_i^{l-1} \cdot \mathrm{Tors}_{p_i^l} M\right) - \dim {}_{R}\!/_{(p_i)}\left(p_i^{l} \cdot \mathrm{Tors}_{p_i^{l+1}} M\right) \tag{3.8.d}$$

Note that ${}^{R}\!/_{(p_i)}$ is a field (it does not contain non-trivial ideals), so this is just counting dimensions of a vector space. The expression on the right side of (3.8.d) is again uniquely determined (after fixing p_i) by the isomorphism class of M, hence so is $m_{i.l}$. □

A special case of Theorem 4.3.8 is the well known structure theorem of finitely generated abelian groups.

Corollary 4.3.9 (Structure theorem for finitely generated abelian groups)**.** *If G is a finitely generated abelian group, then*

$$G \cong \mathbb{Z}^{\oplus m_0} \oplus \left(\bigoplus_{i=1,l=1}^{s,r} \left({}^{\mathbb{Z}}\!/_{(p_i^l)}\right)^{\oplus m_{i,l}}\right)$$

for some integers $m_0, s, r \geq 0$, $m_{i,j} \geq 0$ and different primes $p_i \in \mathbb{Z}$, which are unique up to reordering the indices i, if we assume that s and r cannot be decreased.

4.4 JORDAN NORMAL FORM

What if we apply Theorem 4.3.8 for finitely generated modules over a PID to $R = F[x]$ for some field F? The key observation is the following correspondence

$$\boxed{\text{finitely generated torsion modules } M \text{ over } F[x]} \leftrightarrow \boxed{\begin{array}{l}F\text{-linear transformation } \phi \text{ on a}\\ \text{finite dimensional vector space}\\ M\end{array}} \tag{4.0.a}$$

The correspondence is given as follows:

$\boxed{\leftarrow:}$ Given $p(x) = \sum_{i=0}^{s} a_i x^i \in F[x]$, the action of $p(x)$ on M is given by $\sum_{i=0}^{s} a_i \phi^i \in \mathrm{End}_F(M) \subseteq \mathrm{End}(M)$. This is a module structure because for $p(x) = \sum_{i=0}^{s} a_i x^i \in F[x]$, $q(x) = \sum_{i=0}^{s} b_i x^i \in F[x]$ and for $m \in M$, using the linearity of linear transformations, we have

$$(p(x) + q(x)) \cdot m = \sum_{i=0}^{s} (a_i + b_i)\phi^i(m) = \sum_{i=0}^{s} a_i \phi^i(m) + \sum_{i=0}^{s} b_i \phi^i(m) = p(x) \cdot m + q(x) \cdot m$$

and

$$\begin{aligned}(p(x) \cdot q(x)) \cdot m = \sum_{r=0}^{2s} \left(\sum_{\substack{i+j=2s \\ i\geq 0, j\geq 0}} a_i b_j \right) \phi^r(m) &= \sum_{r=0}^{2s} \left(\sum_{\substack{i+j=2s \\ i\geq 0, j\geq 0}} a_i \phi^i\Big(b_j \phi^j(m)\Big) \right) \\ &= \sum_{i=0}^{s} a_i \phi^i \left(\sum_{j=0}^{s} b_j \phi^j(m) \right) = p(x) \cdot \big(q(x) \cdot m\big)\end{aligned}$$

Additionally the above definition yields a torsion module, because if $q(x)$ is the characteristic polynomial of ϕ, then $q(x) \in \mathrm{Ann}(M)$.

$\boxed{\rightarrow:}$ If M is a torsion module, then only the torsion factors can appear in Theorem 4.3.8. So, to see that M is finite dimensional F-vectorspace, it is enough to see that each torsion factor is finite dimensional. A general one is isomorphic to $F[x] \Big/ \big(p(x)^l\big)$ for some prime polynomial $p(x) \in F[x]$. However, this is finite dimensional over F, of dimension $\deg p(x)^l$.

After establishing that M is finite dimensional, ϕ can be defined as the linear transformation such that $\phi(y) = x \cdot y$ for each $y \in M$. The ϕ defined this way is F-linear because in $F[x]$ the scalars commute with F, and hence for any $\lambda, \mu \in F$ and $a, b \in M$ we have:

$$\begin{aligned}\phi(\lambda a + \mu b) = x \cdot (\lambda a + \mu b) &\underset{\uparrow}{=} (x\lambda) \cdot a + (x\mu) \cdot b \underset{\uparrow}{=} (\lambda x) \cdot a + (\mu x) \cdot b \\ &\qquad \boxed{\text{module axioms}} \qquad\quad \boxed{x \text{ and scalars commute in } F[x]} \\ &\underset{\uparrow}{=} \lambda \cdot (x \cdot a) + \mu \cdot (x \cdot b) = \lambda\phi(a) + \mu\phi(b) \\ &\qquad \boxed{\text{one module axiom}}\end{aligned}$$

This concludes the construction of the equivalence (4.0.a). Notice also that direct sum decomposition on the left side corresponds to direct sum decomposition on the right, which after choosing a basis compatible with the direct sum decomposition becomes a block decomposition of the associated matrix.

To conclude the Jordan normal form we have to understand the above correspondence more precisely for the factors given by Theorem 4.3.8. So, let us assume that F is algebraically closed, and set $M = R/(p^l)$ for some prime $p \in F[x]$. Since we are over an algebraically closed

field $p = x - c$ for some $c \in F$. Then the linear transformation ϕ associated to M is given by multiplication by x. Consider the F-vector space basis $[1], [x-c], [(x-c)^2], \ldots, [(x-c)^{l-1}]$ of M. The action of x (and hence also of ϕ) on this basis is

$$x \cdot (x-c)^i = \begin{cases} (x-c)^{i+1} + c(x-c)^i & \text{if } i < l-1 \\ c(x-c)^{l-1} & \text{if } i = l-1 \end{cases}$$

So, in this basis the matrix of ϕ is

$$\begin{pmatrix} c & 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & c & 1 & & 0 & 0 & 0 \\ 0 & 0 & c & & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & c & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & c & 1 \\ 0 & 0 & 0 & \ldots & 0 & 0 & c \end{pmatrix} \tag{4.0.b}$$

Corollary 4.4.1. *Jordan normal form. If F is an algebraically closed field, then for each linear transformation there is a basis in which its matrix is a block matrix with blocks as in (4.0.b).*

The great feature of this method is that it also gives normal forms over non closed fields, which will be discussed in the exercises (see exercises).

End of 3. class, on 04.10.2021.

Chapter 5

Homological algebra

5.1 Goal

The goal of Chapter 5 is to introduce a part of algebra called Homological algebra. Nowadays, this is mostly thought of not as a separate field of research, but rather an indispensable toolbox for all algebra related research areas such as topology, algebraic geometry, group theory, number theory, and for even differential geometry to some degree. The word indispensable should not be underestimated. All the above fields define and use different types of (co-)homology theories, using homological algebra, without which nowadays these fields would be unimaginable. Some of these (co-)homology theories are as follows:

- group theory: group-cohomology,
- number theory : Galois-cohomology,
- topology: all different kinds of (co-)homology theories such as singular-, CW- or simplicial (co-)homologies,
- algebraic geometry: sheaf-cohomology, étale-cohomology, etc.,
- differential geometry: De-Rham or Dolbeault-cohomology.

In this section we will learn the basics necessary to later in the followup courses you can learn the above theories. We will do this by working out one example of the machinery, by defining and learning the meaning of Ext-modules. The i-th Ext-module answer the question of how many i-degree extensions of two modules there are. Because the $i = 1$ case is the really used one, in this course we learn only what this means for $i = 1$. For two R-modules M and N, the R-module $\mathrm{Ext}^1(M, N)$ counts how many short exact sequences there are

$$0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0$$

up to an adequate equivalence relation.

For the entire Chapter 5 we fix a ring R (with identity). All the mentioned modules will be modules over R.

5.2 The $\mathrm{Hom}_R(\_, N)$ functor

The starting point of homological algebra is that the $Hom_R(\_N)$ functor is not exact. In particular the Ext-modules that we will define are the error terms which make $Hom_R(\_N)$ exact in some sense (Theorem 5.5.6). Hence, Section 5.2 is about explaining:

- what it means that $\mathrm{Hom}_R(\_, N)$ is a functor, and that

- what it means that it is left exact but not exact in general.

We do not define what functors are in general. Instead we state only what it means for $\mathrm{Hom}_R(\_, N)$ to be a contravariant functor, where N is a fixed R-module:

(1) *For every R-module M,*

$$\mathrm{Hom}_R(M,N) = \left\{ \phi : M \to N \;\middle|\; \phi \text{ is an } R\text{-module homomorphism} \right\}$$

is an R-module. Recall from point (10) of Example 2.2.4 that the module structure is give by multiplication in the target, that is for every $\phi \in \mathrm{Hom}_R(M,N)$ and $r \in R$ we have $(r\varphi)(m) = r\varphi(m)$.

(2) *For every R-module homomorphism $\alpha : M \to L$,*

$$\mathrm{Hom}_R(\alpha, N) : \mathrm{Hom}_R(L,N) \to \mathrm{Hom}_R(M,N)$$

is an R-module homomorphism. It is defined by the formula:

$$\mathrm{Hom}_R(L,N) \ni \phi \mapsto \phi \circ \alpha \in \mathrm{Hom}_R(M,N).$$

(3) *For all homomorphisms $\alpha : M \to L$ and $\beta : L \to K$ we have*

$$\mathrm{Hom}_R(\alpha, N) \circ \mathrm{Hom}_R(\beta, N) = \mathrm{Hom}_R(\beta \circ \alpha, N).$$

Indeed, for every $\phi \in \mathrm{Hom}_R(K,N)$ we have

$$\mathrm{Hom}_R(\alpha, N) \circ \mathrm{Hom}_R(\beta, N)(\phi) = \mathrm{Hom}_R(\alpha, N)(\phi \circ \beta) = \phi \circ \beta \circ \alpha = \mathrm{Hom}_R(\beta \circ \alpha, N).$$

The practical consequence of the above three points is that for every commutative diagram of R-modules, we may apply $\mathrm{Hom}_R(\_, N)$ to the commutative diagram, by which we mean:

- we replace every module M in the diagram by $\mathrm{Hom}_R(M,N)$,
- we replace every arrow α in the diagram by $\mathrm{Hom}_R(\alpha, N)$ by changing the direction of the arrow too,

The diagram we obtain this way then commutes by point (3) above.

Having explained what it means for $\mathrm{Hom}_R(\_, N)$ to be a functor, we explain in Lemma 5.2.2 what it means for $\mathrm{Hom}_R(\_, N)$ to be left exact, for which we need also a preparatory lemma:

Lemma 5.2.1. *Let $\alpha : M \to L$ and $\xi : M \to N$ be two R-module homomorphisms and assume that α is surjective. Then for any R-module N, we have $\xi \in \operatorname{im} \mathrm{Hom}_R(\alpha, N) \iff \ker \xi \supseteq \ker \alpha$.*

Proof. First we note that $\xi \in \operatorname{im} \mathrm{Hom}_R(\alpha, N)$ is equivalent to the existence of an R-module homomorphism $\phi : L \to N$ such that $\phi \circ \alpha = \xi$.

$\boxed{\Longrightarrow:}$ If ϕ as above exists, then $\ker \xi = \ker(\phi \circ \alpha) \supseteq \ker \alpha$.

$\boxed{\Longleftarrow:}$ Let us define ϕ as above by setting $\phi(x) = \xi(y)$ for all $x \in L$, where $y \in \alpha^{-1}(x)$ is arbitrary. This is well defined because if $y' \in \alpha^{-1}(x)$ another element, then $\xi(y') = \xi(y + (y' - y)) = \xi(y) + \xi(y' - y) = \xi(y)$, as $y' - y \in \ker \alpha \subseteq \ker \xi$.

The map ϕ is a module homomorphism because for $x, x' \in L$, $y \in \alpha^{-1}(x)$, $y' \in \alpha^{-1}(x')$ and $r \in R$ we have

$$\phi(x + x') \underset{\uparrow}{=} \xi(y + y') = \xi(y) + \xi(y') = \phi(x) + \phi(x')$$

$\boxed{\alpha \text{ is an } R\text{-module homomorphism, so } \alpha(y + y') = x + x'}$

and

$$\phi(rx) \underset{\uparrow}{=} \xi(ry) = r\xi(y) = r\phi(y)$$

α is an R-module homomorphism, so $\alpha(ry) = rx$

Finally, the equality $\phi \circ \alpha = \xi$ follows from the definition of ξ. □

Lemma 5.2.2. *For an R-module N, the functor $\mathrm{Hom}_R(\_, N)$ functor is left exact, which means (by definition) that for every short exact sequence of R-modules*

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} K \longrightarrow 0 \tag{2.2.a}$$

the complex pictured in (2.2.b) and obtained by applying $\mathrm{Hom}_R(\_, N)$ to (2.2.a) and deleting the 0 module at the end is exact:

$$\mathrm{Hom}_R(L, N) \xleftarrow{\mathrm{Hom}_R(\alpha,N)} \mathrm{Hom}_R(M, N) \xleftarrow{\mathrm{Hom}_R(\beta,N)} \mathrm{Hom}_R(K, N) \longleftarrow 0 \tag{2.2.b}$$

Proof. $\mathrm{Hom}_R(\beta, N)$ *is injective:* This is immediate, because if $\phi \in \mathrm{Hom}_R(K, N) \neq 0$ then by defintion there is a $x \in K$ such that $\phi(x) \neq 0$. As β is surjective, there is $y \in M$ such that $\beta(y) = x$. However, then

$$\Big(\mathrm{Hom}_R(\beta, N)(\phi)\Big)(y) \underset{\uparrow}{=} \phi(\beta)(y)) = \phi(x) \neq 0.$$

by the definition of $\mathrm{Hom}_R(\beta, N)$

This means by definition that $\mathrm{Hom}_R(\beta, N)(\phi) \neq 0$.

$\mathrm{im}\,\mathrm{Hom}_R(\beta, N) \subseteq \ker \mathrm{Hom}_R(\alpha, N)$: This is equivalent to the statement that $\mathrm{Hom}_R(\alpha, N) \circ \mathrm{Hom}_R(\beta, N) = 0$. However, property (3) above, $\mathrm{Hom}_R(\alpha, N) \circ \mathrm{Hom}_R(\beta, N) = \mathrm{Hom}_R(\beta \circ \alpha, N)$, which is 0 as so is $\beta \circ \alpha$.

$\mathrm{im}\,\mathrm{Hom}_R(\beta, N) = \ker \mathrm{Hom}_R(\alpha, N)$: This is shown by the following equivalences:

$$\phi \in \ker \mathrm{Hom}_R(\alpha, N) \iff \alpha \circ \phi = 0 \iff \mathrm{im}\,\alpha \subseteq \ker \phi \underset{\uparrow}{\iff} \ker \beta \subseteq \ker \phi \underset{\uparrow}{\iff} \phi \in \mathrm{im}\,\mathrm{Hom}_R(\beta, N)$$

$\mathrm{im}\,\alpha = \ker \beta$ as (2.2.a) is exact

Lemma 5.2.1

□

Remark 5.2.3. Similarly to the above definitions and statements, there is a corresponding story for $\mathrm{Hom}_R(M, \_)$. For example for an R-module homomorphism $\alpha : N \to L$, the map $\mathrm{Hom}_R(M, \alpha)$ is defined by

$$\mathrm{Hom}_R(M, N) \ni \phi \mapsto \alpha \circ \phi \in \mathrm{Hom}_R(M, L).$$

Then, if $\beta : L \to K$ is another R-module homomorphism, then the equality $\mathrm{Hom}_R(M, \beta) \circ \mathrm{Hom}_R(M, \alpha) = \mathrm{Hom}_R(M, \beta \circ \alpha)$ follows as property (3) above. Note that compared to property (3), here the orders of α and β in the composition changed. It will be a homework on the exercise sheet to show the version of Lemma 5.2.2 for $\mathrm{Hom}_R(M, \_)$.

Example 5.2.4. Finally we show the example showing that $\mathrm{Hom}_R(\_, N)$ is not exact, that is, we show a short exact sequence, such that $\mathrm{Hom}_R(\_, N)$ applied to it is not exact. Set $R := \mathbb{Z}$, and consider the following short exact sequence:

$$0 \longrightarrow b\mathbb{Z} \xrightarrow{x \mapsto 2x} b\mathbb{Z} \xrightarrow{x \mapsto x + 2\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \tag{2.4.c}$$

Applying $\mathrm{Hom}_{\mathbb{Z}}(\_, \mathbb{Z})$ to this exact sequence yields the following exact sequence, where exactness follows from Lemma 5.2.2:

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z} \xleftarrow[x \mapsto 2x]{} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z} \xleftarrow{} 0 = \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}\right) \xleftarrow{} 0$$

However, the map on the left is not surjective, as the image is $2\mathbb{Z}$. With other words (2.4.c) does not stay exact, when $\mathrm{Hom}_{\mathbb{Z}}(\_, \mathbb{Z})$ is applied to it.

5.3 Ext-MODULES GIVEN BY FREE RESOUTIONS

As we have hinted at the beginning of Section 5.2, the Ext-modules can be thought of as correction terms for the failure of exactness of $\mathrm{Hom}(\_, N)$. The main idea is that $\mathrm{Hom}(\_, N)$ really becomes exact if we replace our modules on which we apply it with certain chain complexes:

Definition 5.3.1. A sqeuence of R-modules (see Definition 2.2.7) is also called a *complex* of R-modules. A *chain complex* of R-modules is a complex of R-modules

$$M_\bullet : \ldots \xrightarrow{f_{n+2}} M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \xrightarrow{f_{n-1}} \ldots$$

such that for all integers i the following equivalent conditions hold:

$$\mathrm{im}\, f_{i+1} \subseteq \ker f_i \iff f_i \circ f_{i+1} = 0.$$

A *cochain complex* is defined analogously, but the indices are increasing instead of decreasing.

The *i-th homology group* of a chain complex $M_\bullet$ as above is

$$H_i(M_\bullet) := \ker f_i / \mathrm{im}\, f_{i+1}.$$

The *cohomology* of a cochain complex is defined analogously and it is denoted by $H^i(M_\bullet)$.

A chain complex $M_\bullet$ is *bounded above* (resp. *bounded below*), if $M_i = 0$ for all $i > n$ (resp. for all $i < n$) for some integer n. In this case, we usually write at most one 0 term. In the same spirit, if a (co-)chain complex stops at a given point, we think about the rest of the indices containing a 0 module.

Remark 5.3.2. Matching Definition 2.2.7 and Definition 5.3.1, we obtain that a complex $M_\bullet$ is *exact* if and only if $H_i(M_\bullet) = 0$ for all $i \in \mathbb{Z}$.

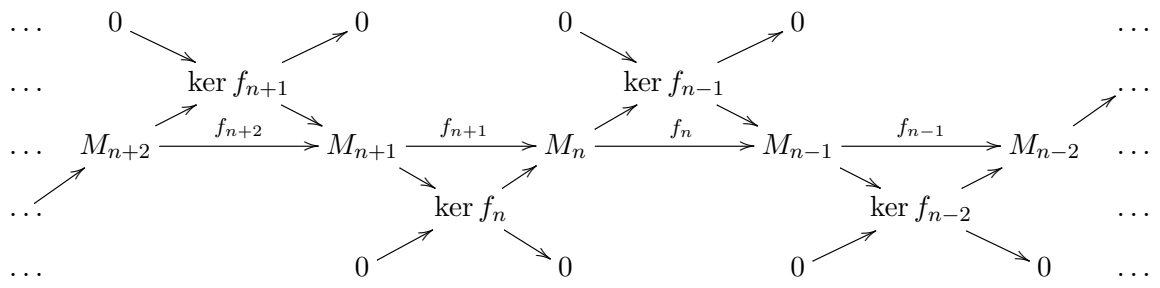
Remark 5.3.3. Giving an exact sequence

$$\mathcal{M} : \ldots \xrightarrow{f_{n+2}} M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \xrightarrow{f_{n-1}} \ldots$$

is equivalent to giving a collection of short exact sequences

$$\{\, 0 \longrightarrow \ker f_i \longrightarrow M_i \xrightarrow{f_i} \ker f_{i-1} \longrightarrow 0 \,\}_{i \in \mathbb{Z}}.$$

With a picture,



Remark 5.3.4. We may apply $\mathrm{Hom}_R(\_, N)$ to chain complexes. This way we obtain a cochain complex again by property (3) above. The property $f_{i+1} \circ f_i = 0$ is preserved, because $\mathrm{Hom}_R(\_, N)$ is a functor, and because $\mathrm{Hom}_R(0, N) = 0$, where the 0's denote the zero homomorphisms.

As we mentioned in the introduction of Section 5.3, the main idea is that $\mathrm{Hom}(\_, N)$ really becomes exact if we replace our modules on which we apply it with certain chain complexes. These chain complexes are called free resolutions:

Definition 5.3.5. A *free resolution* of an R-module M is a chain complex of free modules as follows:

$$F_\bullet : \ldots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0$$

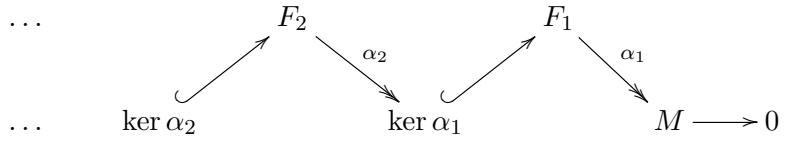
that becomes exact when attaching an M to it:

$$\ldots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

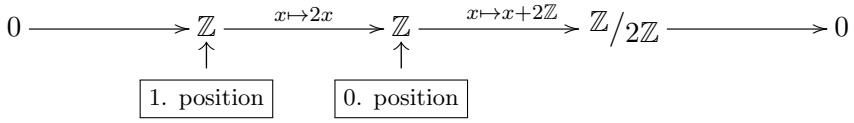
For an R-module N, the *i-th* Ext-*module* of M and N given by the free resolution $F_\bullet$ and is defined by

$$\mathrm{Ext}^i_{F_\bullet}(M, N) := H^i\big(\mathrm{Hom}(F_\bullet, N)\big)$$

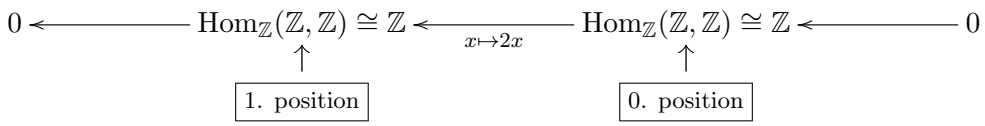
Remark 5.3.6. Every module is a surjective mage of a free module. Hence, free resolutions always exist.



Example 5.3.7. Set $R := \mathbb{Z}$ and $M := \mathbb{Z}/2\mathbb{Z}$. Then a free resolution is the following exact chain complex



Dropping the $\mathbb{Z}/2\mathbb{Z}$ from the beginning, and applying $\mathrm{Hom}_\mathbb{Z}(\_, \mathbb{Z})$ to this exact sequence yields the cochain complex



Taking cohomology then yields then

$$\mathrm{Ext}^0_{F_\bullet}\left(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}\right) = 0 \qquad \mathrm{Ext}^1_{F_\bullet}\left(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}\right) \cong \mathbb{Z}/2\mathbb{Z}$$

Proposition 5.3.8. *Let M be a module over R, and let $F_\bullet$ be a free resolution of M. Then,* $\mathrm{Ext}^0_R(M, N) \cong \mathrm{Hom}_R(M, N)$.

Proof. Consider the first two terms of a free resolution $\alpha : F_1 \to F_0$ of M. This yields two exact sequences

$$0 \longrightarrow \mathrm{im}\,\alpha \xrightarrow{\iota} F_0 \longrightarrow M \longrightarrow$$

and

$$0 \longrightarrow \ker \alpha \longrightarrow F_1 \xrightarrow{\beta} \in \alpha \longrightarrow$$

Applying $\mathrm{Hom}_R(\_, N)$ yields the following commutative diagram, where the row is exact by Lemma 5.2.2, and $\mathrm{Hom}_R(\beta, N)$ is also injective by Lemma 5.2.2:

$$\begin{array}{ccccccc} \mathrm{Hom}_R(F_1,N) & & & & & & \\ {\scriptstyle \mathrm{Hom}_R(\beta,N)}\uparrow & \nwarrow^{\mathrm{Hom}_R(\alpha,N)} & & & & & \\ \mathrm{Hom}_R(\mathrm{im}\,\alpha,N) & \xleftarrow[\mathrm{Hom}_R(\iota,N)]{} & \mathrm{Hom}_R(F_0,N) & \longleftarrow & \mathrm{Hom}_R(M,N) & \longleftarrow & 0 \end{array} \tag{3.8.a}$$

Then

$$\begin{array}{ccccc} \mathrm{Ext}^0_R(M,N) & \cong & \ker \mathrm{Hom}_R(\alpha,N) & = & \ker \mathrm{Hom}_R(\iota,N) \cong \mathrm{Hom}_R(M,N). \\ \uparrow & & \uparrow & & \uparrow \\ \boxed{\text{by definition}} & & \boxed{\begin{array}{l}\mathrm{Hom}_R(\beta,N) \text{ is injective} \\ \text{and (3.8.a) commutes}\end{array}} & & \boxed{\text{the row of (3.8.a) is exact}} \end{array}$$

□

Example 5.3.9. Consider the modification of Example 4.1.2 where one replaces x and y, by two arbitrary linearly independent linear combinations $ax + by$ and $cx + dy$ of x and y. For each such choice of linear combinations we obtain following the construction of Example 4.1.2 a free resolution of the $R = k[x, y]$-module $(ax+by, cx+dy) = (x, y)$, where the last equality is given by the linear independent assumption. We denote the quotient R-module $k[x,y]\big/(x,y)$ by simply k. Then, for each choice of a, b, c and d we obtain a different free resolution of k:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \longrightarrow & R\oplus R & \longrightarrow & R & \longrightarrow & k & \longrightarrow & 0 \\ & & 1 & \longmapsto & \big(cx+dy, -(ax+by)\big) & & & & & & \\ & & & & (1,0) & \longmapsto & ax+by & & & & \\ & & & & (0,1) & \longmapsto & cx+dy & & & & \end{array} \tag{3.9.b}$$

Additionally, one can add "dummy" summands to further construct different free resolutions:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R\oplus R & \longrightarrow & R\oplus R\oplus R & \longrightarrow & R & \longrightarrow & k & \longrightarrow & 0 \\ & & (1,0) & \longmapsto & \big(cx+dy, -(ax+by), 0\big) & & & & & & \\ & & (0,1) & \longmapsto & (0,0,1) & & & & & & \\ & & & & (1,0,0) & \longmapsto & ax+by & & & & \\ & & & & (0,1,0) & \longmapsto & cx+dy & & & & \\ & & & & (0,0,1) & \longmapsto & 0 & & & & \end{array} \tag{3.9.c}$$

That is, a module (k in the present example) has many different free resolutions with free modules of different ranks, and with vastly varying maps. Let us compute now the groups $\mathrm{Ext}^i_{F_\bullet}(k, R)$, where $F_\bullet$ is the free resolution in (3.9.b). For this first we should apply $\mathrm{Hom}_R(\_, R)$ to $F_\bullet$:

$$\begin{array}{ccccccc} 0 & \xleftarrow[\eta]{} & R & \longleftarrow & R\oplus R & \longleftarrow & R \longleftarrow 0 \\ & & cx+dy & \longmapsto & (1,0) & & \\ & & -ax+by & \longmapsto & (0,1) & & \\ & & & & (ax+by, cx+dy) & \longmapsto & 1 \end{array}$$

Taking cohomology yields

$$\mathrm{Ext}^0_{F_\bullet}(k,R) = \mathrm{Ext}^1_{F_\bullet}(k,R) = 0 \text{ and } \mathrm{Ext}^2_{F_\bullet}(k,R) \cong k$$

The surprising aspect of the result of our computation is that although we considered different free resolutions paramterized by a, b, c and d, the obtained Ext-groups are the same. We leave it as an exercise that in fact the free resolutions of (3.9.c) yield again the same Ext-groups.

5.4 PROJECTIVE MODULES AND RESOLUTIONS

In Example 5.3.9 we have seen that one module can have many free resolutions. On the other hand, we have also seen in Example 5.3.9 that the Ext-groups for the considered free resolutions surprisingly are still the same. One might wonder whether the modules $\mathrm{Ext}^i_{F_\bullet}(M,N)$ maybe do not actually depend on the choice of $F_\bullet$. In fact, this is true. The main idea is that for two different free resolutions $F^1_\bullet$ and $F^2_\bullet$ one can define a map between the two resolutions that has enough unicity properties to induce unique isomorphisms on the Ext-groups. The property needed to run this argument is abstracted by the notion of a projective module, and hence the whole argument works for projective resolutions.

Definition 5.4.1. An R-module P is *projective* if for every surjective morphism of R-modules $\beta\colon N \twoheadrightarrow M$ and every morphism of R-modules $\alpha\colon P \to M$ there exists a morphism $\gamma\colon P \to N$ of R-modules such that $\alpha = \beta \circ \gamma$.

Remark 5.4.2. (1) The definition of projective module can be summarized in the following way: P is projective if any diagram

$$\begin{array}{ccc} & & P \\ & & \downarrow{\scriptstyle \alpha} \\ N & \xrightarrow{\beta} & M \end{array}$$

of R-modules M, N and morphisms α, β with β surjective can be completed to a diagram

$$\begin{array}{ccc} & \overset{\gamma}{\swarrow} & P \\ & & \downarrow{\scriptstyle \alpha} \\ N & \xrightarrow{\beta} & M \end{array}$$

where γ is also a morphism of R-modules.

(2) By definition of the $\mathrm{Hom}_R(M,\_)$ functor (see Remark 5.2.3), Definition 5.4.1 is equivalent to saying that P is projective if and only if $\mathrm{Hom}_R(P,\_)$ takes surjective homomorphisms to surjective homomorphisms. Taking into account the exercise on the exercise sheet where you proved that $\mathrm{Hom}_R(M,\_)$ is left exact, this is equivalent to requiring that $\mathrm{Hom}_R(P,\_)$ takes short exact sequences to short exact sequences (including the two 0's at the end). This is just the definition for $\mathrm{Hom}_R(P,\_)$ being an exact functor. To sum up, Definition 5.4.1 is equivalent to requiring that $\mathrm{Hom}_R(P,\_)$ is an exact functor.

Example 5.4.3. Every free module is a projective module. Indeed, assume that F is a free module with free generators $\{a_i\}_{i\in I}$, that $\alpha : M \to N$ is a surjective morphism of modules and $\beta : F \to N$ is a morphism of modules. For every $i \in I$, let $m_i \in M$ such that $\alpha(m_i) = \beta(a_i)$. Then by Proposition 2.2.17 there is a unique morphism $\gamma : F \to M$ that sends $a_i \to m_i$ for all $i \in I$.

To see that $\alpha\circ\gamma = \beta$ holds, by the universal property of direct sums (Proposition 2.2.17) one just need to verify that $\alpha \circ \gamma$ and β take a_i to the same elements, which holds by construction.

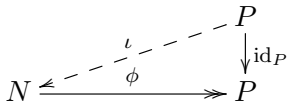
Proposition 5.4.4. *Let R be a ring and P an R-module. Then the following are equivalent:*

(1) P is projective,

(2) there exists an R-module M such that $P \oplus M$ is a free module.

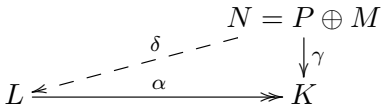
Proof. *(1) $\Longrightarrow$ (2)* According to an exercise on the exercise sheet it is enough to find a free module N, a surjection $\phi : N \twoheadrightarrow P$ and a splitting $s : P \to N$, which by definition means htat $s \circ \phi = \mathrm{id}_P$. In fact we claim that such a splitting exists for any ϕ. Additionally such a ϕ exists because by Proposition 2.2.17 it is equivalent to giving a generator set of P.

Having figured out the existence of a ϕ as above, the existence of a splitting is given by applying Definition 5.4.1 to the following diagram



(2) $\Longrightarrow$ (1) Let $N = P \oplus M$ be a free module. We have to show that Definition 5.4.1 holds for P. So take a surjective homomorphism $\alpha : L \to K$ and an arbitrary homomorphism $\beta : P \to K$. Set $\gamma : N \to K$ be the composition of β with the projection $N \to P$. In particular we can identify $\gamma|_{P \oplus 0}$ with β.

As free modules are projective (Example 5.4.3) we have a lift of γ as in the following commutative diagram



□

Example 5.4.5. Proposition 5.4.4 and Theorem 4.3.8 imply that if R is a PID and let P is a finitely generated R-module, then the following are equivalent:

(1) P is projective;

(2) P is free;

(3) P is torsion free.

Definition 5.4.6. A *projective resolution* of an R-module M is an exact sequence of projective R-modules

$$P_\bullet : \ldots \xrightarrow{f_{i+2}} P_{i+1} \xrightarrow{f_{i+1}} P_i \xrightarrow{f_i} P_{i-1} \xrightarrow{f_{i-1}} \ldots \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0$$

together with an R-module homomorphism $f : M_0 \to M$, such that the sequence

$$\ldots \xrightarrow{f_{i+2}} P_{i+1} \xrightarrow{f_{i+1}} P_i \xrightarrow{f_i} P_{i-1} \xrightarrow{f_{i-1}} \ldots \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \xrightarrow{f} M \longrightarrow 0$$

is exact.

If $P_\bullet$ is a projective resolution, one defines the associated Ext-modules $\mathrm{Ext}^i_{P_\bullet}(M, N)$ as for free resolutions.

As explained earlier our goal is to show that $\mathrm{Ext}^i_{P_\bullet}(M, N)$ is independent of $P_\bullet$, and we are going to do this by constructing maps between different projective resolutions. First we define these maps carefully:

Definition 5.4.7. A *morphism ϕ of chain complexes* of R-modules

$$F_\bullet: \quad \ldots \longrightarrow F_{i+1} \xrightarrow{f_{i+1}} F_i \xrightarrow{f_i} F_{i-1} \longrightarrow \ldots$$

$$G_\bullet: \quad \ldots \longrightarrow G_{i+1} \xrightarrow{g_{i+1}} G_i \xrightarrow{g_i} G_{i-1} \longrightarrow \ldots$$

is a collection $\phi_i : F_i \to G_i$ of R-module homomorphisms for all integers i, such that $g_i \circ \phi_i = \phi_{i-1} \circ f_i$ for all integers i.

A *morphism of cochain complexes* is defined analogously.

We use the notation ϕ and $\phi_\bullet$ for morphisms of (co-)chain complexes interchangeably.

Remark 5.4.8. A morphism of chain complexes $F_\bullet, G_\bullet$ is nothing but a diagram of R-modules and morphisms

$$\begin{array}{lccccccc} F_\bullet: & \ldots \longrightarrow & F_{i+1} & \xrightarrow{f_{i+1}} & F_i & \xrightarrow{f_i} & F_{i-1} & \longrightarrow \ldots \\ & & \downarrow{\scriptstyle \phi_{i+1}} & & \downarrow{\scriptstyle \phi_i} & & \downarrow{\scriptstyle \phi_{i-1}} & \\ G_\bullet: & \ldots \longrightarrow & G_{i+1} & \xrightarrow{g_{i+1}} & G_i & \xrightarrow{g_i} & G_{i-1} & \longrightarrow \ldots \end{array}$$

such that for every i the maps in every square

$$\begin{array}{ccc} F_i & \xrightarrow{f_i} & F_{i-1} \\ \downarrow{\scriptstyle \phi_i} & & \downarrow{\scriptstyle \phi_{i-1}} \\ G_i & \xrightarrow{g_i} & G_{i-1} \end{array}$$

commute. This means that in each square as above $\phi_{i-1} \circ f_i = g_i \circ \phi_i$.

End of 4. class, on 11.10.2021.

Remark 5.4.9. Applying Definition 5.4.7 to the chain complexes given by two projective resolutions $P_\bullet$ and $Q_\bullet$ of the same module M, we are able to say what morphisms of chain complexes we will use to show that $\mathrm{Ext}^i_{P_\bullet}(M,N) \cong \mathrm{Ext}^i_{Q_\bullet}(M,N)$ via a uniquely determined isomorphism: as shown in the next diagram we will append M to the -1-positions of these two projective resolutions and then we will take a moprhism of chain complexes extending id_M in the -1 position:

$$\begin{array}{ccccccc} \ldots \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M \\ & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_0} & & \downarrow{\scriptstyle \mathrm{id}_M} \\ \ldots \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & M \end{array}$$

Consider a morphism of chain complexes as in Remark 5.4.9. Applying $\mathrm{Hom}_R(\_, N)$ yields a morphism of cochain complexes. To see that we obtain a homomorphism $\mathrm{Ext}^i_{Q_\bullet}(M,N) \to \mathrm{Ext}^i_{P_\bullet}(M,N)$ we are supposed to show that a morphism of cochain complexes induces a homomorphism on cohomology:

Proposition 5.4.10. *A morphism of cochain-(resp. chain-)complexes of R-modules $\phi_\bullet : F_\bullet \to G_\bullet$ induces a homomorphism $H^i(\phi) : H^i(F_\bullet) \to H^i(G_\bullet)$ (resp. $H_i(\phi) : H_i(F_\bullet) \to H_i(G_\bullet)$) of R-modules defined by applying ϕ_i to any representative $\overline{x} \in F_i$ of a given $x \in H^i(F_\bullet)$.*

Proof. We show only the cochain complex version of the statement, as the chain complex version is verbatim the same up to the adequate change of indices.

Denote by $f_i : F_i \to F_{i+1}$ and $g_i : G_i \to G_{i+1}$ the structure homomorphisms of the cochain complexes $F_\bullet$ and $G_\bullet$ respectively. Then:

- $\boxed{\phi_i(\ker f_i) \subseteq \ker g_i\text{:}}$ if $x \in \ker f_i$, then

$$g_i\left(\phi_i(x)\right) \underset{\uparrow}{=} \phi_{i+1}\big(f_i(x)\big) \underset{\uparrow}{=} \phi_{i+1}(0) = 0.$$

$\boxed{\phi_\bullet \text{ is a morphism of cochain complexes}}$ $\boxed{x \in \ker f_i}$

- $\boxed{\phi_i(\operatorname{im} f_{i-1}) \subseteq \operatorname{im} g_{i-1}\text{:}}$ if $x \in \operatorname{im} f_{i-1}$, then $x = f_{i-1}(y)$ for some $y \in F_{i-1}$, and hence

$$\phi_i(x) = \phi_i\big(f_{i-1}(y)\big) \underset{\uparrow}{=} g_{i-1}\big(\phi_{i-1}(y)\big) \in \operatorname{im} g_{i-1}.$$

$\boxed{\phi_\bullet \text{ is a morphism of cochain complexes}}$

- $\boxed{H^i(\phi) \text{ is an } R\text{-module homomorphism:}}$ The previous two points tell us that there is an induced commutative diagram as follows, where ξ is the quotient homomorphism:

$$\begin{array}{ccccc} \operatorname{im} f_{i-1} & \hookrightarrow & \ker f_i & \longrightarrow & \ker f_i/\operatorname{im} f_{i-1} = H^i(F_\bullet) \\ \downarrow{\scriptstyle \phi_i} & & \downarrow{\scriptstyle \phi_i} & \nearrow{\scriptstyle \xi\circ\phi_i} & \\ \operatorname{im} g_{i-1} & \hookrightarrow & \ker g_i & \xrightarrow[\xi]{} & \ker g_i/\operatorname{im} g_{i-1} = H^i(G_\bullet) \end{array} \tag{4.10.a}$$

$H^i(\phi)$ is the unique homomorphism $H^i(F_\bullet) \to H^i(G_\bullet)$ given by the universal property of quotients, that is, by applying Lemma 5.2.1 to F_i, $H^i(F_\bullet)$ and to $H^i(G_\bullet)$. Note that to apply Lemma 5.2.1 we have to verify that $\operatorname{im} f_{i-1} \subseteq \ker(\xi \circ \phi_i)$. This follows from the commutativity of (4.10.a):

$$\xi \circ \phi_i \circ f_{i-1} \underset{\uparrow}{=} \xi \circ g_{i-1} \circ \phi_{i-1} \underset{\uparrow}{=} 0$$

$\boxed{\text{commutativity of (4.10.a)}}$ $\boxed{\xi \circ g_{i-1} = 0}$

□

Remark 5.4.11. If $\phi_\bullet : F_\bullet \to G_\bullet$ and $\psi_\bullet : G_\bullet \to H_\bullet$ are two morphisms of (co-)chain complexes. Then from the definition it follows immediately that $\psi_\bullet \circ \phi_\bullet : F_\bullet \to H_\bullet$ is also a morphism of (co-)chain complexes.

In this situation, from the definition of $H^i(\_)$ (resp. of $H_i(\_)$) one obtains $H^i(\psi \circ \phi) = H^i(\psi) \circ H^i(\phi)$ (resp. $H_i(\psi \circ \phi) = H_i(\psi) \circ H_i(\phi)$).

Proposition 5.4.10 yieds that given a morphism of chain complexes as in Remark 5.4.9, there is an induced homomorphism $\operatorname{Ext}^i_{Q_\bullet}(M,N) \to \operatorname{Ext}^i_{P_\bullet}(M,N)$. However, given two projective resolutions $P_\bullet$ and $Q_\bullet$ of the same R-module M there are many chain complex homomorphisms lifting id_M as in Remark 5.4.9. Hence, if we want to show that the induced maps on $\operatorname{Ext}^i_{Q_\bullet}(M,N) \to \operatorname{Ext}^i_{P_\bullet}(M,N)$ are unique, we need a machinery to understand when two morphisms of (co-)chain complexes induce the same homomorpism on (co-)homology. The idea here is borrowed from topology: homotopy equivalent continuous maps induce the same homomorphism on all associated invariants of topological spaces, such as the fundamental groups, singular homology or singular cohomology. Hence, we define homotopy for morphisms of (co-)chain complexes:

Definition 5.4.12. For two morphisms of chain complexes of R-modules $\phi, \psi : F_\bullet \to G_\bullet$ we say that ϕ is *homotopy equivalent* to ψ if there exists a collection of R-module homomorphisms $h_i : F_i \to G_{i+1}$ for all integers i, such that

$$\phi_i - \psi_i = g_{i+1} \circ h_i + h_{i-1} \circ f_i. \tag{4.12.b}$$

where $f_i : F_i \to F_{i-1}$ and $g_i : G_i \to G_{i-1}$ are the structure homomorphisms of $F_\bullet$ and $G_\bullet$, respectively.

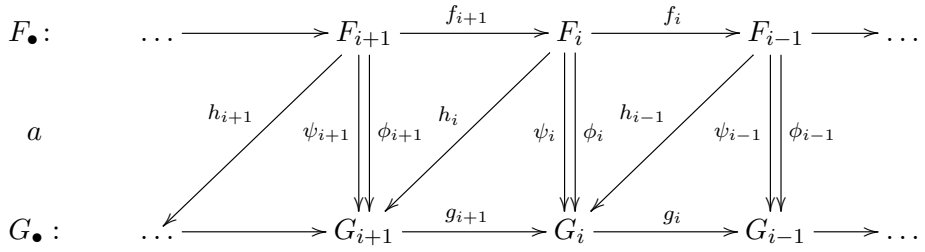
For cohain complexes the definition is similar, but with a change of indexing (we denoted the differences by red color): for two morphisms of cochain complexes $\phi, \psi : F_\bullet \to G_\bullet$ we say that ϕ is *homotopy equivalent* to ψ if there exists a collection of R-module homomorphisms $h_i : F_i \to G_{i-1}$ for all integers i, such that

$$\phi_i - \psi_i = g_{i-1} \circ h_i + h_{i+1} \circ f_i. \tag{4.12.c}$$

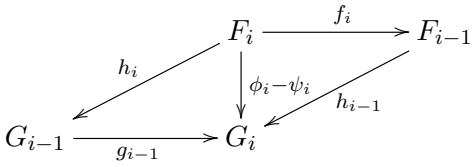
where $f_i : F_i \to F_{i+1}$ and $g_i : G_i \to G_{i+1}$ are the structure homomorphisms of $F_\bullet$ and $G_\bullet$, respectively.

We denote that ϕ is homotopy equivalent to ψ by $\phi \sim \psi$.

Remark 5.4.13. Two morphisms of chain complexes of R-modules $\phi, \psi \colon F_\bullet, G_\bullet$ are homotopy equivalent if there is a collection of morphisms $\{h_i\}$ and a diagram of R-modules and morphisms



such that for any i in parallelogram



the equation (4.12.b) holds.

Remark 5.4.14. It follows directly from Definition 5.4.12 that two morphisms of (co-)chain complexes φ, ψ are homotopy equivalent if and only if $\varphi - \psi$ is homotopy equivalent to 0.

(Note that R-linear combinations of morphisms of (co-)chain complexes are also morphisms of (co-)chain complexes. This is an easy verification of the definition of a morphism of (co-)chain complex, that is, of Definition 5.4.7. We leave this verification to the reader.)

Remark 5.4.15. If h_i yield a homotopy between the chain complex morphisms $\phi, \psi : F_\bullet \to G_\bullet$, then for any R-module N the homomorphisms $\mathrm{Hom}_R(h_i, N)$ yield a homotopy between the chain complex morphisms $\mathrm{Hom}_R(\phi, N), \mathrm{Hom}_R(\psi, N) : \mathrm{Hom}_R(G_\bullet, N) \to \mathrm{Hom}_R(F_\bullet, N)$. To see this,one needs to show that applying $\mathrm{Hom}_R(\_, N)$ to (4.12.b) is turned into the version of (4.12.c) where $\mathrm{Hom}_R(\_, N)$ is applied to all elements:

$$\mathrm{Hom}_R(\phi_i, N) - \mathrm{Hom}_R(\psi_i, N) = \mathrm{Hom}_R(g_{i-1}, N) \circ \mathrm{Hom}_R(h_i, N) + \mathrm{Hom}_R(h_{i+1}, N) \circ \mathrm{Hom}_R(f_i, N).$$

To show this, besides the functoriality properties of $\mathrm{Hom}_R(\_, N)$ explained in Section 5.2, the following additivity properties have to be used, where α and β are R-module homomorphisms $M \to L$ and N is an arbitrary R-modules:

(1) $\boxed{\mathrm{Hom}_R(\alpha, N) + \mathrm{Hom}_R(\beta, N) = \mathrm{Hom}_R(\alpha + \beta, N)\text{:}}$ by definition of the $\mathrm{Hom}_R(\_, N)$ functor this is equivalent to the following statements

$$\forall \xi \in \mathrm{Hom}_R(L, N) : \ \xi \circ \alpha + \xi \circ \beta = \xi \circ (\alpha + \beta).$$

$$\Updownarrow$$

$$\forall \xi \in \mathrm{Hom}_R(L,N), \forall m \in M: \ (\xi \circ \alpha + \xi \circ \beta)(m) = \big(\xi \circ (\alpha+\beta)\big)(m).$$

However, by the definition of addition on $\mathrm{Hom}_R(M,L)$ the both sides of the latter equation are equal to $\xi(\alpha(m)) + \xi(\beta(m))$.

(2) $\boxed{\mathrm{Hom}_R(-\alpha, N) = -\mathrm{Hom}_R(\alpha, N)\text{:}}$ by definition of the $\mathrm{Hom}_R(\_, N)$ functor this is equivalent to the following statements

$$\forall \xi \in \mathrm{Hom}_R(L,N): \ \xi \circ (-\alpha) = -\xi \circ \alpha.$$

$$\Updownarrow$$

$$\forall \xi \in \mathrm{Hom}_R(L,N), \forall m \in M: \ \big(\xi \circ (-\alpha)\big)(m) = (-\xi \circ \alpha)(m).$$

However, by the definition of addition on $\mathrm{Hom}_R(M,L)$ the both sides of the latter equation are equal to $-\xi(\alpha(m))$.

We note that the above two properties of the $\mathrm{Hom}_R(\_, N)$ functor are summarized by saying that the $\mathrm{Hom}_R(\_, N)$ functor is *additive*.

Remark 5.4.16. By the additivity poperties of the $\mathrm{Hom}_R(\_, N)$ functor explained in Remark 5.4.15 we also obtain that *homotopy equivalence is an equivalence relation on the R-module of morphisms of two (co-)chain complexes*. For this one has to verify the three properties of being an equivalence relation, that is, for all morphisms $\phi, \psi, \xi : F_\bullet \to G_\bullet$ of (co-)chain complexes one needs to show

(1) $\boxed{\textit{Reflexivity: } \phi \sim \phi\text{:}}$ as $\phi_i - \phi_i = 0$ take the $h_i = 0$ in (4.12.b) and

(2) $\boxed{\textit{Symmetry: } \phi \sim \psi \Longrightarrow \psi \sim \phi\text{:}}$ if h_i is the homotopy giving $\phi \sim \psi$ then by the additivity properties, $-h_i$ works to show that $\psi \sim \phi$.

(3) $\boxed{\textit{Transitivity: } \phi \sim \psi \textit{ and } \psi \sim \xi \textit{ implies } \phi \sim \xi}$ As $\phi - \xi = (\phi - \psi) + (\psi - \xi)$, if h_i and h'_i give $\phi \sim \psi$ and $\psi \sim \xi$, then $h_i + h'_i$ give $\phi \sim \xi$. Here we again use that composition commutes with addition as explained in Remark 5.4.15.

Proposition 5.4.17. *If $\phi, \psi : F_\bullet \to G_\bullet$ are homotopy equivalent maps of (co-)chain complexes, then φ and ψ induce the same morphisms on (co-)homology.*

Proof. We show only the cochain complex case, and we leave to the reader the chain complex case. Given $i \in \mathbb{Z}$ choose $a \in H^i(F_\bullet)$ and a lift $\overline{a} \in \ker f_i$. By Proposition 5.4.10, $\big(H^i(\phi)\big)(a)$ is the lift of the following element of G_i:

$$\phi_i(\overline{a}) \underset{\uparrow}{=} \psi_i(\overline{a}) + g_{i-1}\big(h_i(\overline{a})\big) + h_{i+1}\big(f_i(\overline{a})\big) \underset{\uparrow}{=} \psi_i(\overline{a}) + g_{i-1}\big(h_i(\overline{a})\big).$$

$\boxed{(4.12.b)}$ $\qquad\qquad$ $\boxed{a \in \ker f_i}$

which is just a lift of $\big(H^i(\psi)\big)(a)$. □

Definition 5.4.18. Two complexes $F_\bullet$ and $G_\bullet$ are homotopy equivalent if there are morphisms of complexes $\phi_\bullet : F_\bullet \to G_\bullet$ and $\psi_\bullet : G_\bullet \to F_\bullet$ such that $\phi \circ \psi \sim \mathrm{id}_{G_\bullet}$ and $\psi \circ \phi \sim \mathrm{id}_{F_\bullet}$.

Corollary 5.4.19. *Let $F_\bullet$ and $G_\bullet$ be homotopy equivalent (co-)chain complexes, and let $\phi_\bullet : F_\bullet \to G_\bullet$ and $\psi_\bullet : G_\bullet \to F_\bullet$ be the morphisms of (co-)chain complexes such that $\phi \circ \psi \sim \mathrm{id}_{G_\bullet}$ and $\psi \circ \phi \sim \mathrm{id}_{F_\bullet}$.*

Then, for all $i \in \mathbb{Z}$, the R-module homomorphisms $H_i(\psi)$ and $H_i(\phi)$ (resp. $H^i(\psi)$ and $H^i(\phi)$) are isomorphisms between $H_i(F_\bullet)$ and $H_i(G_\bullet)$.

Proof. We show only the cochain complex version of the statement, as the chain complex version is verbatim the same up to the adequate change of indices. By Remark 5.4.11 we obtain that

$$H^i(\psi) \circ H^i(\phi) = H^i\left(\mathrm{id}_{F_\bullet}\right) = \mathrm{id}_{H^i(F_\bullet)} \qquad \text{and} \qquad H^i(\phi) \circ H^i(\psi) = H^i\left(\mathrm{id}_{G_\bullet}\right) = \mathrm{id}_{H^i(G_\bullet)}.$$

Hence, $H^i(\psi)$ and $H^i(\phi)$ induce isomorphism $H^i(F_\bullet) \cong H^i(G_\bullet)$. □

Theorem 5.4.20. *Let*

$$F_\bullet: \quad \ldots \longrightarrow F_{i+1} \xrightarrow{f_{i+1}} F_i \xrightarrow{f_i} F_{i-1} \longrightarrow \ldots \qquad \ldots \xrightarrow{f_1} F_0 \longrightarrow 0$$

$$G_\bullet: \quad \ldots \longrightarrow G_{i+1} \xrightarrow{g_{i+1}} G_i \xrightarrow{g_i} G_{i-1} \longrightarrow \ldots \qquad \ldots \xrightarrow{g_1} G_0 \longrightarrow 0$$

be chain complexes of modules, such that F_i are projective for all integers i, and $H_i(G_\bullet) = 0$ for all $i > 0$.

Then, for every morphism $\alpha : H_0(F_\bullet) \to H_0(G_\bullet)$ of modules there exists a morphism of chain complexes $\phi_\bullet : F_\bullet \to G_\bullet$ such that $H_0(\phi) = \alpha$. Additionally, such $\phi_\bullet$ is unique up to homotopy equivalence.

Proof. *Step 1: consruction of ϕ_0:* Consider the diagram

$$\begin{array}{ccc} F_0 & \twoheadrightarrow & H_0(F_\bullet) \\ \downarrow{\scriptstyle \phi_0} & & \downarrow{\scriptstyle \alpha} \\ G_0 & \twoheadrightarrow & H_0(G_\bullet) \end{array}$$

The projectivity of F_0 yields the existence of the dashed arrow such that the diagram commutes.

Step 2: construction of ϕ_i for $i > 0$ inductively: Assume ϕ_j are constructed for $j < i$ such that the following diagram commutes (in the $i = 1$ case we take $F_{-1} = H_0(F_\bullet)$, $G_{-1} = H_0(G_\bullet)$ and $\phi_{-1} = \alpha$):

$$\begin{array}{ccccccccc} \ldots & \xrightarrow{f_{i+1}} & F_i & \xrightarrow{f_i} & F_{i-1} & \xrightarrow{f_{i-1}} & F_{i-2} & \xrightarrow{f_{i-2}} & \ldots \\ & & & & \downarrow{\scriptstyle \phi_{i-1}} & & \downarrow{\scriptstyle \phi_{i-2}} & & \\ \ldots & \xrightarrow[g_{i+1}]{} & G_i & \xrightarrow[g_i]{} & G_{i-1} & \xrightarrow[g_{i-1}]{} & G_{i-2} & \xrightarrow[g_{i-2}]{} & \ldots \end{array} \tag{4.20.d}$$

We are going to prove that the diagram can be extended with ϕ_i. First, *we claim that*:

$$\mathrm{im}(\phi_{i-1} \circ f_i) \subseteq \mathrm{im}\, g_i. \tag{4.20.e}$$

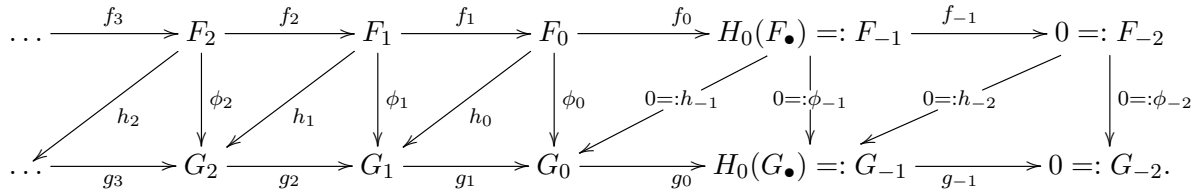
As $\mathrm{im}\, g_i = \ker g_{i-1}$ by the $H_i(G_\bullet) = 0$ assumption, (4.20.e) is equivalent to the equality $g_{i-1} \circ \phi_{i-1} \circ f_i = 0$. By the commutativity of (4.20.d), we have $g_{i-1} \circ \phi_{i-1} \circ f_i = \phi_{i-2} \circ f_{i-1} \circ f_i$, which is zero as $F_\bullet$ is a chain complex and therefore $f_{i-1} \circ f_i = 0$ by Definition 5.3.1. This concludes (4.20.e).

By (4.20.e), we can enhance the commutative diagram (4.20.d) as follows:

$$\begin{array}{ccccccccc} \ldots & \xrightarrow{f_{i+1}} & F_i & & \xrightarrow{f_i} & & F_{i-1} & \xrightarrow{f_{i-1}} F_{i-2} & \xrightarrow{f_{i-2}} \ldots \\ & & & \searrow^{\phi_{i-1} \circ f_i} & & & \downarrow{\scriptstyle \phi_{i-1}} & \downarrow{\scriptstyle \phi_{i-2}} & \\ \ldots & \xrightarrow[g_{i+1}]{} & G_i & \twoheadrightarrow & \mathrm{im}\, g_i & \hookrightarrow & G_{i-1} & \xrightarrow[g_{i-1}]{} G_{i-2} & \xrightarrow[g_{i-2}]{} \ldots \\ & & & \searrow_{g_i} & & \nearrow & & & \end{array} \tag{4.20.f}$$

Applying now Definition 5.4.1 to the homomorphism $G_i \to \operatorname{im} g_i$, we obtain the existence of ϕ_i. This concludes Step 2, and in particular the existence of $\phi_\bullet : F_\bullet \to G_\bullet$.

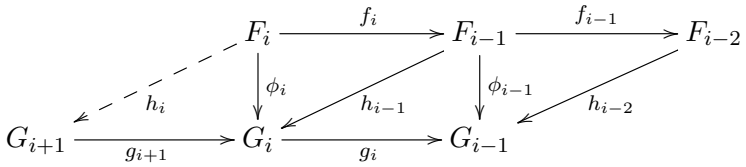
Step 3: $\phi_\bullet : F_\bullet \to G_\bullet$ is unique up to homotopy. By Remark 5.4.14, it is enough to show that if $\alpha = 0$, then $\phi \sim 0$. With other words assuming that the following diagram commutes after erasing the h_i, it is enough to find h_i such that $\phi_i = g_{i+1} \circ h_i + h_{i-1} \circ f_i$ for every $i \geq 0$:



(4.20.g)

Note that in diagram (4.20.g) we introduced new values for F_{-1}, F_{-2}, G_{-1}, G_{-2}, f_0, ... so that we can make the induction step in the next paragraph uniform for all i. Note also that this way $G_\bullet$ becomes exact at all positions.

As in the previous step, this means that we have to construct h_i for $i \geq 0$ as shown in the following diagram assuming that they were constructed for all lower indices



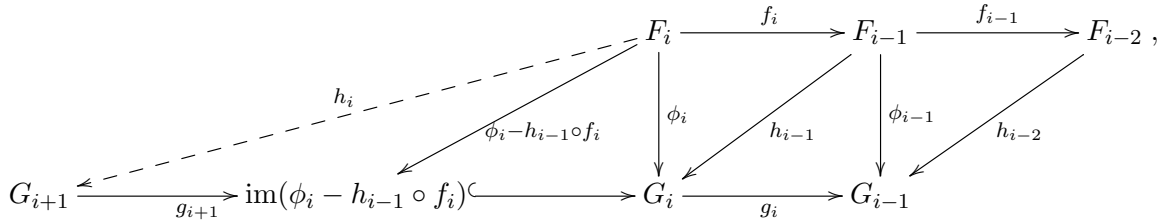
(4.20.h)

Also as in the previous step, for this it is enough to show that

$$\operatorname{im}(\phi_i - h_{i-1} \circ f_i) \subseteq \operatorname{im} g_{i+1} \iff g_i \circ (\phi_i - h_{i-1} \circ f_i) = 0 \tag{4.20.i}$$

$\uparrow$ $\operatorname{im} g_{i+1} = \ker g_i$

Indeed, (4.20.i) would imply that we could extend (4.20.h) as follows



(4.20.j)

and then we could apply the projectivity of F_i and Definition 5.4.1 to the left triangle of (4.20.j).

So, indeed we are left to show (4.20.i). However, (4.20.i) follows directly from the following computation:

$$g_i \circ (\phi_i - h_{i-1} \circ f_i) \underset{\uparrow}{=} \phi_{i-1} \circ f_i - g_i \circ h_{i-1} \circ f_i = (\phi_{i-1} - g_i \circ h_{i-1}) \circ f_i \underset{\uparrow}{=} h_{i-2} \circ f_{i-1} \circ f_i \underset{\uparrow}{=} 0$$

commutativity of (4.20.g) | by induction $\phi_{i-1} = g_i \circ h_{i-1} + h_{i-2} \circ f_{i-1}$ | $f_{i-1} \circ f_i = 0$

This concludes Step 3, and hence the entire proof as well. □

Corollary 5.4.21. *Any two projective resolutions of the same R-module are homotopy equivalent via cochain morphisms that are uniquely determined up to homotopy.*

Proof. Let $P_\bullet$ and $Q_\bullet$ be two projective resolutions of a module M. Apply Theorem 5.4.20 to lift id_M to morphisms of chain complexes $\phi : P_\bullet \to Q_\bullet$ and $\psi : Q_\bullet \to P_\bullet$. Theorem 5.4.20 also states that these are unique up to homotopy.

Next, note that $\psi\circ\phi$ and $\mathrm{id}_{P_\bullet}$ are two lifts of id_M to a morphism $P_\bullet \to P_\bullet$ of chain complexes. Hence, by the homotopy part of Theorem 5.4.20 we obtain that $\psi \circ \phi \sim \mathrm{id}_{P_\bullet}$. Similarly, both $\phi \circ \psi$ and $\mathrm{id}_{Q_\bullet}$ are are two lifts of id_M to a morphism $Q_\bullet \to Q_\bullet$ of chain complexes. Hence, by the homotopy part of Theorem 5.4.20 we also have $\phi \circ \psi \sim \mathrm{id}_{Q_\bullet}$. □

Corollary 5.4.22. *Let N be an R-module. Suppose that $P_\bullet$ and $Q_\bullet$ are two projective resolutions of the same R-module M. Then there is a unique isomorphism $\alpha : \mathrm{Ext}^i_{P_\bullet}(M,N) \xrightarrow{\cong} \mathrm{Ext}^i_{Q_\bullet}(M,N)$ (so not only the two groups are isomorphic, but even the isomorphism is uniquely determined).*

Proof. By Corollary 5.4.21, we know that there exist maps of complexes $\phi\colon P_\bullet \to Q_\bullet$ and $\psi\colon Q_\bullet \to P_\bullet$ such that $\psi \circ \phi \sim \mathrm{id}_{P_\bullet}$ and $\phi \circ \psi \sim \mathrm{id}_{Q_\bullet}$, where $h^P_\bullet$ and $h^Q_\bullet$ are the corresponding homotopies. Additionally, also by Corollary 5.4.21 we know that ϕ and ψ are determined uniquely up to homotopy.

As explained in Remark 5.4.15, $\mathrm{Hom}_R\left(h^Q_\bullet, N\right)$ and $\mathrm{Hom}_R\left(h^P_\bullet, N\right)$ gives homotopies

$$\mathrm{Hom}_R(\psi \circ \phi, N) = \mathrm{Hom}_R(\phi, N) \circ \mathrm{Hom}_R(\psi, N) \sim \mathrm{id}_{\mathrm{Hom}_R(P_\bullet, N)}$$

and

$$\mathrm{Hom}_R(\phi \circ \psi, N) = \mathrm{Hom}_R(\psi, N) \circ \mathrm{Hom}_R(\phi, N) \sim \mathrm{id}_{\mathrm{Hom}_R(Q_\bullet, N)},$$

and it also implies that $\mathrm{Hom}_R(\phi, N)$ is determined uniquely up to homotopy.

Now, Corollary 5.4.19 yields that for all $i \in \mathbb{Z}$, the homomorphisms $H^i\big(\mathrm{Hom}_R(\phi, N)\big)$ and $H^i\big(\mathrm{Hom}_R(\psi, N)\big)$ are isomorphisms:

$$\mathrm{Ext}^i_{P_\bullet}(M,N) = H^i\big(\mathrm{Hom}(P_\bullet, N)\big) \underset{H^i\left(\mathrm{Hom}_R(\phi,N)\right)}{\overset{H^i\left(\mathrm{Hom}_R(\psi,N)\right)}{\rightleftarrows}} H^i\big(\mathrm{Hom}(Q_\bullet, N)\big) = \mathrm{Ext}^i_{Q_\bullet}(M,N)$$

Additionally Proposition 5.4.10 tells us that $H^i\big(\mathrm{Hom}_R(\phi, N)\big)$ and $H^i\big(\mathrm{Hom}_R(\psi, N)\big)$ are uniquely determined, because they are unique up to homotopy. □

Definition 5.4.23. If M and N are R-modules, we define *the i-th* Ext*-module* $\mathrm{Ext}^i_R(M,N)$ *of M and N* by $\mathrm{Ext}^i_{P_\bullet}(M,N)$, where $P_\bullet$ is an projective resolution of M. We note that:

- such resolution always exists by Remark 5.3.6 and Example 5.4.3, and
- $\mathrm{Ext}^i_{P_\bullet}(M,N)$ is uniquely determined up to unique isomorphism independently of the choice of $P_\bullet$ by Corollary 5.4.22.

Hence, $\mathrm{Ext}^i_R(M,N)$ is uniquely defined up to a unique isomorphism.

Corollary 5.4.24. *If P is a projective R-module and N is an arbitrary R-module, then $\mathrm{Ext}^i_R(P,N) = 0$ for $i > 0$.*

Proof. In this case the projective resolution contains just P itself. □

Definition 5.4.25. If $\alpha : M \to L$ is a homomorphism of R-modules, then $\mathrm{Ext}^i_R(\alpha, N)$ is defined by taking projective resolutions $P_\bullet \to M$ and $Q_\bullet \to L$ and a morphism of chain complexes $\phi_\bullet : P_\bullet \to Q_\bullet$ given by Theorem 5.4.20, and then setting

$$\mathrm{Ext}^i_R(\alpha, N) := H^i\big(\mathrm{Hom}_R(\phi_\bullet, N)\big) : \mathrm{Ext}^i_R(L,N) \to \mathrm{Ext}^i_R(M,N)$$

This is uniquely defined by Remark 5.4.26

Remark 5.4.26. Here we show that, taking into account that $\mathrm{Ext}^i_R(M,N)$ and $\mathrm{Ext}^i_R(L,N)$ are defined up to unique isomorphism, $\mathrm{Ext}^i_R(\alpha,N)$ is uniquely defined as well. This precisely means that the diagram (4.26.k) commutes where the vertical arrows are the unique isomorphisms between different representatives of $\mathrm{Ext}^i_R(M,N)$ and $\mathrm{Ext}^i_R(L,N)$ and the horizontal arrows are the definitions of $\mathrm{Ext}^i_R(\alpha,N)$ for these different representatives. Below we explain this in details.

Let $\phi_\bullet : P_\bullet \to Q_\bullet$ be as in Definition 5.4.25. Then, by Theorem 5.4.20, $\phi_\bullet$ is unique up to homotopy. Hence, $H^i(\phi_\bullet)$ is unique by Proposition 5.4.17.

Therefore, we just have to deal with the ambiguity given by choosing different projective resolutions. Hence consider other projective resolutions $P'_\bullet \to M$ and $Q'_\bullet \to M$. By Theorem 5.4.20 we get unique chain complex morphisms $\xi : P'_\bullet \to P_\bullet$ and $\eta : Q_\bullet \to Q'_\bullet$ lifting id_M and id_L, respectively. According to Definition 5.4.23,

$$H^i(\mathrm{Hom}(\xi,N)) : \mathrm{Ext}^i_{P_\bullet}(M,N) \to \mathrm{Ext}^i_{P'_\bullet}(M,N)$$

and

$$H^i(\mathrm{Hom}(\eta,N)) : \mathrm{Ext}^i_{Q'_\bullet}(L,N) \to \mathrm{Ext}^i_{Q_\bullet}(L,N)$$

are the unique isomorphisms between the different representatives of $\mathrm{Ext}^i_R(M,N)$ and $\mathrm{Ext}^i_R(L,N)$, respectively. Additionally, $\eta\circ\phi\circ\xi$ is a lift of α to a morphism $P'_\bullet \to P'_\bullet$. Hence, if intead of $P_\bullet$ and $Q_\bullet$, the projective resolutions $P'_\bullet$ and $Q'_\bullet$ were used to define $\mathrm{Ext}^i_R(\alpha,N)$, then $\mathrm{Ext}^i_R(\alpha,N)$ would be defined as $H^i\big(\mathrm{Hom}_R(\eta\circ\phi\circ\xi,N)\big)$. Therefore, the following commutative diagram shows that $\mathrm{Ext}^i_R(\alpha,N)$ is uniquely defined:

$$\begin{array}{ccc} Ext^i_{P'_\bullet}(M,N) & \xleftarrow{H^i\left(\mathrm{Hom}_R(\eta\circ\phi\circ\xi,N)\right)} & Ext^i_{Q'_\bullet}(L,N) \\ {\scriptstyle H^i\left(\mathrm{Hom}_R(\xi,N)\right)}\uparrow \ \text{unique isomorphism} & & \text{unique isomorphism}\ \downarrow{\scriptstyle H^i\left(\mathrm{Hom}_R(\eta,N)\right)} \\ Ext^i_{P_\bullet}(M,N) & \xleftarrow[H^i\left(\mathrm{Hom}_R(\phi,N)\right)]{} & Ext^i_{Q_\bullet}(L,N) \end{array} \tag{4.26.k}$$

End of 5. class, on 18.10.2021.

5.5 Long exact sequence of Ext-modules

As we hinted already at the beginning of Section 5.3, the Ext-modules can be thought of as correction terms for the failure of the exactness of the $\mathrm{Hom}(\_,N)$ functor. One way to make this precise, is Theorem 5.5.6, which follows from a general statement about short exact sequences of cochain complexes:

Proposition 5.5.1 (Long exact sequence of co-homology)**.** *Let*

$$0 \longrightarrow F_\bullet \xrightarrow{\alpha_\bullet} G_\bullet \xrightarrow{\beta_\bullet} H_\bullet \longrightarrow 0$$

be a short exact sequence of co-chain complexes, that is, $\alpha_\bullet$ and $\beta_\bullet$ are co-chain morphisms such that

$$0 \longrightarrow F_i \xrightarrow{\alpha_i} G_i \xrightarrow{\beta_i} H_i \longrightarrow 0$$

is exact for every $i \in \mathbb{Z}$. Let $f_i : F_i \to F_{i+1}$, $g_i : F_i \to F_{i+1}$ and $h_i : H_i \to H_{i+1}$ be the structure homomorphisms of $F_\bullet$, $G_\bullet$ and $H_\bullet$, respectively. Then:

(1) the following defines a well defined R-module homomorphism $\delta_i : H^i(H_\bullet) \to H^{i+1}(F_\bullet)$ for every integer i: for an element $x \in H^i(H_\bullet)$,

- *let $\overline{x} \in H_i$ be a lift of x,*
- *let $y \in G_i$ be such that $\beta_i(y) = \overline{x}$*
- *let $z \in F_{i+1}$ be such that $\alpha_{i+1}(z) = g_i(y)$ (such an element exists by the above exactness assumption, and by the computation $\beta_{i+1}(g_i(y)) = h_i(\beta_i(y)) = h_i(\overline{x}) = 0$), and*
- *as $z \in \ker f_{i+1}$ (indeed, $\alpha_{i+2}(f_{i+1}(z)) = g_{i+1}(\alpha_{i+1}(z)) = g_{i+1}(g_i(y)) = 0$, and α_{i+2} is injective by assumption), we define $\delta_i(x) := [z]$, where $[z]$ is the residue class of z in $H^{i+1}(F_\bullet) = \ker f_{i+1}/\operatorname{im} f_i$.*

(2) the following sequence is exact:

$$\ldots \xrightarrow{\delta_{i-1}} H^i(F_\bullet) \xrightarrow{H^i(\alpha_\bullet)} H^i(G_\bullet) \xrightarrow{H^i(\beta_\bullet)} H^i(H_\bullet) \xrightarrow{\delta_i} H^{i+1}(F_\bullet) \xrightarrow{H^{i+1}(\alpha_\bullet)} \ldots \tag{5.1.a}$$

There is also a chain complex version of the lemma with indices reversed (so each occurence of $i+1$ has to be replaced by $i-1$).

Proof. *δ_i is well-defined:* we need to verify that δ_i does not depend on the choices we have made. For that consider a fixed $x \in H^i(H_\bullet)$, and let $\overline{x}$, y and z be chosen as above along the way of defining $\delta_i(x)$.

- First, assume that we choose another y' instead of y. That is, $y' = y + \alpha_i(w)$ for some $w \in F_i$. Then,

$$g_i(y') = g_i\left(y + \alpha_i(w)\right) = g_i(y) + g_i\left(\alpha_i(w)\right) = g_i(y) + \alpha_{i+1}\left(f_i(w)\right)$$

  In particular, we obtain $z' = z + f_i(w)$, which determines the same class in $H^{i+1}(F_\bullet)$ as z. Hence, our definition is independent of the choice of y.

- Second, assume that we choose $\overline{x}' = \overline{x} + h_{i-1}(u)$ instead of $\overline{x}$ for some $u \in H_{i-1}$. Let $v \in G_{i-1}$ be such that $\beta_{i-1}(v) = u$. Then, instead of y, we may choose $y' = y + g_{i-1}(v)$. Indeed,

$$\beta_i\left(y + g_{i-1}(v)\right) = \beta_i(y) + \beta_i\left(g_{i-1}(v)\right) = \overline{x} + h_{i-1}\left(\beta_{i-1}(v)\right) = \overline{x} + h_{i-1}(u) = \overline{x}'.$$

  Hence,

$$g_i(y') = g_i\left(y + g_{i-1}(v)\right) = g_i(y) + g_i\left(g_{i-1}(v)\right) = g_i(y),$$

  where $g_i \circ g_{i-1} = 0$,

  and so this choice yields the same z.

So, we showed that δ_i is well-defined.

δ_i is an R-module homorphism: For that let us keep the same notation for $\overline{x}$, y and z, and additionally let $\overline{x}'$, y' and z' be the elements chosen the same way but for $x' \in H^i(H_\bullet)$. Then:

- by additivity of the module homomorphisms we have $\beta_i(y+y') = \overline{x}+\overline{x}'$ and $\alpha_{i+1}(z+z') = g_i(y+y')$, and hence $\delta_i(x+x') = z+z' = \delta_i(x) + \delta_i(x')$.
- if $r \in R$, then similarly $\beta_i(ry) = r\overline{x}$ and $\alpha_{i+1}(rz) = g_i(ry)$, and hence $\delta_i(rx) = rz = r\delta_i(x)$.

So, we showed that δ_i is an R-module homomorphism. Finally we prove exactness at each position of the long exact sequence:

- $\boxed{\operatorname{im} H^i(\alpha) \subseteq \ker H^i(\beta):}$ This follows from the definition of H^i applied to morphism of complexes and from the assumption that $\beta \circ \alpha = 0$.

- $\boxed{\operatorname{im} H^i(\alpha) = \ker H^i(\beta):}$ Take $x \in \ker H^i(\beta)$, represented by $\overline{x} \in G_i$. By definition $x \in \ker H^i(\beta)$ means that there is $y \in H_{i-1}$, such that $\beta_i(\overline{x}) = h_{i-1}(y)$. Let $z \in G_{i-1}$ such that $\beta_{i-1}(z) = y$. Then,

$$\beta_i\left(\overline{x} - g_{i-1}(z)\right) = \beta_i(\overline{x}) - \beta_i\left(g_{i-1}(z)\right) = \beta_i(\overline{x}) - h_{i-1}\left(\beta_{i-1}(z)\right) = \beta_i(\overline{x}) - h_{i-1}(y) = 0$$

  So, there is $v \in F_i$, such that $\alpha_i(v) = \overline{x} - g_{i-1}(z)$, and

$$\alpha_{i+1}\left(f_i(v)\right) = g_i\left(\alpha_i(v)\right) = g_i\left(\overline{x} - g_{i-1}(z)\right) = g_i(\overline{x}) - g_i\left(g_{i-1}(z)\right) = 0 - 0 = 0.$$

  Since, α_{i+1} is injective, it follows that $f_i(v) = 0$. In particular $x = H^i(\alpha)([v])$, where $[v]$ is the class of v in $H^i(F_\bullet)$.

- $\boxed{\operatorname{im} H^i(\beta) \subseteq \ker \delta_i:}$ We have to show $\delta_i \circ H^i(\beta) = 0$. Take $x \in \ker g_i$. Then $\delta_i\left(H^i(\beta)([x])\right)$ can be computed as follows: as $H^i(\beta)([x])$ is represented by $\beta_i(x)$, so we may take x as a lift in G_i, and then, as $g_i(x) = 0$, we have $\delta_i\left(H^i(\beta)([x])\right) = 0$.

- $\boxed{\operatorname{im} H^i(\beta) = \ker \delta_i:}$ Take an element in $\ker \delta_i$, that is we take $x \in \ker h_i$, with $y \in G_i$ a lift of x to G_i, and $z \in F_{i+1}$ such that $\alpha_{i+1}(z) = g_i(y)$, and about all these we assume that there is a $v \in F_i$, such that $f_i(v) = z$. Then:

$$g_i\left(y - \alpha_i(v)\right) = g_i(y) - g_i\left(\alpha_i(v)\right) = g_i(y) - \alpha_{i+1}\left(f_i(v)\right) = g_i(y) - \alpha_{i+1}(z) = 0.$$

  In particular $[y - \alpha_i(v)] \in H^i(G_\bullet)$, and $H^i(\beta)\left([y - \alpha_i(v)]\right) = [x]$, as

$$\beta_i\left(y - \alpha_i(v)\right) = \beta_i(y) - \beta_i\left(\alpha_i(v)\right) = \beta_i(y) = x.$$

- $\boxed{\operatorname{im} \delta_i \subseteq \ker H^{i+1}(\alpha):}$ As in the previous point take $x \in \ker h_i$, with $y \in G_i$ a lift of x to G_i, and $z \in F_{i+1}$ such that $\alpha_{i+1}(z) = g_i(y)$. The class $[z] \in H^{i+1}(F_\bullet)$ gives a general element of $\operatorname{im} \delta_i$. So, we need to show that $H^{i+1}(\alpha)([z]) = 0$. However, $\alpha_{i+1}(z) = g_i(y)$ by construction, which yields exactly this.

- $\boxed{\operatorname{im} \delta_i = \ker H^{i+1}(\alpha):}$ Take $[z] \in \ker H^{i+1}(\alpha)$. That is, $\alpha_{i+1}(z) = g_i(y)$ for some $y \in G_i$. However, then for $x := \beta_i(y)$ we have $\delta_i([x]) = [z]$ as soon as we prove that $x \in \ker h_i$. However,

$$h_i(x) = h_i\left(\beta_i(y)\right) = \beta_{i+1}\left(g_i(y)\right) = \beta_{i+1}\left(\alpha_{i+1}(z)\right) = 0.$$

□

To apply Proposition 5.5.1 to prove Theorem 5.5.6, one needs to take projective resolutions of the modules from a short exact sequence so that the induced morphisms between these projective resulutions, given by Theorem 5.4.20, after applying $\operatorname{Hom}_R(\_, N)$ yields a short exact sequence of co-chain complexes. As $\operatorname{Hom}_R(\_, N)$ preserves exactness of split exact sequences (see following lemma), the easiest way to achieve this is to construct projective resolutions such that the middle one is a direct sum of the two projective resolutions on the sides. This is done in Lemma 5.5.5, after which finally we are able to show Theorem 5.5.6.

First we need a definition that already appeared on one of the exercise sheets:

Definition 5.5.2. An exact sequence of R-modules of the form

$$0 \longrightarrow K \xrightarrow{\alpha} M \xrightarrow{\beta} L \tag{5.2.b}$$

is *split* if there exists an R-module homomorphism $s : L \to M$ such that $\beta \circ s = \mathrm{id}_L$.

Remark 5.5.3. Note that in the case of Definition 5.5.2 β is automatically surjective. In particular, if the sequence in (5.2.b) is split, then it is exact.

Lemma 5.5.4. *If a short exact sequence of R-modules*

$$0 \longrightarrow K \xrightarrow{\alpha} M \xrightarrow{\beta} L \longrightarrow 0 \tag{5.4.c}$$

is split, then the sequence

$$0 \longrightarrow \mathrm{Hom}_R(L,N) \xrightarrow{\mathrm{Hom}_R(\beta,N)} \mathrm{Hom}_R(M,N) \xrightarrow{\mathrm{Hom}_R(\alpha,N)} \mathrm{Hom}_R(K,N) \longrightarrow 0. \tag{5.4.d}$$

obtained by applying $\mathrm{Hom}_R(\_,N)$ *to (5.4.c) is exact.*

Proof. By the adequate exercise on the exercise sheet, splitness is characterized not only by the existence of a homomorphism $L \to M$, but also by the existence of an R-module homomorphism $u : M \to K$ such that $u \circ \alpha = \mathrm{id}_K$. Applying now, Lemma 5.2.2 one obtains sequence of the form (5.2.b), which is exact everywhere, except possibly $\mathrm{Hom}_R(\alpha, N)$ is not surjective. Now, we take into account that $\mathrm{Hom}_R(\_, N)$ preserves composition and it takes id_K into $\mathrm{id}_{\mathrm{Hom}(K,N)}$. Hence, the $u \circ \alpha = \mathrm{id}_K$ equality transforms into the equality $\mathrm{Hom}(u, N) \circ \mathrm{hom}(\alpha, N) = \mathrm{id}_{\mathrm{Hom}(L,N)}$. This means that (5.4.*d*) is split in the sense of Definition 5.5.2, and therefore it is surjective by Remark 5.5.3.

□

Lemma 5.5.5 (Horseshoe lemma)**.** *For every short exact sequence of R-modules*

$$0 \longrightarrow K \xrightarrow{\alpha} M \xrightarrow{\beta} L \longrightarrow 0,$$

and projective resolutions $Q_\bullet \to K$ and $S_\bullet \to L$ there exists a projective resolution : $P_\bullet \to M$ such that

(1) $P_i := Q_i \oplus S_i$ (but the structure homomorphisms of $P_\bullet$ are NOT the products of the structure homomorphisms fo $Q_\bullet$ and $S_\bullet$),

(2) the inclusions $\iota_i : Q_i \to P_i = Q_i \oplus S_i$ of the Q_i factors define a chain complex morphism $\iota_\bullet : Q_\bullet \to P_\bullet$,

(3) the projections $pr_i : Q_i \oplus S_i = P_i \to S_i$ onto the S_i factors define a chain complex morphism $\mathrm{pr}_\bullet : P_\bullet \to S_\bullet$,

(4) the following diagram commutes:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Q_\bullet & \xrightarrow{\iota_\bullet} & P_\bullet & \xrightarrow{\mathrm{pr}_\bullet} & S_\bullet & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & L & \longrightarrow & 0
\end{array}$$

Proof of Lemma 5.5.5. Denote by $q_i : Q_i \to Q_{i-1}$ and $s_i : S_i \to S_{i-1}$ the structure homomorphisms that are already given. We only have to construct the structure homomorphisms $p_i : P_i \to P_{i-1}$ of $P_\bullet$ and the homomorphism $P_0 \to M$.

Step 1: Construction of the homomorphism $P_0 \to M$: As S_0 is projective, there exists an R-module homomorphism $S_0 \to M$ making the following diagram commute:

$$\begin{array}{ccc} & & S_0 \\ & {\scriptstyle\phi_0}\swarrow & \downarrow{\scriptstyle s_0} \\ M & \xrightarrow{\beta} & L \end{array}$$

By the universal property of direct sums, there is a unique R-module homomorphism $Q_0 \oplus S_0 \to M$ making the following diagram commute (ι_0 and j_0 are the inclusions of the summands):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q_0 & \xrightarrow{\iota_0} & P_0 = Q_0 \oplus S_0 & \xleftarrow{j_0} & S_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle q_0} & & \downarrow{\scriptstyle p_0} & \swarrow{\scriptstyle \phi_0} & \downarrow{\scriptstyle s_0} & & \\ 0 & \longrightarrow & K & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & L & \longrightarrow & 0 \end{array} \tag{5.5.e}$$

We claim that $s_0 \circ \mathrm{pr}_0 = \beta \circ p_0$, where $\mathrm{pr}_0 : Q_0 \oplus S_0 \to S_0$ is the second projection, as defined in the statement of the present lemma. Indeed, by the commutativity of (5.5.e) we have

$$s_0 \circ \mathrm{pr}_0 = \beta \circ \phi_0 \circ \mathrm{pr}_0 = \beta \circ p_0 \circ j_0 \circ \mathrm{pr}_0 \,.$$

Hence, it is enough to show that $\beta \circ p_0 \circ (\mathrm{id}_{P_0} - j_0 \circ \mathrm{pr}_0) = 0$. Note now that $\operatorname{im}\left(\mathrm{id}_{P_0} - \mathrm{pr}_0 \circ j_0\right) = \operatorname{im} \iota_0$. Hence, it is enough to show that $\beta \circ p_0 \circ \iota_0 = 0$. However, using again the commutativity of (5.5.e), we have $\beta \circ p_0 \circ \iota_0 = \beta\alpha \circ q_0 = 0$. This concludes our above claim, which tells us that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q_0 & \xrightarrow{\iota_0} & P_0 = Q_0 \oplus S_0 & \xrightarrow{\mathrm{pr}_0} & S_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle q_0} & & \downarrow{\scriptstyle p_0} & & \downarrow{\scriptstyle s_0} & & \\ 0 & \longrightarrow & K & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & L & \longrightarrow & 0 \end{array} \tag{5.5.f}$$

Additionally note that p_0 is surjective by the adequate 4-lemma (see the exercise sheet).

Step 2: Induction step: defining the structure homomorphism $p_i : P_i \to P_{i-1}$: If $i = 1$, then define temporary just for this step $Q_{-1} := K$, $P_{-1} := M$ and $S_{-1} := L$ with the structure maps being the maps of (5.5.e). Having made these definitions, we start with the situation

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q_{i-1} & \longrightarrow & P_{i-1} & \longrightarrow & S_{i-1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle q_{i-1}} & & \downarrow{\scriptstyle p_{i-1}} & & \downarrow{\scriptstyle s_{i-1}} & & \\ 0 & \longrightarrow & Q_{i-2} & \longrightarrow & P_{i-2} & \longrightarrow & S_{i-2} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle q_{i-2}} & & \downarrow{\scriptstyle p_{i-2}} & & \downarrow{\scriptstyle s_{i-2}} & & \\ & & \vdots & & \vdots & & \vdots & & \end{array} \tag{5.5.g}$$

where the diagram goes indefinitely in the negative direction (the groups for $i < -1$ all taken to be zeros), and the columns are exact in the $i-2$ and smaller positions. Extend the above diagram with zeros also in the positions greater than $i-1$, and apply the chain complex version of Proposition 5.5.1. This yields the following long exact sequence

$$0 = H_i(S_\bullet) \to H_{i-1}(Q_\bullet) = \ker q_{i-1} \to H_{i-1}(P_\bullet) = \ker p_{i-1} \to H_{i-1}(S_\bullet) = \ker s_{i-1} \to H_{i-2}(Q_\bullet) = 0$$

Take this exact sequence now, and construct as in Step 1 the following commutative diagram (it is verbatim the same argument as in Step 1, after we make the following replacements: $Q_0 \rightsquigarrow Q_i$, $P_0 \rightsquigarrow P_i$, $S_0 \rightsquigarrow Q_i$, $K \rightsquigarrow \ker q_{i-1}$, $M \rightsquigarrow \ker p_{i-1}$, $L \rightsquigarrow \ker s_{i-1}$):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Q_i & \longrightarrow & P_i & \longrightarrow & S_i & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \ker q_{i-1} & \longrightarrow & \ker p_{i-1} & \longrightarrow & \ker s_{i-1} & \longrightarrow & 0
\end{array}$$

Assembling this with diagram (5.5.g) we obtain

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Q_i & \longrightarrow & P_i & \longrightarrow & S_i & \longrightarrow & 0 \\
 & & {\scriptstyle q_i}\downarrow & & {\scriptstyle p_i}\downarrow & & {\scriptstyle s_i}\downarrow & & \\
0 & \longrightarrow & \ker q_{i-1} & \longrightarrow & \ker p_{i-1} & \longrightarrow & \ker s_{i-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Q_{i-1} & \longrightarrow & P_{i-1} & \longrightarrow & S_{i-1} & \longrightarrow & 0 \\
 & & {\scriptstyle q_{i-1}}\downarrow & & {\scriptstyle p_{i-1}}\downarrow & & {\scriptstyle s_{i-1}}\downarrow & & \\
0 & \longrightarrow & Q_{i-2} & \longrightarrow & P_{i-2} & \longrightarrow & S_{i-2} & \longrightarrow & 0 \\
 & & {\scriptstyle q_{i-2}}\downarrow & & {\scriptstyle p_{i-2}}\downarrow & & {\scriptstyle s_{i-2}}\downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

□

Theorem 5.5.6. *Let N be an R-module. For every short exact sequence*

$$0 \longrightarrow K \xrightarrow{\alpha} M \xrightarrow{\beta} L \longrightarrow 0$$

of R-modules, there are R-module homorphisms $\delta_i : \operatorname{Ext}^i_R(K,N) \to \operatorname{Ext}^{i+1}_R(L,N)$ making the following sequence is exact

$$\begin{array}{l}
0 \longrightarrow \operatorname{Hom}_R(L,N) \xrightarrow{\operatorname{Hom}_R(\beta,N)} \operatorname{Hom}_R(M,N) \xrightarrow{\operatorname{Hom}_R(\alpha,N)} \operatorname{Hom}_R(K,N) \\
\qquad \xrightarrow{\delta_0} \operatorname{Ext}^1_R(L,N) \xrightarrow{\operatorname{Ext}^1_R(\beta,N)} \operatorname{Ext}^1_R(M,N) \xrightarrow{\operatorname{Ext}^1_R(\alpha,N)} \operatorname{Ext}^1_R(K,N) \\
\qquad \xrightarrow{\delta_1} \operatorname{Ext}^2_R(L,N) \xrightarrow{\operatorname{Ext}^2_R(\beta,N)} \operatorname{Ext}^2_R(M,N) \xrightarrow{\operatorname{Ext}^2_R(\alpha,N)} \dots,
\end{array} \tag{5.6.h}$$

Proof. According to Proposition 5.3.8, we may replace in the first row of (5.6.h) each appearance of Hom with Ext^0's. Apply now Lemma 5.5.5. This yields projective resolutions $Q_\bullet \to K$, $P_\bullet \to M$ and $S_\bullet \to L$ with the properties stated in Lemma 5.5.5. Applying the $\operatorname{Hom}(-,N)$ functor, we obtain a short exact sequence of cochain complexes

$$0 \longrightarrow \operatorname{Hom}_R(S_\bullet, N) \xrightarrow{\operatorname{Hom}_R(\iota_\bullet,N)} \operatorname{Hom}_R(P_\bullet, N) \xrightarrow{\operatorname{Hom}_R(\mathrm{pr}_\bullet,N)} \operatorname{Hom}_R(Q_\bullet, N) \longrightarrow 0. \tag{5.6.i}$$

with the following properties:

(1) the cohomologies of these cochain complexes are exactly the Ext modules in (5.6.h).

(2) the restriction of (5.6.i) to any index i, is obtained by applying $\mathrm{Hom}_R(\_, N)$ to a split exact sequence, which then by Lemma 5.5.4 is exact as well.

Therefore applying Proposition 5.5.1 to (5.6.i) yields exactly (5.6.h) □

Example 5.5.7. As an application of Theorem 5.5.6, we compute $\mathrm{Ext}^i_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right)$. Consider the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{x \mapsto nx} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

Applying $\mathrm{Hom}_{\mathbb{Z}}\left(\_, \mathbb{Z}/m\mathbb{Z}\right)$ to this short exact sequence yields the following long exact sequence, where the groups that are labeled to be zero are zero because of Corollary 5.4.24:

$$\begin{aligned}
&0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) \cong \mathbb{Z}/m\mathbb{Z} \xrightarrow{x \mapsto nx} \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) \cong \mathbb{Z}/m\mathbb{Z} \\
&\quad \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}\left(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) = 0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}\left(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) = 0 \\
&\quad \longrightarrow \mathrm{Ext}^2_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) \longrightarrow \mathrm{Ext}^2_{\mathbb{Z}}\left(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) = 0 \longrightarrow \mathrm{Ext}^2_{\mathbb{Z}}\left(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) = 0 \\
&\quad \longrightarrow \mathrm{Ext}^3_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) \longrightarrow \mathrm{Ext}^3_{\mathbb{Z}}\left(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) = 0 \longrightarrow \dots,
\end{aligned}$$

Buy the exactness of the above sequence we obtain that

$$\mathrm{Ext}^i_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) \cong \begin{cases} 0 & \text{if } i \neq 0, 1 \\ \mathbb{Z}/\gcd(m,n)\mathbb{Z} & \text{if } i = 0, 1 \end{cases}$$

End of 6. class, on 25.10.2021.

5.6 Meaning of Ext-modules

In this section, we fulfill our promise made in Section 5.1, that is, we show that $\mathrm{Ext}^1_R(M, N)$ classifies extensions of N by M (WARNING: order is reversed). First, we define carefully what extensions are and when we call them equivalent.

Definition 5.6.1. Given two R-modules M and N, consider an exact sequence of R-modules as follows:

$$0 \longrightarrow N \xrightarrow{\alpha} K \xrightarrow{\beta} M \longrightarrow 0$$

In this situation:

- the module K is called an *extension* of N by M, and
- the entire sequence, that is, the data of K, α and β is called a *Yoneda extension* of N by M.

Two Yoneda extensions

$$0 \longrightarrow N \xrightarrow{\alpha} K \xrightarrow{\beta} M \longrightarrow 0$$

and

$$0 \longrightarrow N \xrightarrow{\alpha'} K' \xrightarrow{\beta'} M \longrightarrow 0$$

of N by M are Yoneda equivalent if there exists an R-module homomorphism $f : K \to K'$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\alpha} & K & \xrightarrow{\beta} & M & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle f} & & \| & & \\ 0 & \longrightarrow & N & \xrightarrow[\alpha']{} & K' & \xrightarrow[\beta']{} & M & \longrightarrow & 0 \end{array} \tag{6.1.a}$$

We note that by the 5-lemma (Lemma 5.6.2), f must always be an isomorphism. We also note that it is immediate from the definition that Yoneda equivalence is indeed an equivalence relation on the class of Yoneda extensions.

We denote Yoneda equivalence by $\equiv_{\text{Yoneda}}$.

Lemma 5.6.2 (Five Lemma)**.** *Let*

$$\begin{array}{ccccccccc} A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & E \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \epsilon} \\ A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & E' \end{array}$$

be a commutative diagram of R-modules. Assume that each row is exact and that β, δ are isomorphisms, α is surjective and ϵ is injective. Then γ is an isomorphism.

Proof. This is just the union of the two 4-lemmas, which were homework exercises. □

The goal of this section, performed in Theorem 5.6.6, is to show that $\text{Ext}^1(M, N)$ is in bijection with the set of Yoneda extensions of N by M, up to Yoneda equivalence. First, in an example we explain the tricky aspects of this correspondence, and then we show Theorem 5.6.6.

Example 5.6.3. Consider Definition 5.6.1 for $R = \mathbb{Z}$ and $M = N = \mathbb{Z}/3\mathbb{Z}$. A Yoneda extension then has of the form

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{\alpha} K \xrightarrow{\beta} \mathbb{Z}/3\mathbb{Z} \longrightarrow 0 \tag{6.3.b}$$

In particular K is an abelian group of order 9. We know that there are two groups of this type up to imorphism: $K = \mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. It is immediate that in fact both of these options fit into an exact sequence as (6.3.b). Hence, there are two extensions of $\mathbb{Z}/3\mathbb{Z}$ by $\mathbb{Z}/3\mathbb{Z}$. However $\text{Ext}^1_{\mathbb{Z}}\left(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}\right) \cong \mathbb{Z}/3\mathbb{Z}$. So, according to Theorem 5.6.6, the extra data in the definition of Yoneda extension somehow has to give two different Yoneda extensions for one of the two choices of K.

In fact, there are two non-equivalent Yoneda extensions with $K = \mathbb{Z}/9\mathbb{Z}$. Below, we explain this. To understand the example, it is crucial to understand that here one needs to fix the $\mathbb{Z}/3\mathbb{Z}$ s, not only up to isomorphism. That is, we should think about the standard representative, the elements of which are

$$\mathbb{Z}/3\mathbb{Z} = \left\{\ [0] = 3\mathbb{Z},\ [1] = 1 + 3\mathbb{Z},\ [2] = 2 + 3\mathbb{Z}\ \right\}$$

and the same for $\mathbb{Z}/9\mathbb{Z}$. Let us take then the standard Yoneda extension with $K = \mathbb{Z}/9\mathbb{Z}$:

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{\alpha:[1]\mapsto[3]} \mathbb{Z}/9\mathbb{Z} \xrightarrow{\beta:[1]\mapsto[1]} \mathbb{Z}/3\mathbb{Z} \longrightarrow 0 \tag{6.3.c}$$

The point, is that one can change (6.3.c) by precomposing α or post-composing β by the only non-trivial automorphism of $\mathbb{Z}/3\mathbb{Z}$ given by $[1] \mapsto [2]$. If one does it on both ends, then one

obtains an equivalent Yoneda extension:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/3\mathbb{Z} & \xrightarrow{[1]\mapsto[3]} & \mathbb{Z}/9\mathbb{Z} & \xrightarrow{[1]\mapsto[1]} & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & 0 \\ & & \Big\| {\scriptstyle [1]\mapsto[1]} & & \Big\downarrow {\scriptstyle [1]\mapsto[2]} & & \Big\| {\scriptstyle [1]\mapsto[1]} & & \\ 0 & \longrightarrow & \mathbb{Z}/3\mathbb{Z} & \xrightarrow{[1]\mapsto[6]} & \mathbb{Z}/9\mathbb{Z} & \xrightarrow{[1]\mapsto[2]} & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & 0 \end{array}$$

However, (6.3.c) and the following Yoneda extension are not equivalent:

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{\gamma:[1]\mapsto[3]} \mathbb{Z}/9\mathbb{Z} \xrightarrow{\delta:[1]\mapsto[2]} \mathbb{Z}/3\mathbb{Z} \longrightarrow 0 \tag{6.3.d}$$

Indeed, if they were equivalent, that would mean the existence of $f : \mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$ as in (6.1.a). That is, we would have

$$\beta = \delta \circ f \iff [1] = [2][f(1)] \in \mathbb{Z}/3\mathbb{Z} \iff f(1) = [2], [5], \text{ or } [8] \in \mathbb{Z}/9\mathbb{Z} \tag{6.3.e}$$

But, we would also need to have

$$f \circ \alpha = \gamma \iff f(1)[3] = [3] \in \mathbb{Z}/9\mathbb{Z} \iff f(1) = [1], [4], \text{ or } [7] \in \mathbb{Z}/9\mathbb{Z} \tag{6.3.f}$$

Equations (6.3.f) and (6.3.e) contradict to each other. Hence, we showed that (6.3.c) and (6.3.d) are non-equivalent Yoneda extensions.

Remark 5.6.4. We have seen in an exercise on the exercise sheet that the Yoneda extension

$$0 \longrightarrow N \longrightarrow K \longrightarrow M \longrightarrow 0 \tag{6.4.g}$$

is Yoneda-equivalent to the Yoneda-extension

$$0 \longrightarrow N \xrightarrow{\iota_N} N \oplus M \xrightarrow{\mathrm{pr}_M} M \longrightarrow 0 \tag{6.4.h}$$

if and only if (6.4.g) is split. In particular we call (6.4.h) the trivial Yoneda extension.

Notation 5.6.5. Let M and N be R-modules and let

$$P_\bullet : \ \ldots \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0$$

be a projective resolution of M with structure homomorphism $f_0 : P_0 \to M$. We define maps

$$\xi : \mathrm{Ext}^1_R(M, N) \longrightarrow \Big\{\text{Yoneda extensions of } N \text{ by } M\Big\}\Big/\equiv_{\text{Yoneda}}$$

and

$$\mu : \Big\{\text{Yoneda extensions of } N \text{ by } M\Big\}\Big/\equiv_{\text{Yoneda}} \longrightarrow \mathrm{Ext}^1_R(M, N)$$

the well definedness of which is shown in Theorem 5.6.6.

The definition of ξ: for

$$x \in \mathrm{Ext}^1_R(M, N) = \ker \mathrm{Hom}_R(f_2, N)\Big/\mathrm{im}\,\mathrm{Hom}_R(f_1, N)$$

we take a representative $\phi \in \ker \mathrm{Hom}_R(f_2, N) \subseteq \mathrm{Hom}_R(P_1, N)$, and then we define $\xi(x)$ to be the Yoneda-equivalence class of the following Yoneda extension, where for a homomorphism γ

we denote by $[\gamma]$ the homomorphism induced by γ on the corresponding cokernel (it is shown in the proof of Theorem 5.6.6 that this does make sense):

$$0 \longrightarrow N \xrightarrow{\alpha: n \mapsto [(n,0)]} \operatorname{coker}\left(P_1 \xrightarrow{(\phi, f_1)} N \oplus P_0\right) \xrightarrow{\beta := [f_0 \circ \mathrm{pr}_{P_0}]} M \longrightarrow 0 \tag{6.5.i}$$

The definition of μ: it sends a Yoneda extension z:

$$0 \longrightarrow N \xrightarrow{\gamma} K \xrightarrow{\delta} M \longrightarrow 0$$

to the class of the morphism $-\phi_z$, where $\phi_z : P_1 \to N$ obtained by lifting id_M in the diagram

$$\begin{array}{ccccccccc} P_2 & \xrightarrow{f_2} & P_1 & \xrightarrow{f_1} & P_0 & \xrightarrow{f_0} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_z} & & \downarrow{\scriptstyle \psi_z} & & \| {\scriptstyle \mathrm{id}_M} & & \\ 0 & \longrightarrow & N & \xrightarrow{\gamma} & K & \xrightarrow{\delta} & M & \longrightarrow & 0 \end{array} \tag{6.5.j}$$

via Theorem 5.4.20.

Theorem 5.6.6. *The maps ξ and μ of Notation 5.6.5 do make sense, they are well defined and they are bijections.*

Material not on the exam but strongly suggested if you are seriously interested in algebra

Proof. We use Notation 5.6.5 throughout the proof.

Step 1 : the sequence (6.5.i) makes sense. To make sure that β makes sense on $\operatorname{coker}(\phi, f_1)$, by Lemma 5.2.1, we have to show that:

$$\ker\left(f_0 \circ \mathrm{pr}_{P_0}\right) \supseteq \operatorname{im}(\phi, f_1) \iff 0 = f_0 \circ \mathrm{pr}_{P_0} \circ (\phi, f_1) = f_1 \circ f_0,$$

where the last composition is zero by $P_\bullet$ being a resolution.

Step 2: The sequence (6.5.i) is exact.

- We have

$$\operatorname{coker}\left(P_1 \xrightarrow{(\phi, f_1)} N \oplus P_0\right) = {}^{N \oplus P_0} \Big/ \left\{ \left(\phi(p),\ f_1(p)\right) \;\middle|\; p \in P_1 \right\}.$$

  So, for the injectivity of α we have to prove that $f_1(p) = 0$ implies $\phi(p) = 0$. This is equivalent to:

$$\ker f_1 \subseteq \ker \phi \iff \underbrace{\operatorname{im} f_2 \subseteq \ker \phi}_{\operatorname{im} f_2 = \ker f_1} \iff \phi \circ f_2 = 0 \iff \phi \in \operatorname{Hom}_R(f_2, N)$$

  which holds by assumption.

- Surjectivity of β is immediate as it is defined as the composition of surjective maps.

- To see that $\ker \beta = \operatorname{im} \alpha$ note first that by $\ker f_0 = \operatorname{im} f_1$ we get that

$$\ker \beta = {}^{N \oplus \operatorname{im} f_1} \Big/ \left\{ \left(\phi(p),\ f_1(p)\right) \;\middle|\; p \in P_1 \right\}. \tag{6.6.k}$$

We see immediately that $\operatorname{im}\alpha \subseteq \ker\beta$.

For the opposite containment, take an element of $\ker\beta$, which is by (6.6.k) represented by some $\big(n,\ f_1(p)\big) \in N \oplus \operatorname{im} f_1$ for some $p \in P_1$. In the quotient of (6.6.k), this is the same element as

$$\big(n-\phi(p),\ f_1(p)-f_1(p)\big) = (n-\phi(p),\ 0),$$

which is in $\operatorname{im}\alpha$.

So, to summarize we proved Step 1 & 2, which together imply that the definition of ξ makes sense.

Step 3: ξ is well-defined. We have to show that $\xi(x)$ does not depend on the choice of representative ϕ of x. For this take another representative ϕ'. Then $\phi-\phi' = \psi\circ f_1$, for some $\psi \in \operatorname{Hom}_R(P_0, M)$. We define the R-module homomorphism

$$\begin{array}{rccc} g_\psi\colon & N\oplus P_0 & \longrightarrow & N\oplus P_0 \\ & (m,p) & \mapsto & (m-\psi(p),p). \end{array}$$

We note that g_ψ is an isomorphism, as $g_{-\psi}$ is an inverse to it. In particular, g_ψ induces an isomorphism

$$\operatorname{im}\left(P_1 \xrightarrow{(\phi,f_1)} N\oplus P_0\right) \to \operatorname{im}\left(P_1 \xrightarrow{(\phi,f_1)} N\oplus P_0 \xrightarrow{g_\psi} M\oplus P_0\right) \underset{\boxed{\phi-\psi\circ f_1=\phi'}}{\uparrow =} \operatorname{im}\left(P_1 \xrightarrow{(\phi',f_1)} N\oplus P_0\right). \tag{6.6.l}$$

It follows that g_ψ descends to the quotients by the above images, which is the middle vertical arrow in the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\alpha: n\mapsto[(n,0)]} & \operatorname{coker}\left(P_1 \xrightarrow{(\phi,f_1)} N\oplus P_0\right) & \xrightarrow{\beta:=[f_0\circ \mathrm{pr}_{P_0}]} & M & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle [g_\psi]} & & \| & & \\ 0 & \longrightarrow & N & \xrightarrow{\alpha': n\mapsto[(n,0)]} & \operatorname{coker}\left(P_1 \xrightarrow{(\phi',f_1)} N\oplus P_0\right) & \xrightarrow{\beta':=[f_0\circ \mathrm{pr}_{P_0}]} & M & \longrightarrow & 0 \end{array} \tag{6.6.m}$$

We claim that (6.6.m) is a Yoneda equivalence, which will conclude the proof of Step 3, as the two rows of (6.6.m) are the two exact sequences given by defining $\xi(x)$ using ϕ and ϕ', respectively.

To prove our claim we have to check that (6.6.m) is commutative, which amounts to checking that the two squares commute:

- For the first square we need to show that $[g_\psi]\circ\alpha = \alpha'$. However, this equality holds even before quotienting out by the images in (6.6.l). The argument is as follows (where $[\_]$ denotes passing to the corresponding equivalence classes in the quotients):

$$[g_\psi]\circ\alpha(n) = [g_\psi(\alpha(n))] = [g_\psi(n,0)] = [(n,0)] = \alpha'(n)$$

- We need to check that $\beta'\circ[g_\psi] = \beta$. This is checked in the following computation, where $p \in P_0$ and $n \in N$:

$$\beta'\circ[g_\psi]([n,p]) = \beta'([n-\psi(p),p]) = f_0(p) = \beta([n,p]).$$

This conlcudes Step 3, and hence the map ξ is well defined.

Step 4: μ makes sense: To prove that μ makes sense we have to prove that the $-\phi_z \in \ker \mathrm{Hom}(f_2, N)$, so that $-\phi_z$ defines a class in $\mathrm{Ext}^1_R(M,N)$. However, this is equivalent to

$$\phi_z \in \ker \mathrm{Hom}(f_2,N) \iff \phi_z \circ f_2 = 0 \underset{\uparrow}{\iff} 0 = \gamma \circ \phi_z \circ f_2 = \psi_z \circ f_1 \circ f_2.$$

γ is injective

Here the last composition is zero, as $P_\bullet$ is a chain complex.

Step 5: μ is well-defined: There are two ambiguities with which we have to deal: id_N can be lifted to two different elements of $\mathrm{Hom}_R(P_1,N)$, and z can be replaced by another Yoneda equivalent Yoneda extension:

- If ϕ'_z is another lift of id_N in (6.5.j), then it is homotopy equivalent to ϕ_z by Theorem 5.4.20, i.e. there exists an R-module homomorphism $h_0 : P_0 \to N$ such that $\phi_z - \phi'_z = h_0 \circ f_1$. Here we use the convention that whichever map or group is not written out in a complex, it is zero, hence strictly speaking we apply Theorem 5.4.20 to the extension of (6.5.j) to a diagram where all vertical arrows are drawn in, and they are all zeros, except the ones in the diagr am. In particular, then all the arrows of our homotopy left of h_0 are also zero automatically.

  The equation $\phi_z - \phi'_z = h_0 \circ f_1$ means that $-\phi_z$ and $-\phi'_z$ define the same class in $\mathrm{Ext}^1_R(M,N)$.

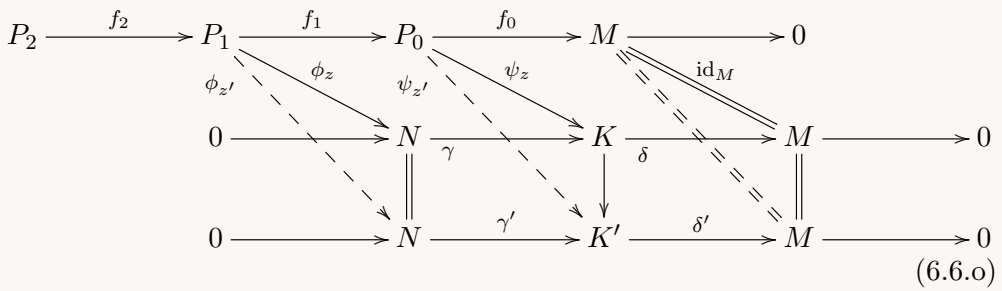
- If z' is another Yoneda extension

$$0 \longrightarrow N \xrightarrow{\gamma'} K' \xrightarrow{\delta'} M \longrightarrow 0$$

  such that z and z' are Yoneda equivalent via

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\gamma} & K & \xrightarrow{\delta} & M & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & N & \xrightarrow{\gamma'} & K' & \xrightarrow{\delta'} & M & \longrightarrow & 0 \end{array} \tag{6.6.n}$$

  then take the R-module homomorphisms as in (6.5.j) for z. Note that via (6.6.n) we also get the corresponding homomorphisms for z':



(6.6.o)

  Diagram (6.6.o) shows that in fact $\phi_z = \phi_{z'}$. This shows that z and z' define the same class in $\mathrm{Ext}^1_R(M,N)$.

This concludes Step 5.

Step 6: $\xi \circ \mu = \mathrm{id}$:. Let z be the Yoneda extension

$$0 \longrightarrow N \xrightarrow{\gamma} K \xrightarrow{\delta} M \longrightarrow 0$$

Let ϕ_z and ψ_z be defined as in (6.5.j). Then, to prove this step, we need to show that the Yoneda extension z is Yoneda equivalent to the Yoneda extension $\xi(-\phi_z)$. For this, let $\gamma + \psi_z : N \oplus P_0 \to K$ be the R-module homomorphism that sends (n, a) to $\gamma(n) + \psi_z(a)$. Then we have the following containment between submodules of $N \otimes P_0$:

$$\gamma \circ \phi_z = \psi_z \circ f_1 \implies (\gamma + \psi_z) \circ (-\phi_z, f_1) = 0 \implies \mathrm{im}(-\phi_z, f_1) \subseteq \ker(\gamma + \psi_z).$$

In particular, by Lemma 5.2.1, $\gamma + \psi$ descends to a homomorphism

$$[\gamma + \psi] : {}^{N \oplus P_0}\Big/_{\mathrm{im}(-\phi_z, f_1)} \to K.$$

Consider then the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N & \xrightarrow{\alpha : n \mapsto [(n,0)]} & \frac{N \oplus P_0}{\mathrm{im}(-\phi_z, f_1)} & \xrightarrow{\beta := f_0 \circ \mathrm{pr}_{P_0}} & M & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle [\gamma + \psi_z]} & & \| & & \\
0 & \longrightarrow & N & \xrightarrow[\gamma]{} & K & \xrightarrow[\delta]{} & M & \longrightarrow & 0
\end{array} \tag{6.6.p}$$

We verify that diagram (6.6.p) is commutative:

- for any $n \in N$ we have $[\gamma + \psi_z](\alpha(n)) = \gamma(n)$ by the definition of $\gamma + \psi$, and
- for any $(n, p) \in N \oplus P_0$ we have

$$\delta\big([\gamma + \psi_z](n, p)\big) = \delta(\gamma(n) + \psi(p)) = \delta(\psi(p)) = f_0(p) = f_0(\mathrm{pr}_{P_0}(n, p))$$

$\delta \circ \gamma = 0$ (6.5.j) commutes

Hence (6.6.p) yields a Yoneda equivalence between z and $\xi(-\phi_z)$. This finishes the proof of Step 6.

Step 7: $\mu \circ \xi = \mathrm{id}$: Conversely, given an R-module homomorphism $\phi : P_1 \to M$ such that $\phi \circ f_2 = 0$, we have to prove that $-\phi$ is a lift of id_N in the following diagram, which means that we can fill in the diagram with $-\phi$ and another R-module homomorphism $\psi : P_0 \to {}^{N \oplus P_0}\Big/_{\mathrm{im}(\phi, f_1)}$ such that the diagram becomes commutative:

$$\begin{array}{ccccccccc}
P_2 & \xrightarrow{f_2} & P_1 & \xrightarrow{f_1} & P_0 & \xrightarrow{f_0} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle -\phi} & & \downarrow{\scriptstyle \psi} & & \| {\scriptstyle \mathrm{id}_M} & & \\
0 & \longrightarrow & N & \xrightarrow[\alpha : n \mapsto [(n,0)]]{} & N \oplus P_0 \Big/ \mathrm{im}(\phi, f_1) & \xrightarrow{[f_0 \circ \mathrm{pr}_{P_0}]} & M & \longrightarrow & 0
\end{array} \tag{6.6.q}$$

For this, let us take $\psi(a) = [(0, a)]$. This makes the right square of (6.6.q) commute. Then the morphism $-\phi : P_1 \to N$ makes also the left square of (6.6.q) commute, because

$$\alpha(-\phi(p)) = [-\phi(p), 0)] \underset{\uparrow}{=} [(0, f_1(p))] = \psi(f_1(p)).$$

$$\boxed{\text{in } {}^{N \oplus P_0}\big/_{\text{im}(\phi, f_1)}}$$

□

Remark 5.6.7. We note that one can define also a group structure on the set of Yoneda extensions modulo Yoneda equivalence. This way the map of Theorem 5.6.6 becomes even an isomorphism of groups. As the proof of Theorem 5.6.6 is already quite long, we do not cover this detail in this course.

5.7 VARIATIONS ON THE SAME THEME

We conclude our homological algebra discussion with some remarks about generalizations. This is in fact an immense topic, so we just mention a very few directions out of all:

- If one reverses all arrows, one obtains injective resolutions. Then, by using injective resolution of N and then applying the functor $\text{Hom}_R(M, \_)$ one obtains another definition of Ext-modules, which can be showed to be isomorphic to the one we gave.
- One can do the projective story we did, or the injective one of the previous point in general for additive left-/right-exact functors.
- Instead of working with modules, one can in general work with abelian categories.
- One can make a general framework, where Theorem 5.5.6 becomes integrated into the objects, and in which setting some variant of Hom becomes exact. This is the theory of derived categories, which can be further generalized to ∞-categories, where the analogy with topology gets even stronger.
- The cohomology theories mentioned in Section 5.1 use the above abelian category approach, or they work with specific resolutions (such as De-Rham forms or simplices in a fixed topological space).

End of 7. class, on 01.11.2021.

Chapter 6

Dimension theory and integral dependence

From now all rings are commutative (and with identitiy as always).

6.1 Dimension of rings

In this section we explain the overall goal of Chapter 6 and Chapter 7. The main question is what is the dimension of a ring. First, there is one very general notion of dimension defined in Definition 6.1.1. As we will see in a few lines, this definition resembles very much the definition of a length of a module (Definition 3.2.8), and so theoretically looks quite natural. On the other hand, it is really hard to compute it outside of the case of fields and PID's, for which it gives a dimension 0 and 1, respectively (Example 6.1.2). On the other hand, when our rings are domains that are quotients of a polynomial ring over a field F, there is another way of attaching a notion of dimension: the transcendence degree of the fraction field. This just counts the number of algebraically independent elements over F in the fraction field (Definition 6.1.9). In particular, it gives what we would expect for $F[x_1, \dots, x_n]$, that is, that it has dimension n.

It would be nice if the above two notions of dimensions would agree at least in the case when the latter makes sense. This will be the the main theorem that we prove in Chapter 6 and Chapter 7, and it is stated precisely in Theorem 6.1.12.

During the course of the proof of Theorem 6.1.12, in Chapter 6 and Chapter 7 we work out a big part of the foundations of commutative algebra. Some examples are:

(1) we define integral dependence, which is a crucial notion both in number theory and algebraic geometry (Definition 6.2.1)

(2) we establish many tools to compute dimensions of rings: going up theorem (Proposition 7.4.2), Noether normalizationTheorem 6.2.10), etc

(3) we introduce basic constructions of commutative algebra, such as localization (Theorem 7.2.2) and tensor products (Theorem 7.1.3),

(4) finally, in Chapter 8, we use Theorem 6.1.12 to prove Nullstellensatz (Theorem 8.3.9), which is the starting point of algebraic geometry.

Definition 6.1.1. If $p \subseteq R$ is a prime ideal, then its *height* is

$$\operatorname{ht} p = \sup \left\{ \; n \;\middle|\; \exists \text{ a chain of prime ideals } p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_{n-1} \subsetneq p \; \right\}$$

The *dimension* of R is

$$\dim R = \sup \left\{ \; \operatorname{ht} p \;\middle|\; p \subseteq R \text{ is a prime ideal } \; \right\}.$$

Example 6.1.2. (1) If F is a field, then $\dim F = 0$.

(2) If R is a PID, which is not a field (for example $R = F[x]$), then $\dim R = 1$. Indeed, every non-zero ideal is of the form (f), which is prime if and only if f is prime. Furthermore, $(f) \subsetneq (g)$ is equivalent to g being a non-trivial divisor of f, which cannot happen with primes. Therefore, each maximal chain of prime ideals is of the form $(0) \subseteq (f)$, where $f \in R$ is prime.

(3) It is not immediate, but one can prove that $\dim F[x_1, \dots, x_n] = n$; one can obtain this result for example by combining Theorem 6.1.12 with point (1) of Example 6.1.11.

Let us recall a few notations and notions from the theory of fields extensions. If $F \subseteq L$ is a field extension, then a(n) (ordered or unordered) collection A of elements of L is *algebraically independent* over F if for any multivariable polynomial $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ and any choice of n distinct elements $a_1, \dots, a_n \in A$, we have $f(a_1, \dots, a_n) \neq 0$. We will denote by $F(A)$ the subfield of L generated by F and A, and by $F[A]$ the subring of L generated by F and A. It is crucial that one traces always whether in such a notation A is a subset or a collection of indeterminant elements. In the latter case, $F[x_1, \dots, x_n]$ and $F(x_1, \dots, x_n)$ denote the polynomial ring and the field of rational functions in the variables $x_1, \dots, x_n$. We also note that by definition $F(x_1, \dots, x_n) = \operatorname{Frac} F[x_1, \dots, x_n]$.

We also note that if $R \subseteq L$ is a subring, then $\operatorname{Frac}(R)$ can be identified naturally with the subfield $\left\{ \frac{r}{s} \in L \,\middle|\, r, s \in R, s \neq 0 \right\} \subseteq L$. In particular, this gives the relation $F(A) = \operatorname{Frac} F[A]$.

Definition 6.1.3. If $F \subseteq L$ is a field extension, a *transcendence basis* of L over F is a subset $A \subseteq L$, such that A is algebraically independent over F and L is algebraic over $F(A)$.

Remark 6.1.4. The notion of transcendence basis can be thought as the modification of a linear basis to the situation where we consider polynomial relations instead of linear relations. In particular, most proofs about transcendence bases have counterparts in linear algebra. Furthermore, the main ideas in these counterparts are the same, but the transcendence basis proofs are typically a bit more involved because polynomial relations are trickier than linear relations.

Lemma 6.1.5. *If $F \subseteq L$ is a field extension, and $b \in L$ is algebraic over $F(a_1, \dots, a_m) \subseteq L$, then there exists a polynomial $f \in F[x_1, \dots, x_n, y]$ such that $f(a_1, \dots, a_m, b) = 0$ and $f(a_1, \dots, a_m, y) \in F(a_1, \dots, a_m)[y] \neq 0$.*

Proof. Consider the minimal polynomial $\sum_i c_i y^i \in F(a_1, \dots, a_m)[y]$ of b over $F(a_1, \dots, a_m)$. Note that by the paragraph before Definition 6.1.3, the generated subfield is always the fraction field of the generated subring. Applying this to $F(a_1, \dots, a_m)$ we obtain that for each $c_i \in F(a_1, \dots, a_m)$, we may find polynomials $g_i, h_i \in F[x_1, \dots, x_n]$ such that $c_i = \frac{g_i(a_1, \dots, a_m)}{h_i(a_1, \dots, a_m)}$ and additionally $h_i(a_1, \dots, a_m) \neq 0$ for every i. However, then the polynomial

$$\left(\prod_i h_i(a_1, \dots, a_m) \right) \left(\sum_i \frac{g_i(a_1, \dots, a_m)}{h_i(a_1, \dots, a_m)} y^i \right) = \sum_i \left(g_i(a_1, \dots, a_m) \prod_{j \neq i} h_j(a_1, \dots, a_m) y^i \right) \in F(a_1, \dots, a_m)[y]$$

is also a minimal polynomial of b over $F(a_1, \dots, a_m)$, and additionally it can be written as $f(a_1, \dots, a_m, y)$ for

$$f(x_1, \dots, x_m, y) = \sum_i \left(g_i(x_1, \dots, x_m) \prod_{j \neq i} h_j(x_1, \dots, x_m) y^i \right) \in F[x_1, \dots, x_m, y].$$

□

Lemma 6.1.6 (Exchange lemma)**.** *If $F \subseteq L$ is a field extension, and $b \in L$ is algebraic over $F(a_1, \ldots, a_m) \subseteq L$ but not over $F(a_1, \ldots, a_{m-1})$, then a_m is algebraic over $F(a_1, \ldots, a_{m-1}, b)$.*

Proof. Let $f \in F[x_1, \ldots, x_n, y]$ given by Lemma 6.1.5. Write

$$f(a_1, \ldots, a_{m-1}, x_m, y) = \sum_{i,j} f_{i,j} x_m^i y^j,$$

where $f_{i,j} \in F[a_1, \ldots, a_{m-1}]$. By the statement of Lemma 6.1.5 the above polynomial is non-zero even after plugging a_m into x_m. Hence, $f(a_1, \ldots, a_{m-1}, x_m, y) \in F(a_1, \ldots, a_{m-1})[x_m, y]$ is non-zero. In particular, there are indices i such that the polynomial $\sum_j f_{i,j} y^j \in F[a_1, \ldots, a_{m-1}][y]$ is not zero. However, for any such index also $\sum_j f_{i,j} b^j \neq 0$, because b is not algebraic over $F(a_1, \ldots, a_{m-1})$. So, we obtain that the polynomial

$$\sum_{i,j} f_{i,j} b^j x_m^i \in F[a_1, \ldots, a_{m-1}, b][x_m]$$

is non-zero. This concludes our proof, since a_m is a root of the latter polynomial. □

Lemma 6.1.7. *If $F \subseteq L$ is a field extension, $A = \{a_1, \ldots, a_n\} \subseteq L$ and $B = \{b_1, \ldots, b_m\} \subseteq L$, such that A is algebraically independent over F and every element of A is algebraic over $F(B)$, then $n \leq m$.*

Proof. Let $a_1, \ldots, a_r$ be the common elements of A and B ($r = 0$ is allowed). The statement is clear if $r = n$. We prove the statement by a descending induction on r. Assume that $r < n$. We may assume that $a_i = b_i$ for $i \leq r$. Choose then a minimal subset $C \subseteq \{b_{r+1}, \ldots, b_m\}$. Such that a_{r+1} is algebraic over $F(\{a_1, \ldots, a_r\} \cup C) = F(\{b_1, \ldots, b_r\} \cup C)$. Note that $C \neq \emptyset$, as $a_1, \ldots, a_{r+1}$ are algebraically independent. Let b_i be an element of C. Then, by Lemma 6.1.6, b_i, and then also A, is algebraic over $F(B \cup \{a_{r+1}\} \setminus \{b_i\})$. So, we may replace B with the latter, and then use induction. □

Corollary 6.1.8. *In the situation of Definition 6.1.3, if there is a finite transcendence basis, then all transcendence bases have the same number of elements in them.*

Proof. It follows immediately from Lemma 6.1.7 □

Definition 6.1.9. The *transcendence degree* $\operatorname{trdeg}_F L$ of a field extension $F \subseteq L$ is the number of elements of a transcendence basis of L over F. This is well defined by Corollary 6.1.8 if it exists.

Before the next lemma, note that being a quotient ring of $F[x_1, \ldots, x_m]$ is the same statement as being a finitely generated F-algebra.

Lemma 6.1.10. *If R is a quotient ring of $F[x_1, \ldots, x_m]$, then $\operatorname{Frac} R$ has a transcendence basis, and hence its transcendence degree exists.*

Proof. The residues of $\overline{x}_i$ of x_i in R generate R as a ring extension of F. Hence, they also generate $\operatorname{Frac} R$ as a field extension of F. Set $A_0 := \{\overline{x}_1, \ldots, \overline{x}_m\}$. We do not keep track of the assumption that A_0 generates $\operatorname{Frac} R$, but only that $\operatorname{Frac} R$ is algebraic over $F(A_0)$.

If A_0 is algebraically independent of F, then it yields a transcendence basis of $\operatorname{Frac} R$ over F by definition (Definition 6.1.3). Otherwise it contains an element $\overline{x}_i$, which is algebraic over the other elements of A_0. In this case set $A_1 := A_0 \setminus \{\overline{x}_i\}$ and repeat the argument of this paragraph for A_0 replaced by A_1. Note that as $\overline{x}_i$ is algebraic over A_1, so it will be the entire $\operatorname{Frac}(R)$. In particular, all our assumptions on A_0 will be satisfied also by A_1.

As there are finitely many elements in A_0 this process will stop with A_j, which will be algebraically independent over F and over which $\operatorname{Frac} R$ will be algebraic. In particular A_j will be a transcendence basis. □

Example 6.1.11. (1) $\operatorname{trdeg}_F F(x_1, \ldots, x_n) = n$.

(2) $\operatorname{trdeg}_F \left(F(x_1)[x_2] \Big/ (x_1^2 + x_2^3) \right) = 1$ because $\{x_1\}$ is a transcendence basis of $F(x_1)[x_2] \Big/ (x_1^2 + x_2^3)$ over F.

We claim hat $F(x_1)[x_2] \Big/ (x_1^2 + x_2^3) \cong \operatorname{Frac}(R)$, where $R = F[x_1, x_2] \Big/ (x_1^2 + x_2^3)$ (and hence by symmetry $F(x_1)[x_2] \Big/ (x_1^2 + x_2^3) \cong F(x_2)[x_1] \Big/ (x_1^2 + x_2^3)$). The construction of this isomorphism goes through the following steps:

- Consider $F[x_1] \hookrightarrow F[x_1, x_2]$.
- As $\{ f(x_1^2 + x_2^3) \mid f \in F[x_1, x_2] \} = (x_1^2 + x_2^3) \subseteq F[x_1, x_2]$, we have $(x_1^2 + x_2^3) \cap F[x_1] = \{0\}$. It follows that $F[x_1] \hookrightarrow F[x_1, x_2]$ induces an embedding $F[x_1] \hookrightarrow F[x_1, x_2] \Big/ (x_1^2 + x_2^3) = R$, the image of which is $F[\overline{x}_1]$, where $\overline{x}_i$ is the residue class of x_i in R.
- Taking fraction fields we obtain ring embeddings:

$$F(x_1) = \operatorname{Frac} F[x_1] \cong F(\overline{x}_1) \to \operatorname{Frac} R$$

- By definition of R, we have $F(\overline{x}_1)[\overline{x}_2] = \operatorname{Frac} R$
- To conclude the argument one needs to show that the minimal polynomial of $\overline{x}_2$ over $F(\overline{x}_1)$ is $m(t) = \overline{x}_1^2 + t^3$. Note that as $\deg m(t) = 3$ for this it is enough to show that $m(t)$ has no root over $F(\overline{x}_1) \cong F(x_1)$. So, assume the contrary, and let $\frac{g}{h} \in F(x_1)$ be a root of $m(t)$. Then we have the following equality in $F(x_1)$:

$$x_1^2 + \left(\frac{g}{h}\right)^3 = 0$$

Multiplying by h^3 we obtain another equality, but now in $F[x_1]$:

$$x_1^2 h^3 + g^3 = 0$$

However, this is impossible, because $3 | \deg g^3$, but $\deg x_1^2 h^3 \equiv 2 \mod (3)$.

(3) $\operatorname{trdeg}_{\mathbb{Q}} \mathbb{C}$ is HUGE.

We will prove eventually the following

Theorem 6.1.12. *If R is an integral domain, which is a quotient of $F[x_1, \ldots, x_n]$ for some field F, then*

$$\dim R = \operatorname{trdeg}_F \operatorname{Frac}(R)$$

And sooner we will prove the special case:

Theorem 6.1.13. *Let R be a domain, which is a quotient of $F[x_1, \ldots, x_n]$ for some field F. If $\operatorname{trdeg}_F \operatorname{Frac}(R) > 0$, then R is not a field.*

We delay the proof of Theorem 6.1.12 and Theorem 6.1.13 until we have the necessary background.

We note that the condition of R being a quotient of $F[x_1, \ldots, x_n]$ is equivalent to requiring that R is a finitely generated F-algebra. Here, being an F-algebra can be either defined as in point (2) of Example 2.1.2, or using that R is commutative as having an injective ring homomorphism $F \hookrightarrow R$ (in the non-commutative case one has to require that the image of this injection is contained in the center of R).

6.2 NOETHER NORMALIZATION

For the proof of Theorem 6.1.13, we have to understand the structure of the quotients of $F[x_1, \dots, x_n]$ much deeper. It turns out that they are very closely related to the polynomial ring, that is, they are extensions of an adequate polynomial ring with nice properties (Noether normalization, Theorem 6.2.10). More precisely this extension is integral (also called finite), the definition of which is our first goal:

Definition 6.2.1. If $S \supseteq R$ is a ring extension, then $s \in S$ is said to be *integral* over R, if it satisfies a monic polynomial with coefficients in R. Here monic means that the leading coefficient is 1. That is, we have an equation of the form

$$s^n + \sum_{i=0}^{n-1} r_i s^i = 0 \tag{2.1.a}$$

for some $r_i \in R$.

The extension $S \supseteq R$ is integral, if all the elements of S are integral over R.

Example 6.2.2. (1) $\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$ because it satisfies the monic polynomial $x^2 - 2$. Using Corollary 6.2.6 we will see that in fact the subring $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{C}$ yields an integral extension $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{2}]$.

(2) $\frac{1}{2} \in \mathbb{C}$ is not integral over $\mathbb{Z}$, because assume that it satisfies an equation of the following form with $r_i \in \mathbb{Z}$:

$$\left(\frac{1}{2}\right)^n + \sum_{i=0}^{n-1} r_i \left(\frac{1}{2}\right)^i = 0$$

Multiplying by 2^n we obtain

$$1 + \sum_{i=0}^{n-1} r_i 2^{n-i} = 0$$

which is a contradiction as it would imply that 2 divides 1.

Proposition 6.2.3. *In the situation of Definition 6.2.1, the following are equivalent*

(1) s is integral

(2) $R[s] \subset S$ is a finitely generated R-module

(3) $R[s] \subset S$ is contained in a subring $R \subseteq T \subseteq S$ such that T is a finite R-module

Proof. *(1) $\Rightarrow$ (2):* (2.1.a) shows that $1, s, \dots, s^{n-1}$ is an R-generator set of $R[s]$.
(2) $\Rightarrow$ (3): take $T = R[s]$.
(3) $\Rightarrow$ (1): Let $1 = y_1, \dots, y_n$ be generators of T as an R-module, and write

$$s \cdot y_i = \sum_j r_{j,i} y_j$$

So, the matrix

$$C := (r_{j,i} - \delta_{i,j} s)$$

with elements in S, multiplies the column vector

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

to zero. Let $\operatorname{adj}(C)$ denote the adjugate matrix of C. Then the following products of vectors, scalars and matrices over S holds:

$$\det(C)\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \operatorname{adj}(C)C\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0$$

In particular, $0 = \det(C)y_1 = \det(C)$, as $y_1 = 1$. However, $\det C$ is obtained by evaluating the monic polynomial $\det(r_{j,i} - \delta_{i,j}x) \in R[x]$ at s. This shows that s is indeed integral over R. □

End of 8. class, on 08.11.2021.

Lemma 6.2.4. *If $T \supseteq S$ and $S \supseteq R$ are ring extensions such that the bigger ring is a finitely generated module over the smaller, then T is a finitely generated module over R.*

Proof. By definition we have an S-module surjection $S^{\oplus n} \twoheadrightarrow T$ for some integer $n > 0$, and an R-module surjection $R^{\oplus m} \twoheadrightarrow S$. By combining these two, we obtain R-module homomorphisms $R^{\oplus m\cdot n} \twoheadrightarrow S^{\oplus n} \twoheadrightarrow T$. □

Corollary 6.2.5. *If $T \supseteq S$ and $S \supseteq R$ are integral ring extensions, then so is $T \supseteq R$.*

Proof. Let $t \in T$ be an element of T. We want to show that t is integral over R. Let $a_0, \dots, a_d$ be the coefficients of a monic polynomial that t satisfies over S. Consider then a_i is integral over R, and hence also it is integral over $R[a_0, \dots, a_{i-1}]$. So, by Proposition 6.2.3, $R[a_0, \dots, a_i]$ is a finitely generated module over $R[a_0, \dots, a_{i-1}]$. Again, by Proposition 6.2.3, $R[a_0, \dots, a_d, t]$ a finitely generated module over $R[a_0, \dots, a_d]$. By applying Lemma 6.2.4 inductively we obtain that $R[a_0, \dots, a_d, t]$ is a finitely generated module over R. Hence, by Proposition 6.2.3, t is integral over R. □

Corollary 6.2.6. *If $S \supseteq R$ is a ring extension, then the elements in S that are integral over R form a subring of S.*

Proof. Let $s, s' \in S$ be integral over R. Then, s' is also integral over $R[s]$. Hence, by point (2) of Proposition 6.2.3 we obtain that $R[s]$ is a finitely generated R-module and $R[s, s']$ is a finitely generated $R[s]$ module. Then, it follows that $R[s, s']$ is a finitely generated R-module, by Lemma 6.2.4. Point (3) of Proposition 6.2.3 concludes then the proof, as it shows that every element of $R[s, s']$ is integral over R, and hence $s + s'$, ss', and $-s$ are all integral over R. □

Definition 6.2.7. The subring of Corollary 6.2.6 is called the *integral closure of R in S*. If R is a domain, then the integral closure of R in $\operatorname{Frac}(R)$ is called the *integral closure of R*.

Example 6.2.8. If R is a UFD, then its integral closure is itself. Indeed, choose a and b coprime elements of R. If $\frac{a}{b} \in \operatorname{Frac} R$ is integral over R, then for some $r_i \in R$ it satisfies

$$\left(\frac{a}{b}\right)^n + \sum_{i=0}^{n-1} r_i \left(\frac{a}{b}\right)^i = 0.$$

Hence, it also satisfies

$$(a)^n + \sum_{i=0}^{n-1} r_i \,(a)^i \, b^{n-i} = 0.$$

This shows that $b|a^n$ which contradicts the choice that a and b is coprime, unless b is a unit.

Example 6.2.9. Let F be a field. We have learned in "Anneaux et corps" that $F[x,y,z]$ is a UFD. Additionally by the Eisenstein criterion $x^2 - y^2z \in F[x,y,z]$ is prime if there is a prime element p of $F[y,z]$ such that $p \nmid x^2$, $p | y^2z$, and $p^2 \nmid y^2z$. Choosing $p = z$ shows that indeed $x^2 - y^2z$ is prime. Then $R := F[x,y,z] \Big/ (x^2 - y^2z)$ is a domain.

Denote by $\overline{x}$, $\overline{y}$ and $\overline{z}$ the residues of x, y and z in R. Then we have $\overline{x}^2 = \overline{y}^2\overline{z}$, and hence $\left(\frac{\overline{x}}{\overline{y}}\right)^2 = \overline{z}$. In particular, $\frac{\overline{x}}{\overline{y}}$ is integral over R.

Let S be the integral closure of R. By the above, we have $S \supseteq F\left[\frac{\overline{x}}{\overline{y}}, \overline{y}\right]$. Furthermore, $\frac{\overline{x}}{\overline{y}}$ and $\overline{y}$ are algebraically independent, because otherwise we would get the following contradiction:

$$2 > \operatorname{trdeg}_F \left(\operatorname{Frac} F\left[\frac{\overline{x}}{\overline{y}}, \overline{y}\right] \right) \geq \operatorname{trdeg}_F \operatorname{Frac}(R) \underset{\uparrow}{=} 2.$$

$\overline{y}$ and $\overline{z}$ are algebraically independent elements of R, because the relations between the elements $\overline{x}$, $\overline{y}$ and $\overline{z}$ correspond to the elements of the ideal $(x^2 - y^2z) \subseteq F[x,y,z]$, all of which contains x

Summarizing, we obtained containments

$$\operatorname{Frac}(R) \supseteq S \supseteq \underbrace{F\left[\frac{\overline{x}}{\overline{y}}, \overline{y}\right]}_{\uparrow} \supseteq R. \tag{2.9.b}$$

$\cong F[t_1, t_2]$, where t_i are independent variables

Taking fraction fields we obtain then the containmens

$$\operatorname{Frac}(R) \supseteq F(t_1, t_2) \supseteq \operatorname{Frac}(R).$$

In particular, $\operatorname{Frac}(R) = F(t_1, t_2)$. By (2.9.b) and by the fact that S is integral over $F[t_1, t_2]$ we obtain that the integral closure of $F[t_1, t_2]$ contains S. However, the integral closure of $F[t_1, t_2]$ is itself by Example 6.2.8. This shows that $S = F[t_1, t_2] = F\left[\frac{\overline{x}}{\overline{y}}, \overline{y}\right]$.

In these notes, and typically in abstract algebra in general around the world, *monomial* means a monic polynomial with only one term. So, if we work over a field F, then this means an element of the form $\prod_{i=1}^n x_i^{d_i} \in F[x_1, \ldots, x_n]$. Note that the French use of language typically considers non-monic polynomials as monomials too.

Theorem 6.2.10. NOETHER NORMALIZATION *Let F be a field, and R is a quotient of $F[x_1, \ldots, x_n]$. Then there is subring S of R such that $S \cong F[t_1, \ldots, t_r]$ as an F-algebra and such that R is integral over S.*

Proof. Before starting the proof we also note that x_i, y_i and t_i denote indeterminant elements throughout the proof, while $\overline{x}_i$ denote the residue classes, or equivalently the cosets of x_i in R.

We prove the statement by induction on n.

$n = 1$: $R \cong F[x_1] \Big/ (f(x_1))$ for some $f(x_1) \in F[x_1]$. We have two cases:

- $f = 0$, then $R \cong F[t_1]$, and hence we may choose $S = F[\overline{x}_1]$.
- If $f \neq 0$, by dividing by the leading coefficient of $f(x_1)$, we may assume that it is monic. This shows that the residue class $\overline{x}_1$ of x_1 in R is integral over F. As R is generated by $\overline{x}_1$ over F, we may choose $S = F$.

$n > 1$: So, from now we assume that we know the statement for smaller values of n. Then, after reordering the variables, by Lemma 6.1.5 we can assume that there is a polynomial $g(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$ such that $g(\overline{x}_1, \ldots, \overline{x}_n) = 0$, and $g(\overline{x}_1, \ldots, \overline{x}_{n-1}, y_n) \neq 0$ as a

polynomial in y_n. Indeed, otherwise $\overline{x}_i$ are algebraically independent, and hence we may choose $S = R$.

Let d be the degree of g, and set $\tilde{y}_i = y_i - y_n^{N^{n-i}}$ for $1 \leq i \leq n-1$ and for integers $N \geq 1$ to be specified later. Consider the polynomial

$$g(y_1, \ldots, y_n) = g\Big(\Big(y_1 - y_n^{N^{n-1}}\Big) + y_n^{N^{n-1}}, \ldots, \Big(y_{n-1} - y_n^{N}\Big) + y_n^{N}, y_n\Big)$$
$$= g\Big(\tilde{y}_1 + y_n^{N^{n-1}}, \ldots, \tilde{y}_{n-1} + y_n^{N}, y_n\Big) \quad (2.10.c)$$

Let us regard the latter polynomial as a polynomial in y_n over $F[\tilde{y}_1, \ldots, \tilde{y}_{n-1}]$. Let us assume that we are able to choose N such that this polynomial, after possibly dividing by an element of F, is a monic polynomial $\tilde{g} \in \big(F[\tilde{y}_1, \ldots, \tilde{y}_{n-1}]\big)[y_n]$. Then, by the definition of $\tilde{g}$ we have

$$0 = \tilde{g}\Big(\overline{x}_1 - \overline{x}_n^{N^{n-1}}, \ldots, \overline{x}_{n-1} - \overline{x}_n^{N}, \overline{x}_n\Big),$$

which shows that $\overline{x}_n$ is integral over $R' := F\Big[\overline{x}_1 - \overline{x}_n^{N^{n-1}}, \ldots, \overline{x}_{n-1} - \overline{x}_n^{N}\Big]$. As the ring R' is a quotient of an $n-1$-variable polynomial ring over F, we may apply our induction assumption. This yields the subring $F[t_1, \ldots, t_r] \cong S \subseteq R'$, over which R' is integral. As R is integral over R', we obtain that R is integral over S too, by Corollary 6.2.5.

So, we are left to choose N such that $\tilde{g}$ is monic in y_n after possibly dividing by an element of F. Let

$$C = \left\{ (c_1, \ldots, c_n) \in \mathbb{N}^n \;\middle|\; \sum_{i=1}^{n} c_i \leq d \right\}$$

Choose then an integer $N > 1$ such that:

(1) for every $(a_1, \ldots, a_n) \in C \setminus \big\{(0, \ldots, 0, d)\big\}$ we have

$$d < \sum_{i=1}^{n} a_i N^{d-i}$$

As all such sums are at least as big as N, this is true for $N \geq d+1$.

(2) for every $(a_1, \ldots, a_n) \neq (b_1, \ldots, b_n) \in C$ we have

$$\sum_{i=1}^{n} a_i N^{d-i} \neq \sum_{i=1}^{n} b_i N^{d-i} \quad (2.10.d)$$

This is doable as for each $(a_1, \ldots, a_n) \in C$ the expression $\sum_{i=1}^{n} a_i N^{d-i}$ is a polynomial in N, and additionally for different choices of elements of C this polynomial is different. There is one special polynomial out of these that is the one associated to $(0, \ldots, 0, d)$, which is just the constant d polynomial. The other polynomials are all monotone increasing for large values of N. Additionally, as they are all different polynomials, no two of them have common values for big enough N. As C is finite, this means that for setting N big enough we can actually make (2.10.d) hold.

Now, we are ready to conclude that $\tilde{g}$ is monic, after possibly dividing by an element of F. If all the monomials of g are just powers of y_n, then $\tilde{g}$ is of the form $c_d y_n^d + \cdots + c_1 y + c_0$ for $c_i \in F$. Hence $\tilde{g}$ becomes monic after dividing by c_d. Otherwise, by the choice of N, the leading term of $\tilde{g}$ is of the form

$$\prod_{i=1}^{n} y_n^{a_i N^{n-i}}$$

for some $(a_1, \ldots, a_n) \in C$ by our choice of N. Hence, $\tilde{g}$ is monic in this case too. □

Remark 6.2.11. In the situation of Theorem 6.2.10, if R is an integral domain, then $\operatorname{trdeg}_F \operatorname{Frac}(R) = r$. Indeed, the inclusion $S \subset R$ induces $\operatorname{Frac}(S) \subseteq \operatorname{Frac}(R)$ on the level of fraction fields. As R is generated by integral elements over S, the same elements show that $\operatorname{Frac}(R)$ is an algebraic extension of $\operatorname{Frac}(S)$.

6.3 Proof of Theorem 6.1.13

Lemma 6.3.1. *Let R be an domain, which is an integral extension of a domain S. R is a field if and only if so is S.*

Proof. $\boxed{\Longrightarrow:}$ Assume first that R is a field. Let $s \in S \setminus \{0\}$. Then $s^{-1} \in R$ exists. We have to show that s^{-1} is in fact in S. Since R is an integral extension of S, we may write

$$\left(s^{-1}\right)^n + \sum_{i=0}^{n-1} a_i \left(s^{-1}\right)^i = 0,$$

for some $a_i \in S$. However, then the following equation shows that $s^{-1} \in S$:

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

$\boxed{\Longleftarrow:}$ Now, assume that S is a field. Let $r \in R \setminus \{0\}$. We may write

$$r^n + \sum_{i=0}^{n-1} a_i r^i = 0.$$

By dividing by r (using that R is an integral domain), we may assume that $a_0 \neq 0$. Then, the following equation shows that r has an inverse in R:

$$\left(\frac{r^{n-1}}{-a_0} + \sum_{i=1}^{n-1} \frac{a_i r^{i-1}}{-a_0}\right) r = 1.$$

□

Remark 6.3.2. The proof of Lemma 6.3.1 shows that if $S \subseteq R$ is an integral extension of rings (not necessarily domains!) then $s \in S$ is invertible in R if and only if it is also invertible in S.

Proof of Theorem 6.1.13. According to the Noether normalization (Theorem 6.2.10) and Remark 6.2.11, there is $S \subseteq R$, such that $S \cong F[t_1, \ldots, t_r]$, and $\operatorname{trdeg}_F \operatorname{Frac}(R) = r$. In particular $r > 0$, so S is not a field. Then R cannot be a field by Lemma 6.3.1. □

Remark 6.3.3. In the situation of the Theorem 6.1.13, the polynomial ring S is a field if and only if $r = 0$. Since by Lemma 6.3.1 R is a field if and only if S is a field it follows that R is a field if and only if $r = 0$. It is easy to see that an integral domain R has dimension zero if and only if it is a field. Therefore, we have proven that if R is an integral domain that is a quotient of $F[x_1, \ldots, x_n]$ for some field F then $\dim(R) = 0$ if and only if $\operatorname{trdeg}_F \operatorname{Frac}(R) = 0$. This is a special case of Theorem 6.1.12

End of 9. class, on 15.11.2021.

Chapter 7

The proof of Theorem 6.1.12

The goal of this chapter is to prove Theorem 6.1.12. After Noether normalization (Theorem 6.2.10) the main missing piece is to compare dimensions of two rings involved in an integral extension (Corollary 7.4.4). For this one has to compare chains of prime ideals, for which it is essential to develop a tool where one can focus just on a particular part of a chain (as in that case we can use simple arguments as in Lemma 6.3.1). The corresponding technical tool is called localization. It is one of the most fundamental tools of commutative algebra, used many times in most commuative algebra arguments.

In fact, one can localize both rings and modules. The relation between the two is given by tensor product, which we develop in Section 7.1. Then in Section 7.2 we develop localization. In Section 7.3 we work out the way localization interacts with ideals. Finally we put everything together in Section 7.4, where we also show Theorem 6.1.12.

7.1 Tensor product

Definition 7.1.1. Let M, N and P be modules over R. A R-bilinear map $\phi : M \oplus N \to P$ is a map satisfying the following identities ($r \in R$, the others are elements of the respective modules):

(1) $\phi(m_1 + m_2, n) = \phi(m_1, n) + \phi(m_2, n)$

(2) $\phi(m, n_1 + n_2) = \phi(m, n_1) + \phi(m, n_2)$

(3) $\phi(rm, n) = r\phi(m, n)$

(4) $\phi(m, rn) = r\phi(m, n)$

Example 7.1.2. (1) If $\alpha : S \to R$ and $\beta : T \to R$ are ring homomorphisms, then the following map is $\mathbb{Z}$-bilinear

$$\begin{array}{ccc} S \times T & \longrightarrow & R \\ \cup & & \cup \\ (s,t) & \longmapsto & \alpha(s)\beta(t) \end{array}$$

(2) Similarly, if $\alpha : S \to R$ and $\beta : T \to R$ are F-algebra homomorphisms for some field F, then the following map is F-bilinear

$$\begin{array}{ccc} S \times T & \longrightarrow & R \\ \cup & & \cup \\ (s,t) & \longmapsto & \alpha(s)\beta(t) \end{array}$$

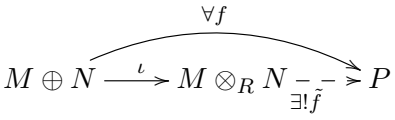
(3) Consider a $\mathbb{Z}$-bilinear map $\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to P$. Then, for any $[y] \in \mathbb{Z}/2\mathbb{Z}$ and $[x] \in \mathbb{Z}/3\mathbb{Z}$ we have

$$\phi([y],[x]) = \phi([y],[4x]) = 2\phi([y],[2x]) = \phi([2y],[2x]) = \phi([0],[2x])$$
$$= \phi(0\cdot[0],[2x]) = 0\cdot\phi([0],[2x]) = 0$$

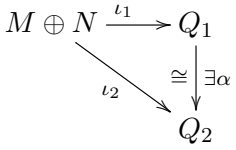
So, $\phi \equiv 0$.

Tensor products are the universal objects for bilinear maps:

Theorem 7.1.3. *Let M and N be modules over R. There exists an R-module $M \otimes_R N$ and an R-bilinear map $\iota : M \oplus N \to M \otimes_R N$ such that for every R-module P and every R-bilinear map $f : M \oplus N \to P$, there exists a unique R-homomorphism $\tilde{f} : M \otimes_R N \to P$, such that $\tilde{f} \circ \iota = f$:*



Moreover, the pair $(M \otimes_R N, \iota)$ is unique upto unique isomorphism, i.e., if (Q_1, ι_1) and (Q_2, ι_2) are two such pairs then there exists a unique isomorphism of R-modules $\alpha : Q_1 \to Q_2$ such that $\iota_2 = \alpha \circ \iota_1$.



Proof. *Unicity:* Let (Q_1, j_1) and (Q_2, j_2) be two candidates for $M \otimes_R N$. Then by the universal property there are unique maps $\tilde{j_2} : Q_1 \to Q_2$ and $\tilde{j_1} : Q_2 \to Q_1$ such that $\tilde{j_2} \circ j_1 = j_2$ and $\tilde{j_1} \circ j_2 = j_1$. Using the the unicity $\tilde{j_1} \circ \tilde{j_2} = \mathrm{Id}_{Q_1}$ and $\tilde{j_2} \circ \tilde{j_1} = \mathrm{Id}_{Q_2}$.

Existence: Denote by $R^{M\oplus N}$, the free R module with basis given by $e_{m,n}$ for some $m \in M, n \in N$. That is, a general element of $R^{M\oplus N}$ is of the form $\sum_{(m,n)\in I} \lambda_{m,n} e_{m,n}$ for some finite subset I of $M \oplus N$. Let K be the submodule of $R^{M\oplus N}$ generated by elements of the form

(1) $e_{m_1,n} + e_{m_2,n} - e_{m_1+m_2,n}$,

(2) $e_{m,n_1} + e_{m,n_2} - e_{m,n_1+n_2}$,

(3) $e_{rm,n} - r e_{m,n}$ and

(4) $e_{m,rn} - r e_{m,n}$.

Then, we define $M \otimes_R N$ to be $R^{M\oplus N}/K$, and $m \otimes n$ is the image of $e_{m,n}$ in $M \otimes_R N$. Lastly, we define $\iota((m,n)) := m \otimes n$. The map ι is indeed bilinear, since

(1) $\iota(m_1+m_2, n) = (m_1+m_2)\otimes n = m_1 \otimes n + m_2 \otimes n = \iota(m_1,n) + \iota(m_2,n)$, where the middle equality follows since $e_{m_1,n} + e_{m_2,n} - e_{m_1+m_2,n} \in K$.

(2) the other conditions of bilinearity are similar.

We are left to show that $M \otimes_R N$ satisfies the universal property. That is, given a bilinear map $f : M \oplus N \to P$ we have to define an R-module map $\tilde{f} : M \otimes N \to P$ as above. We have to have $\tilde{f} \circ \iota = f$, which forces $\tilde{f}(m \otimes n) = \tilde{f}(\iota((m,n))) = f((m,n))$. So, using that the elements $m \otimes n$ are R-module generators of $M \otimes_R N$, if the R-module homomorphism $\tilde{f}$ exists it is unique. We just have to show that $\tilde{f}$ is an R-module homomorphism and that it is well defined. The usual way to show this is that one considers the natural lift $\tilde{f}' : R^{M\oplus N} \to P$,

which in this case is given with the formula $\tilde{f}'(e_{m,n}) = f(m,n)$, and extend linearly by the universal property of free modules. Then $\tilde{f}'$ is automatically an R-module homomorphism, and hence, it is enough to show that $K \subseteq \ker \tilde{f}'$, for which it is enough to show that the generators of K are taken to 0 by $\tilde{f}'$. We do this below:

(1) $\tilde{f}'(e_{m_1,n}+e_{m_2,n}-e_{m_1+m_2,n}) = \tilde{f}'(e_{m_1,n})+\tilde{f}'(e_{m_2,n})-\tilde{f}'(e_{m_1+m_2,n}) = f(m_1,n)+f(m_2,n)-f(m_1+m_2,n) = 0$, where in the last equality we used that f is bilinear.

(2) the rest is similar.

□

Proposition 7.1.4. *$R \otimes_R M \cong M$, via the bilinear map $\iota' : R \oplus M \to M$ given by $\iota'((r,m)) = rm$.*

Proof. ι' is a bilinear map, so we only have to verify the universal property. Let $f : R \oplus M \to P$ be a bilinear map. Assume $\tilde{f} : M \to P$ is an R-module homomorphism, such that $f = \tilde{f} \circ \iota'$. Then necessarily $\tilde{f}(m) = \tilde{f}(\iota'(1,m)) = f(1,m)$. Hence, if $\tilde{f}$ exists, it is unique. Define then $\tilde{f}$ with the above formula. We have to verify that it is an R-module homomorphism (using that f is bilinear):

(1) $\tilde{f}(m_1+m_2) = f(1,m_1+m_2) = f(1,m_1)+f(1,m_2) = \tilde{f}(m_1)+\tilde{f}(m_2)$

(2) $\tilde{f}(rm) = f(1,rm) = rf(1,m) = r\tilde{f}(m)$.

□

Example 7.1.5. In general tensor products can behave very unexpectedly! For example by point (3) of Example 7.1.2 we have $\left(\mathbb{Z}/2\mathbb{Z}\right) \otimes_{\mathbb{Z}} \left(\mathbb{Z}/3\mathbb{Z}\right) \cong 0$.

Remark 7.1.6. The elements of $M \otimes_R N$ of the form $m \otimes n$ are called *simple tensors*. In the above examples (Proposition 7.1.4 and Example 7.1.5) each element of $M \otimes_R N$ is a simple tensor. This is not the case in general. There will be an exercise on the exercise sheet showing that if M and N are F-vector spaces, and $m_1, \dots, m_r$ and $n_1, \dots, n_s$ are F-vector spaces bases of M and N, respectively, then $\left\{ m_i \otimes n_j \;\middle|\; i = 1, \dots, r; j = 1, \dots, s \right\}$ is an F-vectors space basis of $M \otimes_F N$. In particular, elements such as $m_1 \otimes n_1 + m_2 \otimes n_2 \in M \otimes_R N$ are not simple tensors.

Remark 7.1.7. Let R be a ring and N an R-module. If we replace $\mathrm{Hom}(\_, N)$ by $\_ \otimes_R N$ in the definitions of $\mathrm{Ext}^i_R(M,N)$, we obtain $\mathrm{Tor}^i_R(M,N)$. The module N is called *flat* if the functor $\_ \otimes_R N$ is exact.

7.2 LOCALIZATION

Localization is an extremely useful tool. We mention just a few motivations here, but there are many more.

(1) Let F be an algebraically closed field. Consider the rational functions on F^2, that is, fractions f/g of 2 variable polynomials, which contain $(0,0)$ in their domain. This is equivalent to requiring that $g \notin (x,y)$. Such functions form a ring (trivially closed under addition and multiplication). In this case this ring can be easily described as a subring of $F(x,y)$:

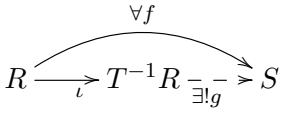
$$\left\{ \frac{f}{g} \in F(x,y) \,\middle|\, g \notin (x,y) \right\},$$

and is called the local ring at $(0,0)$. One would like to construct similar local ring on every subset of F^n defined by polynomial equations. The technical tool that does this algebraically (so without involving any geometry) is localization.

(2) A more algebraic motivation is that many times, we would like to generalize a statement known for maximal ideals to prime ideals. This is typically done using localization.

Definition 7.2.1. Multiplicatively closed subset $T \subseteq R$ is a subset such that $1 \in T$, and $a, b \in T \Rightarrow ab \in T$.

Theorem 7.2.2. *Let $T \subseteq R$ be a multiplicatively closed subset. Then there is a unique pair $(T^{-1}R, \iota)$, where $T^{-1}R$ is a ring and $\iota : R \to T^{-1}R$ is a ring homomorphism, such that for any ring homomorphism $f : R \to S$ for which every element of $f(T)$ is invertible, there is a unique homomorphism $g : T^{-1}R \to S$ such that $f = g \circ \iota$:*



Proof. *Unicity:* The proof of unicity follows the same pattern as we have seen with other objects defined by universal properties (e.g., Theorem 7.1.3). Homework: work out the details.

Existence: This part of proof is also similar in some sense to the corresponding part of the proof of Theorem 7.1.3. That is, we define $T^{-1}R$ as the quotient by an equivalence relation (although here it is not the quotient of a module, just of a set), and then we check all the properties. Unfortunately, there are even more details to check here than in the case of Theorem 7.1.3, so we will leave many of them as homework.

Whatever $T^{-1}R$ is, it has to contain elements of the form $\iota(r)$ for every $r \in R$, and also, if $r \in T$, then we have to be able to divide by $\iota(r)$. So, it has contain generally elements of the form $\iota(r)/\iota(t)$ for $r \in R$ and $r \in T$. Hence, we want to define $T^{-1}R$, as the set of pairs (t, r) ($t \in T$, $r \in R$), where we intuitively we think about (t, r) being formal fractions $\frac{r}{t}$. The operations then on these pairs have to be the ones corresponding to the above fraction representation. That is,

$$(t_1, r_1) \cdot (t_2, r_2) = (t_1 t_2, r_1 r_2),$$

and

$$(t_1, r_1) + (t_2, r_2) = (t_1 t_2, t_1 r_2 + t_2 r_1) \qquad -(t, r) = (t, -r).$$

We define the zero and unit element to be $(1, 0)$ and $(1, 1)$. Furthermore, also by thinking about the intuitive fraction representation, we see that we should introduce some kind of equivalence relation. The first natural suggestion is that let (t, r) and (t', r') equivalent if and only if $tr' - t'r = 0$. However, this does not quite qive an equivalence relation: take 3 pairs (t, r), (t', r') and (t'', r''), and assume that the first an second are equivalent and so are the second and the third. We want to prove that then the first and the third are also equivalent. So, we know that

$$t'r = tr', \text{ and } t''r' = t'r''.$$

We want to prove that $tr'' = rt''$. However, instead by multiplying the first equation by t'' and the second by t, we obtain:

$$t'rt'' = tr't'' = tt'r''.$$

So, instead of $tr'' - rt'' = 0$, we obtained that $t'(tr'' - rt'') = 0$. Since R does not have to be a domain, the latter does not imply the former. Hence, we have to relax our equivalence relation to the following:

$$(t, r) \equiv (t', r') \Leftrightarrow (tr' - t'r)u = 0 \quad (\exists u \in T).$$

Note that this is equivalent to $tr' - t'r = 0$ if R is a domain.

Now, we check that the above is an equivalence relation. Assume that we have the 3 pairs as before. That is, there are u and $u'' \in T$, such that

$$t'ru = tr'u \text{ and } r't''u'' = t'r''u''.$$

Then we obtain by multiplying the first equation by $t''u''$ and the second by tu that

$$t''u''t'ru = t''u''tr'u = tuu''r''t',$$

or equivalently

$$(t''r - r''t)u''t'u = 0.$$

Since, T is multiplicatively closed, $u''t'u \in T$, so indeed, $(t, r) \equiv (t'', r'')$.

We now have to check that the operations are well defined on the equivalence classes. We do the multiplication, and then we leave addition as homework. So, choose two-two equivalent pairs (t, r), (t', r') and $(\tilde{t}, \tilde{r})$, $(\tilde{t}', \tilde{r}')$. That is, there are $u, \tilde{u} \in T$ such that

$$(tr' - rt')u = 0, \text{ and } (\tilde{t}\tilde{r}' - \tilde{r}\tilde{t}')\tilde{u} = 0.$$

We need to prove then that $(t\tilde{t}, r\tilde{r})$ and $(t'\tilde{t}', r'\tilde{r}')$ are equivalent. Indeed

$$t\tilde{t}r'\tilde{r}'u\tilde{u} = rt'u\tilde{t}\tilde{r}'\tilde{u} = rt'u\tilde{t}'\tilde{r}\tilde{u},$$

or equivalently

$$(t\tilde{t}r'\tilde{r}' - t'\tilde{t}'r\tilde{r})u\tilde{u},$$

which concludes proving that multiplication is well-defined using that T is multiplicatively closed. As we already said we leave addition as homework. Hence, we are ready with well definedness of operations. We also have to check that the operations yield a ring, that is, $+$ is associative $(1, 0)$ is identity for $+$, etc. We leave this also as homework.

We define then ι as $\iota(r) = (1, r)$. (Homework: this is a homomorphism. Actually, the operations on $T^{-1}R$ are defined exactly so that this holds.)

We have then for any $t \in T$, that $\iota(t) = (1, t)$ is invertible as $(1, t) \cdot (t, 1) = (t, t) \equiv (1, 1)$.

We are left then to show the universal property. So, assume we are given a ring homomorphism $f : R \to S$, such that $f(t)$ is invertible for all $t \in T$. The we define $g\big((t, r)\big) := f(t)^{-1}f(r)$. Indeed, this is the only map that satisfies $f = g \circ \iota$. So, we are done with unicity. We are left to show that g is well defined and that it is a ring homomorphism.

For the well definedness, choose two equivalent pairs (t, r) and (t', r'). That is, there is an $u \in T$, such that $u(tr' - rt') = 0$. Then applying f to this equality, we obtain

$$f(u)(f(t)f(r') - f(r)f(t')) = 0$$

Since $f(u)$ is invertible, we may multiply with $f(u)^{-1}$, and obtain $f(t)f(r') - f(r)f(t') = 0$. However, then

$$g\big((t, r)\big) = f(t)^{-1}f(r) = f(t')^{-1}f(r') = g\big((t', r')\big).$$

Finally, g is a ring homomorphism, by the computation below.

(1) $g\big((t, r)(t', r')\big) = g\big((tt', rr')\big) = f(tt')^{-1}f(rr') = f(t)^{-1}f(t')^{-1}f(r)f(r') = g\big((t, r)\big)g\big((t', r')\big)$

(2) $g\big((t, r) + (t', r')\big) = g\big((tt', tr' + rt')\big) = f(tt')^{-1}f(tr' + rt') = f(t)^{-1}f(t')^{-1}(f(t)f(r') + f(r)f(t')) = f(t)^{-1}f(r) + f(t')^{-1}f(r') = g\big((t, r)\big) + g\big((t', r')\big)$.

□

Notation 7.2.3. The element (t, r) from the proof of Theorem 7.2.2 is usually denoted by $\frac{r}{t}$. Computation with these is done as usually with fractions, keeping in mind that two fractions like this $\frac{r}{t}$ and $\frac{r'}{t'}$ can be equal even if they are not equal in the traditional sense as fractions, that is even if $tr' - rt' \neq 0$, but $u(tr' - rt') = 0$ for some $u \in T$.

Example 7.2.4. (1) In the situation of Theorem 7.2.2,

$$\ker \iota = \left\{ r \in R \;\middle|\; \frac{r}{1} = \frac{0}{1} \in T^{-1}R \right\} = \left\{ r \in R \;\middle|\; \exists u \in T : \; ur = 0 \right\} = \bigcup_{u \in T} \operatorname{Ann}_R(u) \tag{2.4.a}$$

For example,

(i) if $0 \in T$, then we have $\ker \iota = R$

(ii) If R is a domain and $0 \notin T$, then we have $\ker \iota = 0$

(iii) In general if T contains no zero divisors, then $\ker \iota = 0$.

(iv) If $R = F \oplus F$ for a field F, and $T = \{(1,1),(0,1)\}$, then $\ker \iota = F \oplus 0$. Additionally, as we are inverting only two elements, which become the same in $T^{-1}R$, we obtain that ι is surjective. Hence:

$$T^{-1}R = {}^{F \oplus F}\big/_{F \oplus 0} \cong F.$$

(2) If R is a domain and $0 \notin T$, then the universal property of localization shows that there is a natural ring homomorphism $T^{-1}R \to \operatorname{Frac}(R)$ sending $\frac{r}{t}$ to $\frac{r}{t}$. This is injective. Additionally the identifications are the same in $T^{-1}R$ and in $\operatorname{Frac} R$ hence the above ring homomorphism is a ring embedding.

Hence, if R is a domain and $0 \notin T$, then it is easier to understand $T^{-1}R$ as the following subring of $\operatorname{Frac}(R)$, as opposed to a standalone ring:

$$T^{-1}R \cong \left\{ \frac{r}{t} \in \operatorname{Frac}(R) \;\middle|\; t \in T \right\} \subseteq \operatorname{Frac}(R)$$

(3) If $T = \{1, f, f^2, \dots\}$ for some $f \in R$, then

$$T^{-1}R \underset{\uparrow}{=} R_f \underset{\uparrow}{\cong} {}^{R[z]}\big/_{(fz-1)},$$

Notation for $T^{-1}R$ in this special case. Explained below.

Proof of the isomorphism $R_f \cong {}^{R[z]}\big/_{(fz-1)}$: by the universal property of localization yields a commuative diagram as follows, where the objects are rings and the arrows are ring homomorphisms:

$$\begin{array}{ccc} R & \xrightarrow{\iota} & R_f \\ & \searrow^{\psi} & \downarrow{\scriptstyle \phi:\ \frac{r}{1} \mapsto r} \\ & & {}^{R[z]}\big/_{(zf-1)} \end{array} \tag{2.4.b}$$

We show that ϕ is an isomorphism.

End of 10. class, on 22.11.2021.

ϕ is surjective: As all the arrows of the diagram are ring homomorphisms we obtain the following, where by abuse of notation we denote the residue classes of f and z also by f and z:

$$\phi\left(\frac{1}{f}\right) f = \phi\left(\frac{1}{f}\right)\psi(f) = \phi\left(\frac{1}{f}\right)\phi\left(\frac{f}{1}\right) = \phi\left(\frac{1}{1}\right) = 1 \underset{\uparrow}{=} zf. \tag{2.4.c}$$

in ${}^{R[z]}\big/_{(zf-1)}$

As f is a unit in $\phi\left(\frac{1}{f}\right)$, one can simplify equations with it. Hence, (2.4.c) implies that $\phi\left(\frac{1}{f}\right) = z$. As ${}^{R[z]}\big/_{(zf-1)}$ is generated by the elements of R and z, we obtain that ϕ is surjective.

ϕ is injective: We need to prove that $\ker\phi = 0$. As every element of R_f can be written as the product of an element of $\iota(R)$ and a unit, we see that if $\ker\phi$ was non-zero, then we would have a non-zero element in it that is also in $\iota(R)$. With other words, it is enough to show that $(\operatorname{im}\iota)\cap(\ker\phi) = 0$, or equivalently that $\ker\iota = \ker\psi$. Note that by (2.4.b), $\ker\iota \subseteq \ker\psi$ holds automatically, so we only have to show the opposite containment. For that consider $r \in \ker\psi$, that is, $r \in (zf-1)$. By definition this means that there exists a polynomial $\sum_{i=0}^{n} a_i z_i \in R[z]$ such that

$$r = \left(\sum_{i=0}^{n} a_i z^i\right)(zf-1) = -a_0 + fa_n z^{n+1} + \sum_{i=1}^{n}(fa_{i-1} - a_i)z^i$$

as elements of $R[z]$. Hence, we obtain

$$\begin{aligned} & r = -a_0 \\ & 0 = fa_n \\ \forall 1 \le i \le n: \qquad & a_i = fa_{i-1} \end{aligned}$$

This then implies that

$$0 = fa_n = f^2 a_{n-1} = \ldots = f^{n+1}a_0 = -f^{n+1}r$$

Hence, $r \in \ker\iota$, which concludes our proof that ϕ is an isomorphism.

Specific examples:

(i) If $R = F[x]$ and $f = x$, then $R_f = F[x]_x$ is often denoted by $F[x, x^{-1}]$, and as R is a domain it is equal to

$$\left\{ \frac{g}{x^n} \in F(x) \;\middle|\; n \in \mathbb{N} \right\}.$$

(ii) If $R = \mathbb{Z}$ and $f = p$ is a prime, then $R_f = \mathbb{Z}_p$ is equal to the following, again using that R is a domain:

$$\left\{ \frac{n}{p^i} \in \mathbb{Q} \;\middle|\; i \in \mathbb{N} \right\}.$$

(iii) If R is not a domain then things become trickier. For example consider $R = F[x,y]\big/(xy, y^2)$. Then $\operatorname{nil}(R) = (y)$, where by abuse of notation y denotes the residue class of y in R, and $\dim_k\big(\operatorname{nil}(R)\big) = 1$ as $\operatorname{Ann}_R(y) = (x,y)$.

1. If $f = x$, where we denote by x the residue class of x by abuse of notation, then $\operatorname{Ann}_R(x^n) = (y)$ for every $n > 0$. Hence, $\ker\iota = (y)$. Consider now the following commutative diagram, which is constructed using the universal property of localization applied to α, similarly to how the diagram (2.4.b) was constructed above:

$$\begin{array}{ccc} R & \xrightarrow{\ \iota\ } & R_x = R[z]\big/(xz-1) \\ {\scriptstyle y\mapsto 0}\downarrow & \searrow^{\alpha} & \downarrow{\scriptstyle \beta} \\ F[x] & \longrightarrow & k[x]_x = F[x,z]\big/(xz-1) \end{array}$$

As $\ker\alpha = \ker\iota = (y)$, and as every element of R_x is a product of a unit and of an element of $\operatorname{im}\iota$, one can prove as for ϕ above that β is an isomorphism. In particular, R_x is a domain.

2. If $f = x - 1$, then by point (1) above

$$\ker \iota = \bigcup_{i \geq 0} \mathrm{Ann}_R \left((x-1)^i \right).$$

We compute $\mathrm{Ann}_R \left((x-1)^i \right)$. So, take $h \in F[x,y]$ such that $h(x-1)^i \in (xy, y^2)$. Then, $y | h(x-1)^i$, which implies that $y|h$ as $x-1$ and y are relatively prime elements of $F[x,y]$. So, we may write $h = gy$, and hence $g(x-1)^i \in (x,y)$. As (x,y) is a prime ideal and $(x-1) \notin (x,y)$ we obtain that $g \in (x,y)$, and hence $h \in (xy, y^2)$. This shows that $\mathrm{Ann}_R \left((x-1)^i \right) = 0$.
As a consequence we obtain that ι is injective and hence, $R_{(x-1)}$ is not a domain, contrary to the case of $f = x$ above.
The key is that in the primary decomposition (explained later in Chapter 8) of R, one has a primary ideal the radical of which is (x,y). Hence, localization at $x \in (x,y)$ behaves differently than localization at $x - 1 \notin (x,y)$.

(4) If $p \subseteq R$ is a prime ideal, then for $T = R \setminus p$, $T^{-1}R$ is denoted by R_p. For example,

(i) If $R = F[x]$, and $p = (x)$, then R_p is the ring

$$F[x]_{(x)} = \left\{ \frac{f(x)}{g(x)} \in F(x) \;\middle|\; g(0) \neq 0 \right\}.$$

(ii) If $R = \mathbb{Z}$, and $p = (q)$ where $q \in \mathbb{Z}$ is a prime number, then R_p is the ring

$$\mathbb{Z}_{(q)} = \left\{ \frac{s}{t} \in \mathbb{Q} \;\middle|\; q \nmid t \right\}.$$

(iii) If $R = {}^{F[x,y]}\big/_{(xy)}$, and $p = (x)$, then a F-vector space basis of R is

$$1, x, y, x^2, y^2, x^3, y^3, \ldots.$$

Out of these basis elements, the powers of x are the ones contained in (x). So, T consists of those elements of R that have non-zero coefficients at one of the basis elements $1, y, y^2, \ldots$.
In particular, if $t \in T \setminus (y)$, then t has a non-zero coefficient at the basis-element 1 and hence $\mathrm{Ann}_R(t) = 0$. On the other side, if $t \in T \cap (y)$, then $\mathrm{Ann}_R(t) = (x)$. So, we obtain that $\ker \iota = (x)$ and that $\mathrm{im}\, \iota$ can be identified with the quotient $R = {}^{F[x,y]}\big/_{(xy)} \to k[y]$ obtained by sending $x \mapsto 0$. So, we obtain a commutative diagram as follows

$$\begin{array}{ccc} R & \longrightarrow & R_p \\ {\scriptstyle x \mapsto 0}\downarrow & \searrow^{\alpha} & \downarrow{\scriptstyle \beta} \\ F[y] & \longrightarrow & F(y) \end{array}$$

As above, we can show that β is an isomorphism. Intuitively, when we localize at (x), we remove the variable x completely, and we add the inverses of all the remaining non-zero elements.

(5) If $S \subseteq R$ is a ring extension, and $p \subseteq S$ is a prime ideal, then R_p denotes $T^{-1}R$ for $T = S \setminus p$. For a specific example, let us take $S = F[x^2] \subseteq F[x] = R$ and two choices of prime ideals $p \subseteq S$.

(i) If $p = (x^2)$, then $T = F[x^2] \setminus (x^2)$, and hence

$$F[x]_p = \left\{ \frac{f(x)}{\sum_{i=0}^n a_i x^{2i}} \;\middle|\; a_0 \neq 0,\ f(x) \in F[x] \right\} \tag{2.4.d}$$

Let us compare this to the other localization

$$F[x]_{(x)} = \left\{ \frac{f(x)}{\sum_{i=0}^n a_i x^{i}} \;\middle|\; a_0 \neq 0,\ f(x) \in F[x] \right\} \tag{2.4.e}$$

By the above two descriptions $F[x]_p \subseteq F[x]_{(x)}$. To understand the difference, we need to understand when we can write $\frac{f}{g} \in F(x)$ such that $x \nmid g$ as $\frac{h(x)}{\sum_{i=0}^n a_i x^{2i}}$ such that $a_0 \neq 0$. This is equivalent to the equation

$$gh = f\left(\sum_{i=0}^n a_i x^{2i}\right).$$

This is always doable by setting $h(x) = f(x)g(-x)$, as $g(x)g(-x)$ is of the form $\sum_{i=0}^n a_i x^{2i}$. Indeed if $\operatorname{char} F = 2$, then $g(x)g(-x) = g(x)^2$, which is of the stated form, and $\operatorname{char} F \neq 2$, then $s(x) = g(x)g(-x)$ satisfies the equality $s(x) = s(-x)$ and hence all its odd degree terms are zero.

To sum up, we obtain that the rings (2.4.d) and (2.4.e) agree (as subrings of $F(x)$).

(ii) If $p = (x^2 - c)$ for some $c \neq 0, 1$ and $F = \overline{F}$ is algebraically closed, then we will show soon that $F[x]_p$ has two maximal ideals $(x - \sqrt{c})$ and $(x + \sqrt{c})$. We will also learn soon that on the other hand the localization at any prime ideal of $F[x]$ is a local ring. So, in particular, contrary to the case of $p = (x^2)$, here the localization is not isomorphic to the localization of any prime ideal of $F[x]$.

Finally we note that practically all the above localizations and their ordinary or strange behaviors have geometric meanings. You can learn more about this in the algebraic geometry courses at EPFL.

Definition 7.2.5. Let M be a module over a ring R, and T a multiplicatively closed set. Then we define $T^{-1}M$ just as we defined $T^{-1}R$ in Theorem 7.2.2. That is, it is the set of formal fractions $\frac{m}{t}$ $(m \in M, t \in T)$ subject to the equivalence relation $\equiv$ given by

$$\frac{m}{t} \equiv \frac{m'}{t'} \iff \exists u \in T \ :\ u(t'm - tm') = 0.$$

We leave it as a homework to show that $T^{-1}M$ is a $T^{-1}R$ module where operations then are defined as follows for every $\frac{m}{t}, \frac{m'}{t'} \in T^{-1}M$ and $\frac{r}{t} \in T^{-1}R$ (one has to show that these operations are well defined):

- $\frac{m}{t} + \frac{m'}{t'} = \frac{t'm + tm'}{tt'}$ and
- $\frac{r}{t}\frac{m}{t'} = \frac{rm}{tt'}$.

Note that via the natural map $R \to T^{-1}R$, the $T^{-1}R$ module $T^{-1}M$ also comes with a R-module structure.

We will prove on the exercise sheet that $T^{-1}M \cong M \otimes_R T^{-1}R$.

Remark 7.2.6. We observe that for every $t \in T$ the multiplication map is an isomorphism on $T^{-1}M$. The module $T^{-1}M$ comes with a natural R-module map $i_{M,T} \colon M \to T^{-1}M$ defined by the formula $m \mapsto \frac{m}{1}$. This map is universal for morphisms into modules satisfying the property that multiplication by elements of T are isomorphisms. More precisely, for every homomorphism $\phi \colon M \to N$ where N satisfies the above property there exists a unique morphism $\overline{\phi} \colon T^{-1}M \to N$ such that $\phi = \overline{\phi} \circ i_{M,T}$.

Example 7.2.7. If M is a module over a domain R, then by definition $M_{\operatorname{Frac} R} = (R \setminus 0)^{-1}M$ is generated as a $\operatorname{Frac}(R)$ module by the R-module generators of M. Hence, by definition $M_{\operatorname{Frac} R} = 0$ if and only if the natural map $\xi : M \to M_{\operatorname{Frac} R}$ is zero, where $\xi(m) = \frac{m}{1}$. However, by the same argument as for rings in (2.4.a), one can show that $\ker \xi = \bigcup_{t \in R \setminus \{0\}} \operatorname{Ann}_M(t)$. So, we obtain that $M_{\operatorname{Frac} R} = 0$ if and only if each element of M is annihilated by some element of $R \setminus \{0\}$, or with other words if and only if each element of M is torsion.

7.3 LOCALIZATION AND IDEALS

Definition 7.3.1. If $I \subseteq S$ is an ideal and $\phi : S \to R$ is a ring homomorphism, then the extension of I via ϕ is defined as $I^e := R \cdot \phi(I)$.

If $J \subseteq R$ is an ideal and $\phi : S \to R$ is a ring homomorphism, then the contraction of J via ϕ is defined as $J^c := \phi^{-1}(J)$.

Remark 7.3.2. Obviously $I^{ec} \supseteq I$ and $J^{ce} \subseteq J$.

Remark 7.3.3. In the situation of Definition 7.3.1, if $I = (f_1, \ldots, f_r)$, then $I^e = (\phi(f_1), \ldots, \phi(f_r))$. In the case of contraction one cannot write such an easy formula. So, one could guess at first sight that extensions behave better than contractions. For the point of view of Commutative algebra, the situation is in fact the opposite contraction preserves primeness and maximality of ideals, see Lemma 7.3.6 and Corollary 7.3.8. However as shown by the following example, extension does not preserve these properties.

Example 7.3.4. Consider $S = k[x^2] \subseteq k[x] = R$.

(1) For $I = (x^2) = k[x^2]x^2 \subseteq k[x^2]$, $I^e = k[x]x^2 \subseteq k[x]$ is neither a maximal or a prime ideal.

(2) For $J = (x) \subseteq k[x]$, $I^c = (x^2)$.

Lemma 7.3.5. *If $S \subseteq R$ is an integral extension, and J is an ideal in R, then $S/J^c \to R/J$ is an integral extension too.*

Proof. J^c is exactly the kernel of the composition $S \to R \to R/J$. Hence, $\phi : S/J^c \to R/J$ is an injection. Furthermore, ϕ is an integral extension, because for every $[r] \in R/J$, we have a monic

$$r^n + \sum_{i=0}^{n-1} a_i r^i = 0$$

in R ($a_i \in S$). This induces a similar relation in R/I:

$$[r^n] + \sum_{i=0}^{n-1} [a_i][r]^i = 0,$$

where $[a_i] \in S/J^c$. □

Lemma 7.3.6. *If $\phi : S \to R$ is a ring homomorphism and $J \subseteq R$ is a prime ideal, then so is J^c.*

Proof. Choose $a, b \in R$ such that $ab \in J^c$. Then $\phi(ab) = \phi(a)\phi(b) \in J$, which implies that $\phi(a)$ or $\phi(b) \in J$, which then in turn implies that $a \in J^c$ or $b \in J^c$. □

Remark 7.3.7. If $I \subset S$ is a prime ideal then I^e need not to be a prime ideal of R. For example let $\mathbb{Z} \to \mathbb{Z}[i]$ be the embedding of the integers into the Gaussian integers. The prime number 2 is no longer prime in the ring of Gaussian integers. In fact $2 = (1+i)(1-i)$ and neither $(1+i)$ nor $(1-i)$ is a unit in $\mathbb{Z}[i]$, hence the ideal $(2)^e$ is not prime, since neither $(1+i)$ nor $(1-i)$ is in $(2)^e$.

Corollary 7.3.8. *Let $S \subseteq R$ be an integral extension, and $p \subseteq R$ a prime ideal. Then p is maximal if and only if so is p^c.*

Proof. According to Lemma 7.3.5, $S/p^c \subseteq R/p$ is an integral extension of domains. Then we apply Lemma 6.3.1. □

Proposition 7.3.9. *Let $T \subseteq R$ be a multiplicatively closed set of a ring, and consider the structure homomorphism $\iota : R \to T^{-1}R$.*

(1) For any ideal $J \subseteq T^{-1}R$, $J^{ce} = J$. In particular, every ideal of $T^{-1}R$ is extended.

(2) For any ideal $I \subseteq R$, $I^{ec} = \bigcup_{u \in T}(I : u)$, where $(I : u) := \left\{ r \in R \;\middle|\; ur \in I \right\}$.

(3) For an ideal $I \subseteq R$, $I^e = (1)$ if and only if $T \cap I \neq \emptyset$.

(4) If $p \subseteq R$ is a prime ideal such that $T \cap p = \emptyset$, then $p^{ec} = p$. That is, there is a one-to-one correspondence (via extension and contraction) between prime ideals of R avoiding T and prime ideals of $T^{-1}R$.

Proof. (1) The inclusion $J^{ce} \subseteq J$ is a consequence of the definition. We prove that $J \subseteq J^{ce}$ as follows. Take $\frac{r}{t} \in J$. Then $\frac{r}{1} = \frac{t}{1} \cdot \frac{r}{t} \in J$, and hence $r \in J^c$. However then $\frac{r}{t} = \frac{1}{t}\frac{r}{1} \in J^{ce}$.

(2) By definition

$$I^e = \left\{ \sum_{\text{finite}} \frac{r_i}{t_i}\frac{s_i}{1} \;\middle|\; r_i \in R, t_i \in T, s_i \in I \right\}.$$

Since we may write

$$\sum_i \frac{r_i}{t_i}\frac{s_i}{1} = \frac{\sum_i s_i r_i \prod_{j \neq i} t_j}{\prod_i t_i},$$

we may simplify

$$I^e = \left\{ \frac{s}{t} \middle| t \in T, s \in I \right\}.$$

Then, $r \in I^{ec}$ if and only if $\frac{r}{1} = \frac{s}{t}$ for some $t \in T$ and $s \in I$, if and only if $(rt - s)u = 0$ for some $u \in T$.

Now, in this situation $rtu = su \in I$ and $tu \in T$, so $r \in (I : tu)$.

For the other direction, if $r \in (I : t)$ for some $t \in T$, then $rt = s \in I$. In particular, $\frac{r}{1} = \frac{s}{t}$.

(3) By point (1), $I^e = (1) \Leftrightarrow I^e = (1)$ & $I^{ece} = (1) \Leftrightarrow I^{ec} = (1) \Leftrightarrow 1 \in (I : t)$ for some $t \in T$ $\Leftrightarrow T \cap I \neq \emptyset$.

(4) Choose $t \in T$. We have to show that $(p : t) = p$. Obviously $(p : t) \supseteq p$. For the other containment, let $r \in (p : t)$, that is, $rt \in p$. Then, since p is prime, and $t \notin p$ by assumption, $r \in p$.

We also have to show that p^e is a prime ideal. So, let $\frac{a}{t}, \frac{b}{s} \in T^{-1}R$, such that $\frac{a}{t}\frac{b}{s} \in p^e$. However, then $\frac{ab}{1} \in p^e$ too, and then $ab \in p^{ec} = p$. This implies that $a \in p$ or $b \in p$, from where we obtain that $\frac{a}{t} \in p^e$ or $\frac{b}{s} \in p^e$.

□

Definition 7.3.10. A ring is called local if it has a unique maximal ideal.

Corollary 7.3.11. *If $p \subseteq R$ is a prime ideal, then R_p is a local ring.*

Proof. $m := pR_p = p^e$ is a (proper) prime ideal according to (4) of Proposition 7.3.9, and since all the other elements of R_p are invertible (since they are of the form $\frac{r}{t}$ for $r, t \in R \setminus p$), m is a unique maximal ideal (as it contains all the elements that a maximal ideal can contain, i.e., the non invertible ones). □

Example 7.3.12. If $R = k[x, y]$ and $p = (x)$, then $R_p = k[x, y]_{(x)}$ is a local ring, with maximal ideal being $R_p x \subseteq R_p$. In fact, this is the only non-zero prime ideal of R_p. To see this, we use point (4) of Proposition 7.3.9. That is, if $q \subsetneq R_p x$ is another prime ideal of R_p, then it is the extension of a prime ideal $q \subsetneq p$. However, such q is necessarily zero by the following short argument: if $0 \neq f \in q$, then as $q \subseteq (x)$, we have $\frac{f}{x} \in R$. However, then using that q is prime, and that $q \neq (x)$ and hence $x \notin q$, we obtain that $\frac{f}{x} \in q$. Iterating this, we obtain that $\frac{f}{x^i} \in q$ for every $i \geq 0$, which is impossible.

End of 11. class, on 29.11.2021.

7.4 Localization and integral dependence

Proposition 7.4.1. *If $S \subseteq R$ is an integral ring extension and $T \subseteq S$ is a multiplicatively closed set, then $T^{-1}S \to T^{-1}R$ is also an integral extension.*

Proof. The map $T^{-1}S \to T^{-1}R$ is defined by sending $\frac{s}{t} \to \frac{s}{t}$.To show that $T^{-1}S \to T^{-1}R$ is injective, we have to show that $\frac{s}{t}$ is zero in $T^{-1}R$ if and only if it is zero in $T^{-1}S$. However, in both cases this is equivalent to an existence of $u \in T$, such that $us = 0$.
To get the integrality, choose $\frac{r}{t} \in T^{-1}R$. Then we have a monic relation

$$r^n + \sum_{i=0}^{n-1} a_i r^i = 0, \ a_i \in S.$$

Dividing this by t^n yields a monic relation for $\frac{r}{t}$ over

$$\left(\frac{r}{t}\right)^n + \sum_{i=0}^{n-1} \frac{a_i}{t^{n-i}} \left(\frac{r}{t}\right)^i = 0$$

□

Proposition 7.4.2 (Going-Up Theorem)**.** *Let $S \to R$ be an integral extension.*

(1) If $p \subseteq S$ is a prime ideal, then there is a prime ideal $q \subseteq R$, such that $q \cap S = p$.
Addendum: if there are prime ideal $p' \subsetneq p \subseteq S$ and $q' \subseteq R$, such that $q' \cap S = p'$, then we may choose q such that $q' \subseteq q$.

(2) Let $q \subsetneq q' \subseteq R$ be prime ideals. Then $q \cap S \neq q' \cap S$.

Proof. (1) Choose $p \subseteq S$ prime. Then

(i) $S_p \to R_p$ is an integral extension according to Proposition 7.4.1.
(ii) S_p is a local ring according to Corollary 7.3.11, with maximal ideal $m := pS_p$.

Choose now, any maximal ideal n of R_p. According to Corollary 7.3.8, $n \cap S_p$ is a maximal ideal, hence $n \cap S_p$ is necessarily m. Define q then to be the contraction of n along $R \to R_p$. We have the following commutative diagram:

$$\begin{array}{ccc} S & \xhookrightarrow{\iota} & R \\ \downarrow{\scriptstyle j_S} & & \downarrow{\scriptstyle j_R} \\ S_p & \xhookrightarrow{\iota_p} & R_p \end{array} \tag{4.2.a}$$

Using the notations of the diagram:

$$q \cap S = \iota^{-1} q = \iota^{-1} j_R^{-1} n = j_S^{-1} \iota_p^{-1} n = j_S^{-1} m = p,$$

where we used point (4) of Proposition 7.3.9 in the last step.

For the addendum, just note that by point (3) and (4) of Proposition 7.3.9, $q'R_p$ is a proper ideal, such that $j_R^{-1}(q'R_p) = q'$ (we are using that $q' \cap S = p' \subseteq p$ and hence $q' \cap (S \setminus p) = \emptyset$). Hence, we may pick n to contain $q'R_p$, and hence, $q := j_R^{-1}(n)$ contains q'.

(2) Assume the contrary, that is, $p := q \cap S = q' \cap S$. Perform then the same localization construction as above, pictured in (4.2.a). As above, $qR_p \subsetneq q'R_p$ are proper prime ideals, as they avoid $S \setminus p$, and hence their contraction in R is q and q' respectively. Also, their contraction in S_p are prime ideals that contract to p. Hence, these two contractions are equal:

$$pS_p = S_p \cap q = S_p \cap q'.$$

Hence, by Corollary 7.3.8, using that pS_p is maximal, both qR_p and $q'R_p$ are maximal, which is a contradiction.

□

Example 7.4.3. Using localization, one can give many examples of ring extensions $S \subseteq R$ that are not integral extensions, and hence Proposition 7.4.2 fails for them. For example:

(1) If $S = F[x] \subseteq F\left[x, x^{-1}\right] = R$, then by point (4) of Proposition 7.3.9 tells us that all prime ideals of S can be lifted to prime ideals of R, except (x), as that is the only prime ideal intersecting the multiplicatively closed set $T = \{1, x, x^2, \dots\}$.

(2) If S is a UFD, and $R = \operatorname{Frac}(S)$, then by Example 6.2.8 we see that $S \subseteq R$ is as not integral as possible. Also, as R has a single prime ideal $(0) \subseteq R$, only $(0) \subseteq S$ lifts to R, and if S has other prime ideals, then they do not lift to R. For example if $S = \mathbb{Z}$, then (p) does not lift to R for every prime $p \in \mathbb{Z}$.

Corollary 7.4.4. *Let $S \subset R$ be an integral extension. Then,* $\dim S = \dim R$.

Proof. (1) For every chain $p_0 \subsetneq \cdots \subsetneq p_r \subseteq S$ of prime ideals, we have a chain $q_0 \subsetneq \cdots \subsetneq q_r \subseteq R$ of prime ideals, such that $q_i^c = p_i$, by applying inductively point (1) of Proposition 7.4.2. This shows $\dim R \geq \dim S$.

(2) For every chain $q_0 \subsetneq \cdots \subsetneq q_r \subseteq R$ of prime ideals, we obtain a chain $p_0 \subsetneq \cdots \subsetneq p_r \subseteq S$, by setting $p_i := q_i^c$ according to (2) of Proposition 7.4.2. This shows $\dim S \geq \dim R$.

□

Corollary 7.4.5. *Let F be a field. Then* $\dim F[x_1, \dots, x_n] = n$.

Proof. We prove the statement by induction on n. For $n = 0$ it holds because F is a field. For $n = 1$ we have already shown it in point (2) of Example 6.1.2, as $F[x_1]$ is a PID. So, we only have to show the induction step.

We may easily exhibit chains of length n:

$$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \dots, x_n).$$

Hence, $\dim F[x_1, \dots, x_n] \geq n$, we only have to show the opposite inequality. That is, we have to show that for every chain of prime ideals

$$p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_r \subseteq F[x_1, \dots, x_n] \tag{4.5.b}$$

$r \leq n$. First, we may assume that $p_0 = 0$. Second, choose any $0 \neq r \in p_1$. Then, by the prime property there must be a prime factor s of r contained in p_1. However, then we may replace p_1 by (s), that is, we may assume that p_1 is principal. By reindexing the variables, we may

assume that $s \notin F[x_1, \dots, x_{n-1}]$, and hence the residue classes $\overline{x}_1, \dots, \overline{x}_{n-1}$ of $x_1, \dots, x_{n-1}$ are algebraically independent in $R := F[x_1, \dots, x_n]\Big/(s)$.

By Noether normalization there is $F[t_1, \dots, t_l] \cong S \subseteq R$, making the above extension integral. Furthermore, by considering the we see that

$$l = \operatorname{trdeg}_F \operatorname{Frac}\left(F[x_1, \dots, x_n]\Big/(s)\right) = \operatorname{trdeg}_F \underbrace{\left(F(\overline{x}_1, \dots, \overline{x}_{n-1})[x_n]\Big/(s)\right)}_{\uparrow} = n - 1.$$

$s \in F[x_1, \dots, x_n] = F[x_1, \dots, x_{n-1}][x_n]$ is an irreducible element, and it is not a contsant polynomial in $x_n \implies$ by the Gauss-lemma $s \in F[x_1, \dots, x_{n-1}][x_n]$ is a primitive polynomial that is irreducible as a polynomial in $F(x_1, \dots, x_{n-1})[x_n] \implies$ the above ring is a field $\implies$ as it is generated by the elements of R as a field, it is in fact the fraction field of R

Hence, by induction we know that $\dim S = n - 1$. Then, Corollary 7.4.4 implies, that $\dim R = n - 1$ too. However, (4.5.b) yields a chain of length $r - 1$ in R, so $r - 1 \leq n - 1$, which concludes our proof. □

Proof of Theorem 6.1.12. Let $S := F[x_1, \dots, x_r] =: S \subseteq R$ be the Noether normalization. Then $r = \operatorname{trdeg} \operatorname{Frac}(S) = \operatorname{trdeg} \operatorname{Frac}(R)$, and $\dim S = \dim R$ by Corollary 7.4.4. So, it is enough to prove that $\dim S = r$, which was shown in Corollary 7.4.5 □

Remark 7.4.6. It is important in Theorem 6.1.12 that R is the quotient of a polynomial ring. Indeed, we have seen in an exercise that the statement of the theorem fails for $F[\![x]\!]$ in general.

Chapter 8

Nullstellensatz and primary decomposition

8.1 Weak Nullstellensatz

Even to state the weak Nullstellensatz we need to fix some basic set of examples of prime and maximal ideals.

Example 8.1.1. Let F be an *algebraically* closed field. Then:

(1) The only maximal ideals of $F[x]$ are of the form $(x - c)$ for $c \in F$.

(2) Fix $c_1, \dots, c_n \in F$. The multiplication of polynomials is defined so that the map $\phi :: F[x_1, \dots, x_n] \to F$ defined by $\phi(f(x_1, \dots, x_n)) = f(c_1, \dots, c_n)$ is a homomorphism. Additionally this homomorphism is surjective. *We claim that* $\ker \phi = (x_1 - c_1, \dots, x_n - c_n)$. Indeed, as $x_i - c_i \in \ker \phi$ the containment $\ker \phi \supseteq (x_1 - c_1, \dots, x_n - c_n)$ is immediate. For the reverse containment consider the composition

$$F \hookrightarrow F[x_1, \dots, x_n] \Big/ (x_1 - c_1, \dots, x_n - c_n) \xrightarrow[\widetilde{\phi}]{} F \,,$$

where $\widetilde{\phi}$ is induced by ϕ, and hence its kernel is induced by $\ker \phi$. In particular we obtain that $\phi = (x_1 - c_1, \dots, x_n - c_n)$ if and only if $\widetilde{\phi}$ is an isomorphism. For that, it is enough to show that the left horizontal map is surjective, or with other words that each class of $F[x_1, \dots, x_n] \Big/ (x_1 - c_1, \dots, x_n - c_n)$ is represented by a constant, which is immediate, using the relations $[x_i] = [c_i]$.

Hence, we obtain that $(x_1 - c_1, \dots, x_n - c_n)$ is a maximal ideal.

From now, our goal is to prove the following statement, also referred to as Hilbert's Nullstellensatz (or rather this will be the first version and we will generalize it in different ways.

Theorem 8.1.2 (Weak Nullstellensatz)**.** *If F is an algebraically closed field then every maximal ideal of $F[x_1, \dots, x_n]$ is of the form $m_{c_1,\dots,c_n} := (x_1 - c_1, \dots, x_n - c_n)$ for $c_1, \dots, c_n \in F$.*

Proof. Let $m \subseteq F[x_1, \dots, x_n] =: R$ be a maximal ideal. Then $k := F[x_1, \dots, x_n] \Big/ m$ is a field which is a quotient of a polynomial ring over the field F. Moreover, k contains F because of the (injective) ring homomorphism $F \to F[x_1, \dots, x_n] \Big/ m$. Then $\operatorname{trdeg}_F k = \dim k = 0$ by Theorem 6.1.12; thus, k is an algebraic extension of F. But F is algebraically closed, so $k \supset F$ is the trivial extension. Let $c_i := \overline{x_i} \in k = F$. Then $m_{c_1,\dots,c_n} \subseteq \ker(F[x_1, \dots, x_n] \to k) = m$. Since $m_{c_1,\dots,c_n}$ is maximal and m is a proper ideal, we obtain $m_{c_1,\dots,c_n} = m$. □

Example 8.1.3. Theorem 8.1.2 fails for F not algebraically closed. For example if $F = \mathbb{R}$, then (x^2+1) is a maximal ideal of $\mathbb{R}[x]$ not of the form as in Theorem 8.1.2. We can also see that the main step of the proof of Theorem 8.1.2 fails in this case, that is to prove that $F \to {}^{F[x]}\!/_{m}$ is an isomorphism. Indeed, ${}^{F[x]}\!/_{(x^2+1)} \cong \mathbb{C}$ (by sending the residue class of X to i) and so $F \to {}^{F[x]}\!/_{(x^2+1)}$ is not an isomorphism.

8.2 NILPOTENT RADICAL, RADICALS

Material very similar of what we learned in "Anneaux et corps"

Definition 8.2.1. Let R be a ring. Let $I \subset R$ be an ideal. The radical ideal $\sqrt{I}$ of I is

$$\sqrt{I} := \{r \in R \mid \exists n \in \mathbb{N}_{>0} \ : \ r^n \in I\}.$$

I is said to be a radical ideal if $\sqrt{I} = I$.

Lemma 8.2.2. *Let R be a ring. Let $I \subset R$ be an ideal. The radical ideal $\sqrt{I}$ is indeed an ideal.*

Proof. Homework. □

When I is the ideal generated by $0 \in R$, we have a special ideal.

Definition 8.2.3. Let R be a ring. Then the nilpotent radical is

$$\mathrm{nil}(R) := \sqrt{(0)} = \{r \in R \mid \exists n \in \mathbb{N}_{>0} \ : \ r^n = 0\}$$

Lemma 8.2.2 implies that $\mathrm{nil}(R)$ is an ideal as well.

Example 8.2.4. (1) $R = F[x]/(x^2) \Rightarrow \mathrm{nil}\, R = (\overline{x})$, and has dimension 1 as F-vector space.

(2) $R = F[x,y]/(x^2) \Rightarrow \mathrm{nil}\, R = (\overline{x})$, and has infinite dimension as F-vector space.

(3) $R = F[x,y]/(xy, x^2) \Rightarrow \mathrm{nil}\, R = (\overline{x})$, and has dimension 1 as F-vector space.

Material very similar of what we learned in "Anneaux et corps"

Proposition 8.2.5. *Let R be a ring.*

(1) $\mathrm{nil}(R) = \bigcap_{\mathfrak{p} \subseteq R \text{ prime}} \mathfrak{p}$.

(2) $\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p} \subseteq R \text{ prime}} \mathfrak{p}$.

Proof. (1) $\mathrm{nil}(R) \subseteq \bigcap_{\mathfrak{p} \subseteq R \text{ prime}} \mathfrak{p}$: fix a prime ideal $\mathfrak{p}$, and $r \in R$ such that $r^n = 0$ for some integer $n > 0$. Then $\mathfrak{p} \ni r^n = (r^{n-1})r$, so by the prime property either $r^{n-1} \in \mathfrak{p}$ or $r \in \mathfrak{p}$. In the latter case, we are done, while in the former case we proceed by induction on n.
$\mathrm{nil}(R) \supseteq \bigcap_{\mathfrak{p} \subseteq R \text{ prime}} \mathfrak{p}$: by contradiction, assume that there is a non nilpotent $r \in R$, which is contained in every prime ideal $\mathfrak{p}$. Consider then the localization at r, $R \to R_r$. Since r is not nilpotent, $R_r \neq 0$ ($\frac{1}{1}$ is not zero in R_r). Hence, it contains a

maximal ideal $\mathfrak{m}$. In particular, $\mathfrak{m}$ is prime; thus the contraction $\mathfrak{m}^c \subseteq R$ is a prime ideal and $r \notin \mathfrak{m}^c$, by (4) of Proposition 7.3.9. This gives the desired contradiction.
(2) It suffices to note that $\sqrt{I} = \pi^{-1}(\mathrm{nil}(R/I))$, where $\pi\colon R \to R/I$ is the quotient map. At which point the conclusion follows from (1), remembering that there is a 1-1 correspondence between the prime ideals of R/I and the prime ideals of R which contain I. □

8.3 NULLSTELLENSATZ

Within this section, we fix once and for all an algebraically closed field F .

End of 12. class, on 06.12.2021.

Definition 8.3.1. An *algebraic set* is a subset of F^n of the form

$$V(f_1, \dots, f_r) := \{\ (c_1, \dots, c_n) \in F^n \mid \forall j :\ f_j(c_1, \dots, c_n) = 0\ \},$$

for some finitely many $f_1, \dots, f_r \in F[x_1, \dots, x_n]$.

Notation 8.3.2. For an ideal $I \subseteq F[x_1, \dots, x_n]$ we define

$$V(I) := \{\ (c_1, \dots, c_n) \in F^n \mid \forall f \in I :\ f(c_1, \dots, c_n) = 0\ \}. \tag{3.2.a}$$

We note that for any choice of $f_1, \dots, f_r \in F[x_1, \dots x_n]$, we have $V(f_1, \dots, f_r) = V((f_1, \dots, f_r))$. Since $F[x_1, \dots, x_n]$ is Noetherian by the Hilbert Basis Theorem (Theorem 3.3.1), every ideal $I \subset F[x_1, \dots, x_n]$ is finitely generated. Hence, the subsets of F^n of the form $V(I)$ are exactly the algebraic sets.

Proposition 8.3.3. *Let I, J be ideals of $F[x_1, \dots, x_n]$. Then,*

(1) $V(F[x_1, \dots, x_n]) = \emptyset$, $V((0)) = F^n$.

(2) If $I \subseteq J$, *then* $V(I) \supseteq V(J)$.

(3) $V(I \cap J) = V(IJ) = V(I) \cup V(J)$, *where* $IJ = (\ ab \in F[x_1, \dots, x_n] \mid a \in I, b \in J\ )$ *is the ideals generated by the products.*

(4) $V(I + J) = V(I) \cap V(J)$, *where* $I + J = \{\ a + b \in F[x_1, \dots, x_n] \mid a \in I, b \in J\ \}$ *is an ideal of* $F[x_1, \dots, x_n]$.

Proof. This will be an exercise on the exercise sheet. □

Corollary 8.3.4. *If $I \subsetneq F[x_1, \dots, x_n]$ is a proper ideal, then $V(I) \neq \emptyset$.*

Proof. Since I is a proper ideal, it is contained in a maximal ideal $I \subseteq m \subsetneq F[x_1, \dots, x_n]$. However, according to Theorem 8.1.2, $m = (x_1 - c_1, \dots, x_n - c_n)$ for some $c_i \in F$. Hence $(c_1, \dots, c_n) \in V(m) \subseteq V(I)$, by the previous proposition. □

Example 8.3.5. The fact that F is algebraically closed is of fundamental importance for Corollary 8.3.4 to hold. In fact, consider $I = (x^2 + 1) \subset \mathbb{R}[x]$. Then $V(I) = \emptyset$. The issue here is that when F is not algebraically closed, then not all the maximal ideals of $F[x_1, \dots, x_n]$ are of the form $(x_1 - c_1, \dots, x_n - c_n)$.

Algebraic sets are the main objects of algebraic geometry. It turns out that not only ideals define algebraic sets, but also algebraic sets define ideals.

Definition 8.3.6. Let V be an algebraic set in F^n. Then

$$I(V) := \left\{ f \in F[x_1, \dots, x_n] \;\middle|\; \forall (c_1, \dots, c_n) \in V : f(c_1, \dots, c_n) = 0 \right\}.$$

Remark 8.3.7. Let V be an algebraic set in F^n. Then $V(I(V)) = V$. Indeed, $V \subseteq V(I(V))$ by definition of $I(V)$. Moreover, if we write $V = V(f_1, \dots, f_r)$ for some $f_1, \dots, f_r \in k[x_1, \dots, x_n]$, then $f_1, \dots, f_r \in I(V)$, so that $V(I(V)) \subseteq V(f_1, \dots, f_r) = V$.

Additionally, it also follows immediately from the definitions that $I \subseteq I(V(I))$.

Example 8.3.8. It may happen that $I \subsetneq I(V(I))$.

(1) In F, $V(x) = \{0\} = V(x^2)$. Hence, $I(V(x^2)) = (x)$.

(2) Let V be the algebraic set in F^3 defined by $I = (x_1^2 + x_2x_3, x_2)$. That is, $V = V(I)$. Let us notice that $I = (x_1^2, x_2)$. Then,

$$(c_1, c_2, c_3) \in V \iff c_1^2 + c_2c_3 = 0,\ c_2 = 0 \iff c_2 = 0,\ c_1^2 = 0 \iff c_1 = c_2 = 0.$$

Hence $I(V) = (x_1, x_2) = \sqrt{(x_1^2, x_2)} \neq (x_1^2, x_2) = (x_1^2 + x_2x_3, x_2)$.

So, these examples shows that the natural guess that $I(V(I)) = I$ is false. However, it turns out that there is still a surprisingly nice answer.

Theorem 8.3.9. NULLSTELLENSATZ *If $I \subseteq F[x_1, \dots, x_n]$, then $I(V(I)) = \sqrt{I}$.*

Proof. $\boxed{\sqrt{I} \subseteq I(V(I)):}$ if $f^n \in I$, then by definition $0 = f^n(c_1, \dots, c_n) = \big(f(c_1, \dots, c_n)\big)^n$ for every $(c_1, \dots, c_n) \in V(I)$. Thus, $f(c_1, \dots, c_n) = 0$ for every $(c_1, \dots, c_n) \in V(I)$, which means that $f \in I(V(I))$.

$\boxed{\sqrt{I} \supseteq I(V(I)):}$ Set $R := F[x_1, \dots, x_n] \big/ I$ and fix $g \in I(V(I))$. Let $\overline{g}$ be the residue class of g in R. We want to show that $g \in \sqrt{I}$ or equivalently that $\overline{g} \in \operatorname{nil}(R)$. Note that the latter is equivalent to the localization $R_{\overline{g}}$ being 0. Indeed, $R_{\overline{g}} = 0$ if and only if the multiplicative identity element $\frac{1}{1} \in R_{\overline{g}}$ is zero if and only if $g^s = g^s \cdot 1 = 0$ for some $s > 0$, where the last equivalence is explained in point (1) of Example 7.2.4.

To sum up, by the previous paragraph we have to show that $R_{\overline{g}} = 0$. By point (3) of Example 7.2.4 this is equivalent to showing that $R[x_{n+1}] \big/ (x_{n+1}\overline{g} - 1) = 0$. However, by the correspondence theorem (Proposition 2.2.12), we have

$$R[x_{n+1}] \big/ (x_{n+1}\overline{g} - 1) \cong F[x_1, \dots, x_{n+1}] \big/ J \qquad \text{for} \qquad J = (f_1, \dots, f_r, x_{n+1}g - 1).$$

Hence, it is enough to show that $J = (1)$, for which by Corollary 8.3.4 it is enough to show that $V(J) = \emptyset$. For that assume the contrary and take $(c_1, \dots, c_{n+1}) \in V(J)$. Then, the following computation yields a contradiction:

$$0 \underset{\uparrow}{=} \big(x_{n+1}g - 1\big)(c_1, \dots, c_{n+1}) = c_{n+1}g(c_1, \dots, c_n) - 1 \underset{\uparrow}{=} c_{n+1}0 - 1 = -1$$

$\boxed{(c_1, \dots, c_{n+1}) \in V(J)}$ $\qquad$ $\boxed{(c_1, \dots, c_{n+1}) \in V(J) \implies (c_1, \dots, c_n) \in V(I)}$

□

Remark 8.3.10. Putting together Remark 8.3.7 and Theorem 8.3.9 we obtain that there is a 1-1 correspondence

$$\boxed{\text{algebraic subsets } V \subseteq F^n} \longleftrightarrow \boxed{\text{radical ideals } I = \sqrt{I} \subset F[x_1, \dots, x_n]}.$$

The $\to$ direction is given by associating to V the ideal $I(V)$, while the $\leftarrow$ direction is given by associating to a radical ideal I the algebraic subset $V(I)$.

Additionally this 1-1 correspondence reverses inclusion.

8.4 GEOMETRIC PRIMARY DECOMPOSITION OF RADICAL IDEALS

One may wonder that in a Noetherian setting, the intersections that appear in Proposition 8.2.5 could in fact be reduced to finite intersections, thus yielding a very general prime decomposition type theorem for ideals. In this section, we shall treat the case of rings that are quotients of polynomial rings over algebraically closed fields. So, again, within this subsection, we fix an algebraically closed field F.

Definition 8.4.1. Let V be an algebraic subset of F^n and let $I(V) \subseteq F[x_1, \ldots, x_n]$ be its radical ideal. Then the Zariski closed subsets of V are the algebraic subsets contained in V. That is, they are the sets $V(J)$, where $I \subseteq J$ is a radical ideal.

Proposition 8.4.2. *Given an algebraic subset $V \subseteq F^n$, the collection of Zariski closed subsets of V form a topology of V.*

Proof. We have seen in the exercises that

$$V(I \cap J) = V(I) \cup V(J) \qquad \bigcap_i V(I_i) = V\left(\sum_i I_i\right),$$

where we may allow arbitrary index set for i (in the exercise we allowed only an index set of two elements, but the same proof shows the arbitrary index set). Also $V((1)) = \emptyset$ and $V((0)) = F^n$. □

Example 8.4.3. An infinite union of algebraic sets is not necessarily an algebraic set. For example, Let $F = \mathbb{C}$ and $I_m := (x - m) \subseteq \mathbb{C}[x]$ for $m \in \mathbb{N}$. Then $\bigcap_{m\in\mathbb{N}} I_m = 0$, so

$$V\left(\bigcap_{m\in\mathbb{N}} I_m\right) = \mathbb{C} \neq \mathbb{N} = \bigcup_{m\in\mathbb{N}} V(I_m).$$

Definition 8.4.4. The topology formed using the above closed sets is called the Zariski topology.

Example 8.4.5. (1) let $V := F$ (that is the one dimension vector space over F). Then, the Zariski closed subsets of V are V, $\emptyset$ and $\{c_1, \ldots, c_n\}$, $c_i \in F$. So, these are the closed sets.

Definition 8.4.6. A Zariski closed subset W of an algebraic set V is *irreducible*, if whenever we write $W = W_1 \cup W_2$ for some Zariski closed subsets W_i, then $W = W_i$ for some i.

Proposition 8.4.7. *Let $I \subseteq F[x_1, \ldots, x_n]$ be a radical ideal. Then $V(I)$ is irreducible if and only if I is prime.*

Proof. $\boxed{\Longrightarrow:}$ Let us assume that $V(I)$ is irreducible. Let $a, b \in R := F[x_1, \ldots, x_n]$ such that $ab \in I$, and $a, b \notin I$. Then, using that $\sqrt{I} = I$ we have $\sqrt{(a)} \not\subseteq I$ and $\sqrt{(b)} \not\subseteq I$, but $\sqrt{(ab)} \subseteq I$. Hence, by Remark 8.3.10, $V(a) \not\supseteq V(I)$ and $V(b) \not\supseteq V(I)$, but $V(I) \subseteq V(ab) = V(a) \cup V(b)$. Taking $V(a) \cap V(I)$ and $V(b) \cap V(I)$ exhibits $V(I)$ as a union of two closed subsets, none of which equals $V(I)$. This contradicts the irreducibility of $V(I)$.

$\boxed{\Longleftarrow:}$ Let us assume that I is prime, and let $W_1 \cup W_2$ be a decomposition of $V(I)$ into two proper closed subsets. Since $W_i \subsetneq V$, by Remark 8.3.10, $I(W_i) \supsetneq I(V)$. So, there are $a_i \in I(W_i) \setminus I(V)$. As $V(a_1a_2) = V(a_1) \cup V(a_2) \supseteq W_1 \cup W_2 = V(I)$, we have $a_1a_2 \in I$, again by Remark 8.3.10. However, this contradicts I being a prime. □

Proposition 8.4.8. *Every Zariski closed subset X of an algebraic set V can be written as the union of finitely many* irreducible *Zariski closed subsets. The minimal collection of such irreducible closed sets is unique.*

Definition 8.4.9. The elements of the former collection are called the irreducible components.

Proof of Proposition 8.4.8. *Existence:* Let us assume that X cannot be written as a finite union of irreducibles. Then X itself cannot be irreducible. So, we may write $X = X_1 \cup X_2$ as the union of proper closed subsets. By our assumption, it has to be impossible for X_1 or X_2 to write them as a finite union of irreducible closed subsets. We may assume that this is X_1. By replacing X by X_1 we may repeat the process. By repeating this infinitely many times, we obtain an infinite strictly decreasing chain, which by Nullstellensatz yields an infinite strictly increasing chain of ideals. This contradicts the fact that the polynomial ring is Noetherian (by the Hilbert basis theorem).

Unicity: Let $X = \bigcup_{i=1}^{n} X_i = \bigcup_{i=1}^{n'} X_i'$ be two representations of X as minimal unions of irreducible closed subsets. We may assume that $n' \geq n$. We show that there is a bijection between the X_i and the X_i'. Fix $r \in \{1, \ldots, n\}$. For every $1 \leq i \leq n'$ we have

$$X_r = \bigcup_{i=1}^{n'} (X_r \cap X_i').$$

Since X_r is irreducible, $X_r = X_r \cap X_{i_r}'$ for some i_r, and hence $X_r \subseteq X_{i_r}'$. By working with orders reversed, we obtain j_r such that $X_r \subseteq X_{i_r}' \subseteq X_{j_r}$. By the minimality of the chosen representations, we obtain that $X_r = X_{j_r}$, and hence $X_{i_r}' = X_r$. Then, $X = \bigcup_{r=1}^{n} X_{j_r}'$, where $\{j_1, \ldots, j_n\} \subseteq \{1, \ldots, n'\}$. By minimality of the representation $X = \bigcup_{i=1}^{n'} X_i'$, we get $n' = n$. □

Corollary 8.4.10. *Every radical ideal $I \subseteq F[x_1, \ldots, x_n]$ is the intersection of finitely many prime ideals.*

Proof. Let W_i be the irreducible components of $V(I)$. Then $I(V) = I\left(\bigcup_i W_i\right) = \bigcap_i I(W_i)$. □

8.5 Primary decomposition

Here we learn a stunning generalization of Corollary 8.4.10 to arbitary Noetherian rings and arbitrary ideals. This can also be viewed as the generalization of prime decomposition theorem in a UFD to a decomposition theorem for ideals in arbitrary Noetherian ring. More precisely products of elements are replaced by intersection of ideals. The price to pay for having such a general statement is that the notion of prime power elements of a UFD gets replaced with the rather convoluted notion of primary ideals:

Definition 8.5.1. An ideal $I \subseteq R$ is *primary*, if

$$ab \in I \implies a \in I \text{ or } \exists n > 0 : b^n \in I.$$

Proposition 8.5.2. *Let R be a ring and $I \subseteq R$ and ideal. The following are equivalent:*

(1) $I \subseteq R$ is primary, and

(2) every zero divisor in R/I is nilpotent.

(3) for every zero divisor $r \in R/I$ we have $\left(R/I\right)_r = 0$.

Proof. The equivalence (1) ⇔ (2) follows from from Definition 8.5.1. Then, the equivalence (2) ⇔ (3) follows from point (1) of Example 7.2.4 as in the proof of Theorem 8.3.9. □

First, we draw further analogy between prime power elements in a UFD and primary ideals by showing that primary ideals have also a "root" that is a prime ideal:

Proposition 8.5.3. *If $I \subseteq R$ is primary, then $\sqrt{I}$ is the smallest prime ideal containing I (with respect to containment).*

Proof. Every prime ideal p containing I automatically contains $\sqrt{I}$, so it is enough to show that $\sqrt{I}$ is prime.

Take $xy \in \sqrt{I}$, such that $x \notin \sqrt{I}$. Then there is an $n > 0$ such that $(xy)^n = x^n y^n \in I$. Furthermore, for the same n, $x^n \notin I$ (since $x \notin \sqrt{I}$). Then, as I is primary, there is some integer $m > 0$, such that $(y^n)^m = y^{nm} \in I$. However, then $y \in \sqrt{I}$. □

Definition 8.5.4. If $p = \sqrt{I}$ for some primary ideal $I \subseteq R$, then we say that I is *p-primary.*

Example 8.5.5. (1) $(p^n) \subseteq \mathbb{Z}$ is (p)-primary for every prime number $p \in \mathbb{Z}$.

(2) More generally, if R is a PID, and $p \in R$ is a prime element, then the (p)-primary ideals are all those of the form (p^n) for $n > 1$. Indeed, if I is an ideal contained in (p), then by the PID property $I = (r)$ such that $p|r$. So, we may write $r = p^n s$ where $n > 0$ and $(s, p) = 1$. If I is additionally (p)-primary, then s must be a unit, as otherwise s would not be contained in I, but at the same time no power of p^n would be contained in I. Finally, ideals of the form (p^n) are indeed primary as y in Definition 8.5.1 has to be divisible by p and then some power of it is contained in (p^n).

The implication of "prime power" property of primary ideals worded in Proposition 8.5.3 can be reversed in the case of maximal ideals, but not for general prime ideals. We show the former in Proposition 8.5.7 and we give an example of the latter in point (4) of Example 8.5.8.

Lemma 8.5.6. *Every non-invertible element $r \in R$ is contained in a maximal ideal.*

Proof. Since r is not invertible, $R/(r) \neq 0$, hence it has a maximal ideal m, the preimage of which in R is a maximal ideal of R containing r. □

Proposition 8.5.7. *If $I \subseteq R$ is an ideal such that $\sqrt{I} = m$ is maximal, then I is m-primary.*

Proof. By the assumptions of the proposition $\operatorname{nil}(R/I) = \sqrt{I}/I = n$ is a maximal ideal. Hence, every prime ideal of R/I contains n, which implies by the maximality of n that n is the only prime ideal of R/I. According to Lemma 8.5.6 then all the elements of $(R/I) \setminus n$ are invertible. So, every zero-divisor of R/I has to be in n and hence is nilpotent. □

End of 13. class, on 13.12.2021.

In the next example first in points (1) and (2) we show how Proposition 8.5.7 can be used to show that certain ideals are primary. Second, in points (3) and (4) we show how general primary ideals in a Noetherian ring behave much more erratically than prime power elements in a UFD. In (3) we show that unlike p-power elements for a fixed prime element p of a UFD, which are countably many up to multiplication by a unit, p-primary ideals for a prime ideal p can have arbitrary big cardinality. This example would like to convey the message that it is not easy to "list" all the p-primary ideals for a fixed prime ideal p. On the other hand, point (2) of the example tells us that although it is much trickier than for prime power elements, but for a maximal ideal m in a Noetherian ring R the m-primary ideals still can be "listed" as much as we can understand all quotients of the local ring R/m. On the other hand, point (4) of the example puts the nail into the coffin by showing that when one considers a non-maximal prime ideal p then even such a listing of p-primary ideals is not possible.

Example 8.5.8. (1) Let $(x_1, x_2) \subset F[x_1, x_2]$ be the maximal ideal of polynomials vanishing at the origin, then any monomial ideal of the form (x_1^r, x_2^s) is (x_1, x_2)-primary. Indeed, we have

$$(x_1, x_2) \supseteq \sqrt{(x_1^r, x_2^s)} \supseteq (x_1, x_2) \quad \Longrightarrow \quad (x_1, x_2) = \sqrt{(x_1^r, x_2^s)},$$

(x_1, x_2) is prime

$x_1 \in \sqrt{(x_1^r, x_2^s)}$ and $x_2 \in \sqrt{(x_1^r, x_2^s)}$

and hence we may apply Proposition 8.5.7.

(2) Let m be a maximal ideal in a Noetherian ring R. Then we show below that an ideal I is m-primary if and only if $m \supseteq I \supseteq m^n$ for some $n \in \mathbb{N}_{>0}$.

For one direction if $m \supseteq I \supseteq m^n$, then we have $m \subseteq \sqrt{I} \subseteq \sqrt{m^n} = m$ and then we may apply Proposition 8.5.7.

For the other direction as R is Noetherian we may find a finite generator set $m = (r_1, \ldots, r_s)$. Then by Proposition 8.5.3 there is an integer $l > 0$ such that $r_j^l \in I$ for every j. But, then for $N = l(j-1)+1$ we have $m^N \subseteq I$ by the pigeon-hole principle applied to the powers of the generators of m^N (which are monomials in r_j of degree N).

(3) We use point (2) to show that there are at least as many $m = (x, y)$-primary ideals in $R = F[x, y]$ as the cardinatlity $|F|$, where F is a field. Indeed, it follows directly from point (2) that for any $a \in F$ the ideal $m_a = \left(x^2, y^2, xy, ax + y\right)$ is primary. Additionally for different choices $a \in F$ the ideals m_a are different, as in any linear polynomial $0 \neq cx + dy \in m_a$ we have $\frac{c}{d} = a$.

(4) Proposition 8.5.7 does not hold for maximal replaced by prime, which we show in this example. Consider $F[x, y] \supseteq (x) \supseteq I := (x^2, xy) \supseteq (x^2)$, which implies that $\sqrt{I} = (x)$. We claim that I is not primary.

Indeed: $xy \in I$, $x \notin I$, but $y^n \notin I$ also holds for all integers $n > 0$.

Definition 8.5.9. Let $I \subseteq R$ be an ideal. I is (intersection) *irreducible*, if it cannot be written as $I = I_1 \cap I_2$ for $I \subsetneq I_1, I_2 \subsetneq R$.

We call I *decomposable* if it can be written as a finite intersection $I = \bigcap_{i=1}^{d} I_i$ where the I_i are irreducible.

Proposition 8.5.10. *If $I \subseteq R$ an ideal in a Noetherian ring. Then I is decomposable.*

Proof. Assume that I is not decomposable. Then it cannot be irreducible. So, we may write $I = I_1 \cap I_2$, where none of the I_i equals neither I nor R. Then since, I is not decomposable, (after possibly swapping the indices) I_1 is also not decomposable. By repeating the process for I_1, and then continuing indefinitely, we obtain an infinitely increasing chain of ideals, which is a contradiction. □

Lemma 8.5.11. *If I is an irreducible ideal in a Noetherian ring R, then I is primary.*

Proof. We want to verify Definition 8.5.1 for I. That is, let $ab \in I$, and we need to prove that either $a \in I$ or there is an integer $l > 0$ such that $b^l \in I$. We note that $a \in I$ is implied by $(I : b) = I$ (by the assumption $ab \in I$), and $b^l \in I$ is implied by $(b^l) + I = I$. As the irreducibility of I is our only assumption on I, the only thing we can do is to write I as the intersection of ideals as above. So this is what we do below:

For $j \in \mathbb{N}$, the ideals $(I : b^j)$ form an increasing chain. By Noetherianity, the chain has to stabilize, that is, there exists $n \in \mathbb{N}_{>0}$ such that for any $j \geq n$, $(I : b^j) = (I : b^n)$. We define $J := (I : b^n)$, and $K := (b^n) + I$.

Claim. $K \cap J = I$.

Proof. It follows immediately from the definitions that $I \subseteq J \cap K$. Hence, we only need to show that every $r \in K \cap J$ is contained in I. This is shown by the following

implications:

$$r = s + tb^n \implies rb^n = sb^n + tb^{2n} \implies t \in \left(I : b^{2n}\right) = (I : b^n) \implies r = s + tb^n \in I.$$

$r = s + tb^n$: by $r \in K$ for some $s \in I$ and $t \in R$

$t \in \left(I : b^{2n}\right)$: $r \in J \Rightarrow rb^n \in I$

□

As I is irreducible, the above claim implies one of the following: either

(1) $J = I$, then $I = (I : b^n) \supseteq (I : b) \supseteq I$, so $(I : b) = I$ and hence $a \in I$, or

(2) $I = K$, then $b^n \in I$.

□

Lemma 8.5.12. *If I and I' are p-primary ideals of R, then so is $I \cap I'$.*

Proof. Consider $ab \in I \cap I'$, and assume $a \notin I \cap I'$. Then (by possibly swapping I and I'), $a \notin I$. Since I is p-primary, there exists an integer $n > 0$ such that $b^n \in I$. This is equivalent to saying that $b \in p$. However, then (by possibly increasing n), $b^n \in I'$ also holds. That is $I \cap I'$ is indeed primary.

We are left to show that $\sqrt{I \cap I'} = p$. As $\sqrt{I} = \sqrt{I'} = p$, it is immediate that $\sqrt{I \cap I'} \subseteq p$. For the other containment, take $r \in p$. Then there are integer $n, m > 0$ such that $r^n \in I$ and $r^m \in I'$. However then $r^{n+m} \in I \cap I'$, and so $r \in \sqrt{I \cap I'}$.

□

Putting together the statements of Proposition 8.5.10, Lemma 8.5.11, we obtain the following result on the existence of a decomposition into primary ideals in a noetherian ring.

Corollary 8.5.13. *Let R be a Noetherian ring and $I \subset R$ be an ideal.*
Then, there exists a decomposition

$$I = \bigcap_{i=1}^{n} I_i$$

where the I_i are primary ideals such that $\mathfrak{p}_i := \sqrt{I_i}$ are all distinct.
Furthermore, we may assume the following minimality condition:

$$\text{for any } i = 1, \ldots, n,\ I_i \not\supseteq \bigcap_{j \neq i} I_j$$

Definition 8.5.14. The decomposition of an ideal $I \subset R$ whose existence is claimed in Corollary 8.5.13 is called *minimal primary decomposition.*

Example 8.5.15. Let $I = (x^2, xy) \subseteq F[x, y]$, for some field F. Then a minimal primary decomposition is $I := (x) \cap (x^2, y)$. The minimality here is immediate, so we only why $I := (x) \cap (x^2, y)$ holds. By definition, the elements of $(x) \cap (x^2, y)$ are polynomials of the form $f = gx^2 + hy$ for arbitrary $g, h \in F[x, y]$ such that $x | f$. However, as x and y are relatively prime this means that $x | h$. So, if we write $h' := \frac{h}{x}$ then we obtain that $f = gx^2 + h'xy$ for arbitrary $g, h' \in F[x, y]$. This concludes the proof of $I = (x) \cap (x^2, y)$.

Is this decomposition unique? Not quite, as for example, we may write $I := (x) \cap (x^2, xy, y^j)$ for any integer $j > 0$. On the other hand, in either case, the radicals of the two factors are (x) and (x, y). It turns out that this is unique, which we prove below.

Definition 8.5.16. Let R be a ring, let $I \subset R$ be and ideal, and let M be an R-module.

(1) A prime ideal $p \subseteq R$ is called an *associated prime* (or component in some uses of language) of M if $p = \mathrm{Ann}(m)$ for some $m \in M$.

(2) The associated primes of R/I are called the associated primes of I.

The set of associated primes of M (resp. I) are denoted by $\mathrm{Ass}(M)$ (resp. $\mathrm{Ass}(I)$).

The definition of $\mathrm{Ass}(I)$ is an abuse of language, as it is really the set of associated primes of the R-module R/I. However considering the associated primes of I itself as a module over R is not too interesting, as it is a subset of the associated primes of R, this is a widespread notational practice.

Recall that for an R-module M and $m \in M$, the ideal $\mathrm{Ann}(m)$ is defined as $\mathrm{Ann}(m) := \{r \in R \mid rm = 0\}$. The following characterization of the associated primes of I then follows from Definition 8.5.16.

Proposition 8.5.17. *If $I \subseteq R$ is an ideal, then p is an associated prime of I if and only if $p = (I : x)$ for some $x \in R$.*

Proposition 8.5.18. *Let $I \subseteq R$ be a p-primary ideal, and $x \in R$. Then*

(1) if $x \in I$, then $(I : x) = (1)$,

(2) if $x \notin I$, then $(I : x)$ is p-primary, and

(3) if $x \notin I$ and R is Noetherian, then there is an $r \in R$, such that $rx \notin I$ and $(I : rx) = p$.

Proof. *(1):* This is immediate from the definition of a the colon ideal.

(2): Choose $ab \in (I : x)$ such that $a \notin (I : x)$. That is, $abx \in I$, but $ax \notin I$. Then by Definition 8.5.1, there is an integer $n > 0$ such that $b^n \in I$. Hence, $b^n x \in I$, whence $b^n \in (I : x)$. This shows that $(I : x)$ is primary.

We have to also show that $\sqrt{(I : x)} = p$. So, assume $b^n \in (I : x)$ for some integer $n > 0$. Then:

$$b^n x \in I \underset{\uparrow}{\Longrightarrow} \exists m > 0 : \ (b^n)^m = b^{nm} \in I \underset{\uparrow}{\Longrightarrow} b \in p$$

$x \notin I$ and I is primary — $p = \sqrt{I}$

So, we obtain that $\sqrt{(I : x)} = p$ indeed holds.

(3): We start with the following claim:

Claim. *If $x \notin I$ and $(I : x) \neq p$, then there is $t \in R$, such that $tx \notin I$ and $(I : x) \subsetneq (I : tx)$.*

Proof. Choose $s \in p \setminus (I : x)$. Since $\sqrt{(I : x)} = p$, there is an integer $n > 1$, such that $s^n \in (I : x)$. Fix a minimal such integer n. Then the following holds:

- $s^{n-1} \notin (I : x)$ and hence $s^{n-1}x \notin I$, and
- $(I : s^{n-1}x) \supsetneq (I : x)$, as $(I : x) \not\ni s \in (I : s^{n-1}x)$.

Hence we may set $t = s^{n-1}$ □

By applying iteratedly the above claim we obtain an increasing chain of ideals

$$(I : x) \subsetneq (I : t_1 x) \subsetneq (I : t_2 t_1 x) \subsetneq \dots, \tag{5.18.a}$$

unless for some n we reach to a point where $p = \left(I : x \prod_{j=1}^{n} t_j\right)$. In the latter case, we can set $r = \prod_{j=1}^{n} t_j$. So, we may assume that the chain (5.18.a) goes on forever. However, this contradicts Noetherianity. □

Proposition 8.5.19. *Let R be a ring and $x \in R$. If $I_1, \dots, I_n \subseteq R$ are ideals, then*

(1) $\left(\bigcap_{i=1}^{n} I_i : x\right) = \bigcap_{i=1}^{n} (I_i : x)$

(2) $\sqrt{\left(\bigcap_{i=1}^{n} I_i\right)} = \bigcap_{i=1}^{n} \sqrt{I_i}$

Proof. Both follow straight from the definition. In fact, in the first one finiteness of the intersection is not even necessary. On the other hand, in the second one it is important, to be able to pass to a common power. □

Lemma 8.5.20. *Let R be a ring. Let $I_1, \dots, I_n, p \subset R$ be ideals, with p a prime ideal. If $p \supseteq \bigcap_{i=1}^{s} I_i$, then there exists i such that $p \supseteq I_i$.*

Proof. Assume the contrary. Then for every i there exists an $x_i \in I_i \setminus p$. Then $\prod_{i=1}^{s} x_i \in \left(\bigcap_{i=1}^{s} I_i\right) \setminus p$, as p is prime, which gives the desired contradiction. □

Our version of primary decomposition that includes a unicity statement is as follows:

Theorem 8.5.21. *In a Noetherian ring R, any ideal I admits a minimal primary decomposition*

$$I = \bigcap_{i=1}^{s} I_i.$$

Furthermore, the set of prime ideals $\sqrt{I_i}$ is unique, and it agrees with the associated primes of I.

Proof. *Existence:* The existence of the decomposition follows from Corollary 8.5.13.

Uniqueness: Let us compute $(I : x)$ for any $x \in R$, using Proposition 8.5.19:

$$(I : x) = \left(\bigcap_{i=1}^{s} I_i : x\right) = \bigcap_{i=1}^{s} (I_i : x) \tag{5.21.b}$$

By the minimality assumption, for each i, we can find

$$x_i \in \left(\bigcap_{i \neq j} I_j\right) \setminus I_i.$$

By point (3) of Proposition 8.5.18, we may also assume that $(I_i : x_i) = \sqrt{I_i}$. Then, according to (5.21.b), $(I : x_i) = (I_i : x_i) = \sqrt{I_i}$, which shows that every ideal of the form $\sqrt{I_i}$ is an associated prime.

Now, let p be an associated prime that is $p = (I : x)$ for some $x \in R$. Then, also $p = \sqrt{(I : x)}$. By (5.21.b) and Proposition 8.5.19, then $p = \bigcap_{i=1}^{s} \sqrt{(I_i : x)} = \bigcap_{x \notin I_i} \sqrt{I_i}$. However, according to Lemma 8.5.20, this means that $p = \sqrt{I_i}$ for some i. □

Finally we state an even more general version of primary decomposition that we do not prove in this course:

Definition 8.5.22. Let R be a Noetherian ring and $I \subset R$ be an ideal. Let $\{p_1, \dots, p_n\}$ be the associated prime ideals of I.

The ideal p_i is a *minimal associated prime* if p_i is minimal with respect to inclusion among the associated primes of I, that is, $p_j \not\subseteq p_i$, for $j \neq i$.

If p_i is not minimal, then we say that it is an *embedded associated prime*.

Theorem 8.5.23. *Let R be a Noetherian ring, let $I \subset R$ be an ideal, and let*

$$I = \bigcap_{i=1}^{n} I_i$$

be a minimal primary decomposition, as in Theorem 8.5.21. Then, the ideals I_i corresponding to minimal associated primes p_i are uniquely determined. That is, if $I = \cap_{i=1}^{n} I_i'$ is another minimal primary decomposition, then $I_i = I_i'$ if p_i is a minimal associated prime of I.

For the proof of Theorem 8.5.23, one can consult Chapter 4 of Atiyah-MacDonald "Introduction to Commutative Algebra".

Example 8.5.24. We have seen in Example 8.5.15 that the ideal $I := (x^2, xy) \subseteq F[x, y]$ admits several primary decompositions $I = (x) \cap (x^2, xy, y^j)$, $j > 0$. The associated primes are $(x), (x, y)$; thus, (x) is a minimal associated prime, while (x, y) is an embedded one. Therefore, Theorem 8.5.23 implies that the ideal (x) is uniquely identified in the primary decomposition of I and the non-uniqueness can only be induced by the other ideal.

End of 14. class, on 20.12.2021.