Lecture Notes for Commutative Algebra (MS-EV0013)

Milo Orlich

April 5, 2023

Contents

These notes are written for the 2022-2023 implementation of Commutative Algebra (MS-EV0013). The first part is based on the notes by Mateusz Michałek for the 2018-2019 implementation. The students are encouraged to consult textbooks and other material, as suggested in MyCourses.

If you spot typos or just wish to give feedback, please send a message to

`milo.orlich@aalto.fi`

1 Ideals

Definition 1.1. In this course a ***ring*** is a commutative unital ring with $1 \neq 0$.

An ***ideal*** I of a ring R is a nonempty subset for which the following conditions hold:

$$I + I := \{i + j \mid i, j \in I\} \subseteq I, \qquad RI := \{ri \mid r \in R, i \in I\} \subseteq I.$$

An ideal I is ***proper*** if $I \neq R$. To indicate that a subset I is an ideal we will write $I \lhd R$.

A ***unit*** is an element of a ring that has a multiplicative inverse. The set of all units $\mathcal{U}(R)$ of a ring R is an abelian group with respect to multiplication. A ring is a ***field*** if $\mathcal{U}(R) = R \setminus \{0\}$.

A ***nilpotent*** is an element $r \in R$ for which $r^n = 0$ for some positive integer n. The set of all nilpotents will be denoted by $\mathrm{nil}(R)$.

A ***zero-divisor*** is an element $r \in R$ for which there exists an $s \in R \setminus \{0\}$ such that $sr = 0$. The set of all zero-divisors will be denoted by $D(R)$. A ring is called an ***integral domain*** if $D(R) = \{0\}$.

Given two rings A and B, a function $f\colon A \to B$ is a ***ring homomorphism*** if

$$\forall_{x,y \in A} f(x +_A y) = f(x) +_B f(y), \qquad \forall_{x,y \in A} f(x \cdot_A y) = f(x) \cdot_B f(y), \qquad f(1_A) = 1_B.$$

Lemma 1.2. *Let R be a ring.*

1. *$\mathcal{U}(R) + \mathrm{nil}(R) = \mathcal{U}(R)$, that is, a unit plus a nilpotent is a unit, and vice-versa.*
2. *The following conditions are equivalent:*
   - *R is a field;*
   - *R has only two ideals: (0) and R;*
   - *every ring homomorphism from R is injective.*

Proof. Exercise. □

Basic operations on ideals

Let R be a ring, let $I_1, \ldots, I_k$ be a finite collection of ideals, and let $(I_\lambda)_{\lambda \in \Lambda}$ be an arbitrary (possibly infinite) collection of ideals indexed by some set Λ. The followig constructions give ideals:

- sum of finitely many ideals: $I_1 + \cdots + I_k := \{i_1 + \cdots + i_k \mid i_j \in I_j\}$;
- intersection of arbitrarily many ideals: $\bigcap_{\lambda \in \Lambda} I_\lambda$;
- ideal generated by a subset $S \subseteq R$:
$$(S) := \bigcap_{I \lhd R,\, I \supseteq S} I;$$
- sum of an arbitrary family of ideals: $\sum_{\lambda \in \Lambda} I_\lambda := \left(\bigcup_{\lambda \in \Lambda} I_\lambda\right)$;
- product of finitely many ideals: $I_1 \cdots I_k := \left(\{i_1 \cdots i_k \mid i_j \in I_j\}\right)$;
- powers of an ideal: $I^n := I \cdots I$ (product of I with itself n times);
- colon (or quotient) ideal: $I_1 : I_2 := \{x \in R \mid xI_2 \subseteq I_1\}$.

Exercise 1.3.

- Show that the result of any of the above operations is an ideal.
- Show that the set $\{i_1 \cdots i_k \mid i_j \in I_j\}$ might not be an ideal.
- Show that $I_1 \cup I_2$ might not be an ideal.
- In general, $I_1 \cdots I_k \subseteq I_1 \cap \cdots \cap I_k$. Give an example in which $I_1 I_2 = I_1 \cap I_2$ and an example in which $I_1 I_2 \subsetneq I_1 \cap I_2$.

Definition 1.4. An ideal is ***finitely generated*** if it is of the form $(i_1, \dots, i_k) = Ri_1 + \cdots + Ri_k$ for some elements $i_1, \dots, i_k \in R$.

Two important cases of colon ideals are:

- the ***annihilator of an ideal*** J, defined as $\operatorname{ann}(J) := 0 : J$,
- the ***annihilator of an element*** x, defined as $\operatorname{ann}(x) := 0 : (x)$.

Example 1.5. If $R = \mathbb{Z}$ and $I = (m)$ and $J = (n)$, then $I : J = (\frac{m}{\gcd(m,n)})$.

Lemma 1.6 (Basic properties of operations on ideals)**.** *With the same notation as in the definitions above, and for any ideals I, J and L, the following hold:*

1. $I \subset I : J$,
2. $(I : J)J \subset I$,
3. $(I : J) : L = I : (JL) = (I : L) : J$,
4. $(\bigcap_\lambda I_\lambda) : J = \bigcap_\lambda (I_\lambda : J)$,
5. $D(R) = \bigcup_{x \neq 0} \operatorname{ann}(x)$.

Definition 1.7. Let A be a ring.

- For an ideal $I \lhd A$, we define the ***radical*** of I as $\sqrt{I} := \{x \in A \mid \exists_{n \in \mathbb{Z}_+} x^n \in I\}$.
- The ***nilradical*** of A is $\operatorname{nil}(A) := \sqrt{(0)}$. (This is the same as the set of nilponents above.)
- We say that A is ***reduced*** if $\operatorname{nil}(A) = (0)$.
- The ***reduction*** of A is $A_{\text{red}} := A/\operatorname{nil}(A)$.

Example 1.8. Consider $A = \mathbb{Z}$. Recall that all ideals of $\mathbb{Z}$ are principal, that is, of the form $(a) = a\mathbb{Z}$, for $a \in \mathbb{Z}$. If a is not invertible and not zero, let $p_1, \dots, p_r$ be the pairwise distinct prime factors of a, so that $a = p_1^{n_1} \cdots p_r^{n_r}$. Then $\sqrt{(a)} = (p_1 \cdots p_r)$.

Definition 1.9. Let $f \colon A \to B$ be a ring homomorphism. For an ideal $I \lhd A$, we define the ***extension*** of I (along f) as the ideal generated by the image of I, that is,

$$I^e := (f(I)),$$

also denoted as IB. For an ideal $J \lhd B$, we define the ***contraction*** of J (along f) as the preimage of J, that is,

$$J^c := f^{-1}(J),$$

also denoted as $J \cap A$.

Remarks 1.10.

- Observe that $(0)^c = \ker(f)$.

- The image of an ideal might not be an ideal. (Consider $\mathbb{Z} \hookrightarrow \mathbb{Q}$.)
- The notations IB and $J \cap A$ are inspired by the case where $f: A \hookrightarrow B$ is an inclusion of rings.

Example 1.11. Consider the homomorphism $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]$, and the ideal $(2) \subseteq \mathbb{Z}$. Then $(2) = \{2n \mid n \in \mathbb{Z}\}$, and $(2)^e = \{2f \mid f \in \mathbb{Z}[x]\}$. Consider now the ideal $J := \{3f \mid f \in \mathbb{Z}[x]\} \subseteq \mathbb{Z}[x]$. Then $J^c = J \cap \mathbb{Z} = \{3n \mid n \in \mathbb{Z}\}$.

Lemma 1.12. *Let $f: A \to B$ be a ring homomorphism, $I \lhd A$ and $J \lhd B$.*

1. *The contraction J^c is an ideal of A,*
2. *$I \subseteq I^{ec}$ and $J \supseteq J^{ce}$,*
3. *$I^e = I^{ece}$ and $J^c = J^{cec}$.*

Lemma 1.13. *Let $f: A \to B$ be a ring homomorphism. Let $\mathcal{C} := \{J^c \mid J \lhd B\}$ be the set of ideals that are contractions of ideals of B, and let $\mathcal{E} := \{I^e \mid I \lhd A\}$ be the set of ideals that are extensions of ideals of A.*

1. *$\mathcal{C} = \{I \lhd A \mid I^{ec} = I\}$ and $\mathcal{E} = \{J \lhd B \mid J^{ce} = J\}$.*
2. *Extension and contraction give pairwise inverse bijections between $\mathcal{C}$ and $\mathcal{E}$.*
3. *$\mathcal{C}$ is closed under taking intersection and radical.*
4. *$\mathcal{E}$ is closed under taking sum and product.*
5. *For any ideal $J \lhd B$, one has $\sqrt{J^c} = (\sqrt{J})^c$.*
6. *If f is an epimorphism (that is, a surjective homomorphism), then for any ideal I satisfying $\ker(f) \subseteq I$, one has $\sqrt{I^e} = (\sqrt{I})^e$.*

Example 1.14. A very important homomorphism is the canonical "projection"

$$\pi: A \longrightarrow A/I,$$

for some $I \lhd A$. Then, for $I' \lhd A$, we have

$$(I')^e = \pi(I') = (I + I')/I,$$

$$(I')^{ec} = \pi^{-1}(\pi(I')) = I + I'.$$

The contraction map defines a bijection

$$\{\text{ideals of } A/I\} \longrightarrow \{\text{ideals of } A \text{ which contain } I\}.$$

Remark 1.15. By Lemma 1.13, one has $\pi(\sqrt{I}) = \operatorname{nil}(A/I)$, so that A_{red} is a reduced ring.

Lemma 1.16. *For any two ideals $I, J \lhd A$, the following hold:*

1. $I \subseteq \sqrt{I}$
2. $\sqrt{\sqrt{I}} = \sqrt{I}$
3. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
4. $\sqrt{I} = (1) \Leftrightarrow I = (1)$
5. $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$
6. $\sqrt{I} + \sqrt{J} = (1) \Leftrightarrow I + J = (1)$.

Definition 1.17. Let A be a ring. An ideal $\mathfrak{m} \lhd A$ is called a ***maximal ideal*** if it is proper (that is, $\mathfrak{m} \subsetneq A$) and for any $J \lhd A$, if $\mathfrak{m} \subset J \subset A$, then $J = \mathfrak{m}$ or $J = A$. In other words, $\mathfrak{m}$ is maximal with respect to inclusion, among the proper ideals of A. The set

$$\operatorname{Max}(A) := \{\mathfrak{m} \lhd A \mid \mathfrak{m} \text{ is maximal}\}$$

of all maximal ideals of A is called the ***maximal spectrum*** of A. The intersection of all maximal ideals

$$J(A) := \bigcap_{\mathfrak{m} \in \operatorname{Max}(A)} \mathfrak{m}$$

is called the ***Jacobson radical*** of A.

Proposition 1.18. *Let A be a ring.*

1. $\mathfrak{m} \in \operatorname{Max}(A) \Leftrightarrow A/\mathfrak{m}$ *is a field.*

2. *Every proper ideal is contained in a maximal ideal. In particular, every element of $A \setminus \mathcal{U}(A)$ is contained in a maximal ideal.*[1]

3. $\operatorname{Max}(A) \neq \emptyset$.

4. $x \in J(A) \Leftrightarrow \forall_{y \in A} 1 - xy \in \mathcal{U}(A)$.

Proof. 1. Exercise.

2. This is a direct application of Zorn's lemma. (If you are not familiar with it, check Appendix B.)

3. (0) is a proper ideal, since $1 \neq 0$ in this course.

4. ($\Rightarrow$) Let $x \in J(A)$. Suppose that $1 - xy \notin \mathcal{U}(A)$ for some $y \in A$. Then there exists $\mathfrak{m} \in \operatorname{Max}(A)$ such that $1 - xy \in \mathfrak{m}$. Since $x \in \mathfrak{m}$, this would imply that $1 \in \mathfrak{m}$, which is a contradiction.

   ($\Leftarrow$) Suppose by contradiction that for all $y \in A$ we have $1 - xy \in \mathcal{U}(A)$, and there is a maximal ideal $\mathfrak{m}$ that does not contain x. Then $(x) + \mathfrak{m} = (1)$, i.e., there exists $y_0 \in A$ such that $1 - xy_0 \in \mathfrak{m}$, hence $1 - xy_0 \notin \mathcal{U}(A)$.

□

Definition 1.19. A ring A is called a ***local ring*** if it has exactly one maximal ideal $\mathfrak{m}$. A local ring is usually written as a pair $(A, \mathfrak{m})$, or a triple $(A, \mathfrak{m}, k)$, where $k := A/\mathfrak{m}$ is called the ***residue field*** of A. A ring A is called a ***semilocal ring*** if $\#\operatorname{Max}(A) < \infty$.

Example 1.20. Every field is a local ring. We will see more examples in Lecture 6.

Proposition 1.21. 1. *If $(A, \mathfrak{m})$ is a local ring, then $\mathcal{U}(A) = A \setminus \mathfrak{m}$.*

2. *If $\mathfrak{m} \lhd A$, $\mathfrak{m} \neq A$ and $A \setminus \mathfrak{m} \subseteq \mathcal{U}(A)$, then A is local and $\mathfrak{m}$ is the unique maximal ideal.*

3. *If $\mathfrak{m} \in \operatorname{Max}(A)$ and $1 + \mathfrak{m} \subseteq \mathcal{U}(A)$, then A is local.*

Proof. 1. Every proper ideal is disjoint from $\mathcal{U}(A)$, so that $\mathfrak{m} \subseteq A \setminus \mathcal{U}(A)$. Every non-invertible element is contained in a maximal ideal, so $A \setminus \mathcal{U}(A) \subseteq \mathfrak{m}$.

2. It follows that $A \setminus \mathcal{U}(A) \subseteq \mathfrak{m}$, hence every proper ideal is contained in $\mathfrak{m}$.

[1] This statement, commonly known as Krull's theorem, is equivalent to the axiom of choice.

3. If $x \in A \setminus \mathfrak{m}$, then $(x) + \mathfrak{m} = A$. Hence, there exist $y \in A$ and $b \in \mathfrak{m}$ such that $xy + b = 1$. Hence, $xy \in \mathcal{U}(A)$, and therefore $x \in \mathcal{U}(A)$.

□

Theorem 1.22 (Chinese Remainder Theorem). *Let $I_1, \ldots, I_r \lhd A$ be pairwise coprime ideals of a ring A, i.e., $I_i + I_j = A$ for $i \neq j$. Then:*

1. *$I_1 \cdots I_r = I_1 \cap \cdots \cap I_r$. In particular, if A is semilocal, then $J(A)$ is the product of the maximal ideals of A.*
2. *$A/(I_1 \cdots I_r) \cong A/I_1 \times \cdots \times A/I_r$.*

Proof. 1. For $r = 2$, we have

$$I_1 \cap I_2 \;=\; (I_1 + I_2)(I_1 \cap I_2) \;\subseteq\; I_1(I_1 \cap I_2) + I_2(I_1 \cap I_2) \;\subseteq\; I_1 I_2.$$

For $r > 2$, let $J := I_1 \cdots I_{r-1} = I_1 \cap \cdots \cap I_{r-1}$. The claim follows by induction if we know that $J + I_r = A$. To show this, pick $x_i \in I_i$ and $y_i \in I_r$, for all $i \in \{1, \ldots, r-1\}$, so that $x_i + y_i = 1$. Then

$$\prod_{i=1}^{r-1}(1 - y_i) = \prod_{i=1}^{r-1} x_i \in J$$

is 1 modulo I_r.

2. Consider the homomorphism

$$\begin{aligned} f\colon A &\longrightarrow A/I_1 \times \cdots \times A/I_r \\ x &\longmapsto (x + I_1, \ldots, x + I_r). \end{aligned}$$

The kernel of f is equal to $I_1 \cap \cdots \cap I_r$, which by the first part is equal to $I_1 \cdots I_r$. To finish the proof, it remains to show that the f is surjective:

- For $r = 2$, let $(a + I_1, b + I_2) \in A/I_1 \times A/I_2$. Pick $x_1 \in I_1$ and $x_2 \in I_2$ so that $x_1 + x_2 = 1$. Then $f(bx_1 + ax_2) = (a + I_1, b + I_2)$, since $bx_1 + ax_2 = ax_1 + ax_2 = a$ modulo I_1, and similarly for I_2.
- For $r > 2$, the proof follows by induction, as in the previous part.

We conclude by the first isomorphism theorem. □

Example 1.23. $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

2 Prime and primary ideals

Definition 2.1. An ideal $p \lhd A$ is called a ***prime ideal*** if p is proper and for $x, y \in A$, if $xy \in p$, then $x \in p$ or $y \in p$ (equivalently, if $xy \in I$ and $x \notin I$, then $y \in I$). The set

$$\operatorname{Spec}(A) := \{p \lhd A \mid p \text{ is prime}\}$$

is called the ***spectrum*** of A.

Lemma 2.2. *For any ring homomorphism $f \colon A \to B$, we have an induced map of spectra:*

$$\begin{aligned}\overline{f} \colon \operatorname{Spec}(B) &\longrightarrow \operatorname{Spec}(A)\\ q &\longmapsto f^{-1}(q).\end{aligned}$$

Remarks 2.3.

- The contraction of a maximal ideal might not be a maximal ideal. Consider for instance the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ and $(0) \in \operatorname{Max}(\mathbb{Q})$.
- The extension of a prime ideal might not be a prime ideal. Consider for instance $\mathbb{Z} \hookrightarrow \mathbb{Q}$ and $(2) \in \operatorname{Spec}(\mathbb{Z})$, or the projection $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ and $(0) \in \operatorname{Spec}(\mathbb{Z})$.

Definition 2.4. Let A be a ring. A subset $S \subseteq A$ is called a ***multiplicative system*** if $1 \in S$ and for all $x, y \in S$ we have $xy \in S$.

Proposition 2.5. *Let A be a ring.*

1. *$p \in \operatorname{Spec}(A) \Leftrightarrow A/p$ is an integral domain $\Leftrightarrow A \setminus p$ is a multiplicative system,*
2. *$\operatorname{Max}(A) \subseteq \operatorname{Spec}(A)$.*

Theorem 2.6 (Prime Avoidance Lemma)**.** *Let A be a ring.*

1. *If $I_1, \ldots, I_s \lhd A$, $p \in \operatorname{Spec}(A)$ and $I_1 \cdots I_s \subseteq p$, then for some $k \in \{1, \ldots, s\}$ we have $I_k \subseteq p$.*
2. *Let $S \subseteq A$ be closed under multiplication and addition. Let $p_1, \ldots, p_s \lhd A$, with $s \geq 2$, and suppose that $p_3, \ldots, p_s$ are prime. If $S \subseteq p_1 \cup \cdots \cup p_s$, then for some $k \in \{1, \ldots, s\}$ we have $S \subseteq p_k$.*
3. *If $J \subsetneq I$ are ideals of A, $p_1, \ldots, p_s \in \operatorname{Spec}(A)$ and $I \setminus J \subseteq p_1 \cup \cdots \cup p_s$, then there exists some $k \in \{1, \ldots, s\}$ such that $I \subseteq p_k$.*

Proof.

1. By contradiction, suppose that $a_i \in I_i \setminus p$ for all $i \in \{1, \ldots, s\}$. Then $a_1 \cdots a_s \in I_1 \cdots I_s \subseteq p$. Since p is a prime ideal, we have $a_k \in p$ for some k, which is a contradiction.
2. By contradiction, assume that s is minimal such that $S \subseteq p_1 \cup \cdots \cup p_s$. Hence, there exist elements $a_1, \ldots, a_s \in S$ such that $a_i \in p_i$ and $a_i \notin p_1 \cup \cdots \cup p_{i-1} \cup p_{i+1} \cup \cdots \cup p_s$, for all $i \in \{1, \ldots, s\}$.
   - For $s = 2$, we have $a_1 \in p_1$ and $a_2 \notin p_1$, thus $a_1 + a_2 \notin p_1$. In the same way $a_1 + a_2 \notin p_2$, which contradicts $a_1 + a_2 \in S$.
   - For $s > 2$, let $a := a_1 \cdots a_{s-1} + a_s \in S$. As $a_1 \cdots a_{s-1} \in p_1 \cap \cdots \cap p_{s-1}$ and $a_s \notin p_1 \cup \cdots \cup p_{s-1}$, we must have $a \notin p_1 \cup \cdots \cup p_{s-1}$. Since p_s is a prime ideal, we also have $a_1 \cdots a_{s-1} \notin p_s$, but $a_s \in p_s$, hence $a \notin p_s$. So, $a \in S$ but $a \notin p_1 \cup \cdots \cup p_s$, which is a contradiction.
3. The fact that $I \setminus J \subseteq p_1 \cup \cdots \cup p_s$ implies that $I \subseteq J \cup p_1 \cup \cdots \cup p_s$. We conclude by part 2.

□

Theorem 2.7. *Let A be a ring. Let $S \subseteq A$ be a multiplicative system. For any ideal $I \lhd A$ disjoint from S, there exists a prime ideal p containing I and disjoint from S.*

Proof. By Zorn's lemma, there exists an ideal J containing I and disjoint from S that is maximal with respect to inclusion among all ideals containing I and disjoint from S. We prove that J is a prime ideal. Since $1 \in S$, J is proper. Secondly, consider $x, y \notin J$. Since $(x) + J$ and $(y) + J$ intersect S, we know that there exist $a, b \in A$ and $s, s' \in S$ such that $ax = s$ and $by = s'$ modulo J. Hence $abxy - ss' \in J$. Since $ss' \in S$, we have $abxy \notin J$, so that $xy \notin J$. □

Corollary 2.8. *Let A be a ring. For any proper ideal I of A, we have*

$$\sqrt{I} = \bigcap_{\substack{p \in \operatorname{Spec}(A), \\ p \supseteq I}} p.$$

In particular, $\bigcap_{p \in \operatorname{Spec}(A)} p = \operatorname{nil}(A)$.

Proof. ($\subseteq$) This is obvious, as $I \subseteq p$ implies that $\sqrt{I} \subseteq \sqrt{p} = p$ for all $p \in \operatorname{Spec}(A)$.

($\supseteq$) If $x \notin \sqrt{I}$, then $S := \{1, x, x^2, \dots\}$ is a multiplicative system and is disjoint from I. Therefore, by Theorem 2.7, there exists some $p \in \operatorname{Spec}(A)$ containing I and disjoint from S. In particular, $x \notin p$. □

Proposition 2.9. *Let A be a ring. For any proper ideal I of A, let $V(I) := \{p \in \operatorname{Spec}(A) \mid I \subseteq p\}$. The set $V(I)$ contains elements that are minimal with respect to inclusion.*

Definition 2.10. Let A be a ring and $I \subsetneq A$ an ideal. The inclusion-minimal elements of $V(I)$ are called the ***minimal prime ideals of the ideal*** I. For $I = (0)$, we call the inclusion-minimal elements of $V((0))$ the ***minimal prime ideals of the ring*** A.

Examples 2.11.

- Consider the ideal $I := (0) \lhd \mathbb{Z}$. Then I is contained in every prime ideal of $\mathbb{Z}$, that is, $V(I) = \operatorname{Spec}(\mathbb{Z})$, and the only minimal prime of I is I itself.
- In general the only minimal prime of a prime ideal is that prime ideal.
- If A is a domain, then (0) is the only minimal prime of A.
- Consider the ideal $I := (x^2)$ in the polynomial ring $A = \mathbb{K}[x, y]$, where $\mathbb{K}$ is a field. Since $A/(x) \cong \mathbb{K}[y]$ and $A/(x, y) \cong \mathbb{K}$ are integral domains, both (x) and (x, y) are prime ideals, and both of them contain I. So in particular both (x) and (x, y) are elements of $V(I)$. For instance (y) is a prime ideal of A that does not contain (x^2).

2.1 The Zariski topology

For the rest of the section A is a ring. Our next goal is to introduce a topology on the set $\operatorname{Spec}(A)$. Recall that on any set X one can define a ***topology*** in two equivalent ways. First, by distinguishing a family of subsets of X that

1. contains the empty set and the whole space X,
2. is closed under taking arbitrary intersections and finite unions.

The subsets in such a family are called ***closed sets***. One can change the second condition above by asking that the family is closed under taking finite intersections and arbitrary unions, thereby obtaining the family of ***open sets***. The open sets are the complements of the closed sets. (See Appendix A if you are not familiar with topology.)

Definition 2.12. For any subset $Q \subseteq A$, we define $V(Q) := \{p \in \operatorname{Spec}(A) \mid Q \subseteq p\}$.

Lemma 2.13. *1. If $Q_1 \subseteq Q_2$, then $V(Q_2) \subseteq V(Q_1)$.*

2. If $I = (Q)$, then $V(I) = V(Q) = V(\sqrt{I})$.

3. $V(A) = \emptyset$ and $V((0)) = \operatorname{Spec}(A)$.

4. For any family of subsets $\{Q_\lambda\}_{\lambda\in\Lambda}$, we have $\bigcap_{\lambda\in\Lambda} V(Q_\lambda) = V(\bigcup_{\lambda\in\Lambda} Q_\lambda)$.

5. If $I_1, \dots, I_k \lhd A$, then $V(I_1 \cdots I_k) = V(I_1 \cap \cdots \cap I_k) = V(I_1) \cup \cdots \cup V(I_k)$.

Proof. The first four properties are left as an exercise. As for part 5., $V(I_1) \cup \cdots \cup V(I_k) \subseteq V(I_1 \cap \cdots \cap I_k) \subseteq V(I_1 \cdots I_1)$. The inclusion $V(I_1 \cdots V_k) \subseteq V(I_1) \cup \cdots \cup V(I_k)$ follows from the prime avoidance lemma (Theorem 2.6). □

The family $\{V(Q)\}_{Q\subseteq A}$ satisfies the axioms of closed sets. The induced topology on Spec(A) is called the ***Zariski topology of*** A.

Example 2.14.

- Recall that the prime ideals of $\mathbb{Z}$ are (0) and all the ideals (p), for p a prime. For any $a \in \mathbb{Z}$, the set $V(a) := V(\{a\})$ consists of the primes that contain a. If a is a unit, that is, 1 or −1, then $V(a) = \emptyset$, because no prime ideal contains a unit. If $a = 0$, then $V(a) = \operatorname{Spec}(A)$, because all prime ideals contain 0. In all other cases, let $p_1, \dots, p_s$ be the prime factors of a. Then $V(a) = \{(p_1), (p_2), \dots, (p_s)\}$. For instance, $V(4) = V(1024) = \{(2)\}$ and $V(12) = \{(2), (3)\}$.

- Consider the ring $A = \mathbb{C}[x]$. We know that A is a principal ideal domain, i.e., all ideals are of the form (f), for $f \in A$. If $\deg(f) > 1$, then f can be factored as a product of linear terms, so that (f) is not prime. Instead, every linear polynomial $x - a$, for $a \in \mathbb{C}$, generates a maximal ideal, since $\mathbb{C}[x](x - a) \cong \mathbb{C}$ is a field. So $(x - a)$ is prime, and (0) is also prime. These are all the prime ideals of $\mathbb{C}$. Similarly to the case of $\mathbb{Z}$ above, $V(f)$ consists of the ideals generated by the linear factors of f.

Definition 2.15. For $a \in A$, we define the ***distinguished open set*** associated to a as

$$D(a) := \operatorname{Spec}(A) \setminus V(a) = \{p \in \operatorname{Spec}(A) \mid a \notin p\}.$$

Recall that a ***base*** of a topology is a family $\mathcal{B}$ of open sets such that any open set is a union of elements of $\mathcal{B}$. An example is the family of open balls in Euclidean space. A base of a topology determines the family of open sets.

Theorem 2.16. *1. For any subset $Q \subseteq A$, we have* Spec(A) $\setminus V(Q) = \bigcup_{a\in Q} D(a)$. *In particular, $\{D(a)\}_{a\in A}$ is a base of the Zariski topology of A.*

2. Spec(A) *is quasi-compact, i.e., any open cover has a finite open sub-cover.*

3. Spec(A) *is T_0, i.e., for any $p, q \in$* Spec(A)*, there is an open set U for which either $p \in U$ and $q \notin U$, or $p \notin U$ and $q \in U$.*

4. Spec(A) *is T_1 (i.e., for any $p, q \in$* Spec(A)*, there is an open set U for which $p \in U$ and $q \notin U$, or equivalently the singletons are closed sets) if and only if* Spec(A) = Max(A).

5. If $f : A \to B$ is a ring homomorphism, then the contraction map $\overline{f}$: Spec(B) → Spec(A) *is continuous, i.e., the inverse image of an open set is open, or equivalently the inverse image of a closed set is closed.*

Proof. 1. Exercise.

2. Suppose we are given an open cover $\mathrm{Spec}(A) = \bigcup_{\lambda\in\Lambda} D(a_\lambda)$. This means that, for all $p \in \mathrm{Spec}(A)$, there is some $\lambda \in \Lambda$ with $a_\lambda \notin p$, and this holds if and only if $(\{a_\lambda\}_{\lambda\in\Lambda}) = A$. Thus, for some $s_1,\dots,s_n \in A$ and some $\lambda_1,\dots,\lambda_n \in \Lambda$, we have $\sum_{i=1}^n s_i a_{\lambda_i} = 1$. Hence, $(a_{\lambda_1},\dots,a_{\lambda_n}) = A$. But then $\mathrm{Spec}(A) = D(a_{\lambda_1}) \cup \dots \cup D(a_{\lambda_n})$, and this implies the quasi-compactness of $\mathrm{Spec}(A)$.

3. For $p,q \in \mathrm{Spec}(A)$, pick an element a either from $p \setminus q$ or $q \setminus p$, and consider $D(a)$.

4. ($\Leftarrow$) For any $p \in \mathrm{Spec}(A) = \mathrm{Max}(A)$, we have $V(p) = \{p\}$, i.e., the singletons are closed.

   ($\Rightarrow$) If $\{p\} = V(I)$ for some $I \lhd A$, then p is the unique prime ideal containing I. Hence $p \in \mathrm{Max}(A)$.

5. $\overline{f}^{-1}(V(Q)) = V(f(Q))$.

□

2.2 Primary ideals

Definition 2.17. An ideal $I \lhd A$ is called a ***primary ideal*** if I is proper and for all $x,y \in A$, if $xy \in I$, then $x \in I$ or $y \in \sqrt{I}$ (equivalently, if $xy \in I$ and $x \notin I$, then $y \in \sqrt{I}$).

Proposition 2.18. *1. An ideal $I \lhd A$ is primary iff $I \neq A$ and $D(A/I) = \mathrm{nil}(A/I)$.*

2. Every prime ideal is primary.

3. The contraction of a primary ideal is primary.

4. If I is primary, then $\sqrt{I}$ is prime and it is the unique minimal prime ideal of I.

Proof. The first three parts are left as an exercise. Let us prove the last. Assume $xy \in \sqrt{I}$, which means that $(xy)^n = x^n y^n \in I$ for some n. Since I is primary, we have $x^n \in I$ or $y^n \in \sqrt{I}$. Thus, $x \in \sqrt{I}$ or $y \in \sqrt{I}$, so that $\sqrt{I}$ is indeed prime. Next, assume that $p \in \mathrm{Spec}(A)$ contains I. Then $\sqrt{I} \subseteq \sqrt{p} = p$. □

Remarks 2.19. • If $p \in \mathbb{Z}$ is a prime number, then the ideal (p^n) is primary, but it is not prime if $n > 1$.

- A power of a prime ideal might not be primary. Let $A = k[x,y,z]/(xy - z^2)$, where k is a field. Let $p = (\overline{x}, \overline{z})$. Then p is prime, since $A/p \cong k[y]$ is an integral domain. However, p^2 is not primary. Indeed, $\overline{xy} = \overline{z}^2 \in p^2$, but $x \notin p^2$ and $y^s \notin p \supset p^2$ for all s.

- A primary ideal might not be a power of a prime ideal. Let $A = k[x,y]$ and $Q = (x,y^2)$. In $A/Q \cong k[y]/(y^2)$ every zerodivisor is nilpotent, hence Q is primary. For $p = (x,y)$, we have $p^2 \subsetneq Q \subsetneq p$. If $Q = q^n$ for some prime ideal q, we would have $p = \sqrt{p^2} \subseteq \sqrt{q^n} = q \subseteq \sqrt{p} = p$, i.e., $q = p$. But Q is not a power of p.

3 Modules

Modules over rings are a generalization of vector spaces over fields.

Definition 3.1. Let A be a ring. An A-***module*** (or ***module over*** A) is a triple $(M,+,\cdot)$, where

$$+\colon M\times M\longrightarrow M \qquad \text{and} \qquad \cdot\colon A\times M\longrightarrow M$$

(called "sum" and "multiplication by scalars", respectively) satisfy the following conditions:

1. $(M,+)$ is an abelian group;
2. for all $a,b\in A$ and all $x,y\in M$, we have

   $$a(b\cdot x)=(ab)\cdot x, \qquad (a+b)\cdot x=a\cdot x+b\cdot x, \qquad a\cdot(x+y)=a\cdot x+a\cdot y, \qquad 1\cdot x=x$$

   (where $\cdot$ takes precedence over $+$ if there are no brackets).

We will usually drop the symbol $\cdot$ and simply write ax for $a\cdot x$.

Example 3.2. Given a ring A, the polynomial ring $A[x]$ is an A-module.

Definition 3.3. If M and N are A-modules, a function $f\colon M\to N$ is called a ***homomorphism of*** A-***modules*** if it satisfies the following conditions:

(i) f is a group homomorphism from $(M,+)$ to $(N,+)$;

(ii) for all $a\in A$ and $x\in M$, we have $f(a\cdot x)=a\cdot f(x)$.

We denote by $\mathrm{Mod}(A)$ the category of A-modules, where the objects are A-modules and the maps are homomorphisms of A-modules.

Examples 3.4. 1. Any ideal $I\lhd A$ is an A-module, that is, $I\in\mathrm{Mod}(A)$. In particular, a ring is a module over itself. The module-theoretic multiplication by scalars $A\times I\to I$ is the restriction of the ring-theoretic multiplication $A\times A\to A$.

2. $\mathrm{Mod}(\mathbb{Z})=\{\text{abelian groups}\}$, where the multiplication by scalars $\cdot\colon \mathbb{Z}\times G\to G$ is defined by

   $$n\cdot x:=\underbrace{x+\cdots+x}_{n\text{ times}}.$$

3. If k is a field, then $\mathrm{Mod}(k)=\{k\text{-vector spaces}\}$.

Definition 3.5. Let $(M,+,\cdot)$ be an A-module. A subset $N\subseteq M$ is a ***submodule*** of M if:

1. N is a subgroup of $(M,+)$,
2. for all $a\in A$ and all $n\in N$, we have $a\cdot n\in N$.

We will write $N\lhd M$ to say that N is a submodule of M.

Examples 3.6. • Let $f\colon M\to M'$ be a homomorphism of A-modules. Then the kernel $\ker(f):=\{x\in M\mid f(x)=0\}$ (defined as for groups) is a submodule of M, and the image of f is a submodule of M'.

- When we think of a ring A as a module over itself, the submodules of A are exactly the ideals of A.

- Consider A as a module over itself. Then all the homomorphisms of A-modules from A to A are of the form
$$\begin{aligned} A &\longrightarrow A \\ a &\longrightarrow ba, \end{aligned}$$
for a suitable fixed $b \in A$. Note that these are not ring homomorphisms in general.
- Consider the evaluation map
$$\begin{aligned} A[x] &\longrightarrow A[x] \\ f &\longrightarrow f(b), \end{aligned}$$
for a fixed $b \in A$. This is a ring homomorphism but *not* an $A[x]$-module homomorphism in general.

Remark 3.7. If M and N are A-modules, the set
$$\operatorname{Hom}(M,N) := \{\text{module homomorphisms } M \to N\}$$
has a natural A-module structure: sum and scalar multiplication are defined pointwise.

Constructions involving submodules.

Definition 3.8. Suppose $\{N_i\}_{i\in\Lambda}$ is a family of submodules of a module M. Then:

- $\bigcap_{i\in\Lambda} N_i$ is a submodule of M. This allows to define the ***submodule generated by a subset*** $S \subseteq M$, denoted $\langle S\rangle$, as the intersection of all submodules of M that contain S, namely the smallest submodule of M containing S;
- we denote by $\sum_{i\in\Lambda} N_i$ the submodule generated by $\bigcup_{i\in\Lambda} N_i$ and call it the ***sum of submodules*** $\{N_i\}_{i\in\Lambda}$. If we have $N_i \cap \sum_{j\in\Lambda\setminus\{i\}} N_j = \{0\}$ for all $i \in \Lambda$, then we call the submodule $\sum_{i\in\Lambda} N_i$ a ***direct sum***, and denote it by $\bigoplus_{i\in\Lambda} N_i$. In case the family consists of finitely many submodules $N_1,\dots,N_k$, then we write $N_1 + \cdots + N_k$ and $N_1 \oplus \cdots \oplus N_k$, respectively.

Definition 3.9. For any ideal $I \lhd A$ and any submodule $N \lhd M$, we define
$$IN := \Big\{ \sum_i a_i x_i \mid a_i \in I,\, x_i \in N \Big\} \lhd M.$$
For an element $m \in M$, we define $Am := \{am \mid a \in A\} \lhd M$.

Definition 3.10. For two submodules $N, P \lhd M$, we define $N : P := \{a \in A \mid aP \subseteq N\} \lhd A$. In particular, $\operatorname{ann}(M) := 0 : M$ is the ***annihilator of the module*** M. For an element $x \in M$, we define $\operatorname{ann}(x) := \{a \in A \mid ax = 0\} \lhd A$. This is the kernel of the module homomorphism
$$\begin{aligned} A &\longrightarrow M \\ a &\longmapsto ax. \end{aligned}$$

Definition 3.11. Let M be an A-module, and $N \lhd M$. Then one may define the ***quotient*** $M/N := \{m + N \mid m \in M\}$ as for groups (since all subgroups of an abelian group are normal). The quotient M/N is an A-module, with
$$\begin{aligned} \cdot\colon A \times M/N &\longrightarrow M/N \\ (a, \overline{m}) &\longmapsto \overline{am}, \end{aligned}$$
where we write $\overline{m}$ in place of $m + N$.

Remark 3.12. Let $M \in \mathrm{Mod}(A)$. Given any ideal $I \lhd A$, we may consider the submodule $IM = \{\sum_i a_i m_i \mid a_i \in I,\ m_i \in M\}$ of M. The quotient M/IM is an A-module, as remarked above, but it is also an A/I-module, with

$$\begin{aligned} \cdot\colon A/I \times M/IM &\longrightarrow M/IM \\ (\overline{a}, \overline{m}) &\longmapsto \overline{am}. \end{aligned}$$

Theorem 3.13 (First Isomorphism Theorem). *Let $f\colon M \to N$ be a module homomorphism. Then $M/\ker(f) \cong \mathrm{im}(f)$.*

Proof. Use the same isomorphism as for groups, by noting that it is in fact a module homomorphism. □

Lemma 3.14.

1. *For two submodules $N, P \lhd M$, we have $N : P = \mathrm{ann}((N+P)/N)$.*
2. *For two submodules $N, P \lhd M$, we have $\mathrm{ann}(N+P) = \mathrm{ann}(N) \cap \mathrm{ann}(P)$.*
3. *If an ideal $I \lhd A$ is contained in $\mathrm{ann}(M)$, then M has a natural structure of A/I-module.*
4. *(Second Isomorphism Theorem) If N_1 and N_2 are submodules of M, then*

$$(N_1 + N_2)/N_1 \cong N_2/(N_1 \cap N_2).$$

Proof. The first two parts are left as an exercise.

3. For $\overline{a} \in A/I$ and $m \in M$, define $\overline{a}m := am$. You may check that this is well-defined.
4. We have a natural map, given by the composition

$$N_2 \longrightarrow N_1 + N_2 \longrightarrow (N_1 + N_2)/N_1.$$

This map is surjective, and its kernel is $N_1 \cap N_2$.

□

3.1 Free modules

What makes vector spaces much simpler than general modules is that every non-zero element of a field is invertible. Every vector space has a basis, and in particular finitely generated vector spaces are characterized, up to isomorphism, by just one number, their *dimension* (the cardinality of any basis). This fails for modules over more general rings. The modules that do have a basis are called free modules, and every module can be "approximated" with a free module, in the sense that every module is isomorphic to a quotient of a free module.

Definition 3.15. Let $\{M_i\}_{i\in\Lambda}$ be a family of A-modules. We construct the following modules:

- the ***direct product*** $\prod_{i\in\Lambda} M_i$, which as a set is the cartesian product, equipped with component-wise operations;
- the ***direct sum*** $\bigoplus_{i\in\Lambda} M_i$, which is the submodule of the direct product consisting of the tuples where only a finite number of entries can be nonzero.

(These constructions coincide iff the set Λ is finite.) A ***free module*** is an A-module that is isomorphic to an A-module of the form $\bigoplus_{i\in\Lambda} A$, i.e., the direct sum of (possibly infinitely many) copies of the ring A.

Remark 3.16. Note that in Definitions 3.8 and 3.15 we gave two different concepts, both called "direct sum" and both represented with the symbol $\oplus$. The former definition (sometimes going by the name of "internal direct sum") is about submodules of a fixed module, whereas the latter concerns general modules. Let $\{N_i\}_{i\in\Lambda}$ be a family of submodules of a fixed $M \in \mathrm{Mod}(A)$ such that $M = \sum_{i\in\Lambda} N_i$ and the sum is "direct" in the sense of Definition 3.8. Then M is isomorphic to the direct sum $\bigoplus_{i\in\Lambda} N_i$ given in Definition 3.15.

Definition 3.17. Let A be a ring. An A-module M is ***finitely generated*** if there exist $m_1,\dots,m_k \in M$ such that $M = \langle m_1,\dots,m_k\rangle = Am_1 + \cdots + Am_k$. We write $M \in \mathrm{Mod}_S(A)$. We say that $m_1,\dots,m_k$ ***generate*** M, or that they are a ***system of generators*** for M. A system of generators is ***minimal*** if any of its proper subsets does not generate the module. A system of generators $\{m_1,\dots,m_k\}$ is a ***basis*** of M if $m_1,\dots,m_k$ are A-***linearly independent***, that is, if

$$\sum_{i=1}^{k} a_i m_i = 0 \qquad \text{implies} \qquad a_1 = a_2 = \cdots = a_k = 0,$$

for coefficients $a_i \in A$. If a system of generators is infinite, for it to be a basis we require that any *finite* subset of it is linearly independent.

Lemma 3.18. *For $M \in \mathrm{Mod}(A)$, the following are equivalent:*

(a) $B \subset M$ is a basis of M;

(b) for every $N \in \mathrm{Mod}(A)$ and every function $f\colon B \to N$, there exists a unique module homomorphism $\overline{f} \in \mathrm{Hom}(M,N)$ that makes the diagram

$$\begin{tikzcd}
B \arrow[d, hook] \arrow[dr, "f"] & \\
M \arrow[r, dashed, "\overline{f}"'] & N
\end{tikzcd}$$

commute, where the vertical map $B \hookrightarrow M$ is the inclusion;

(c) $M = \bigoplus_{b\in B} Ab$ and $\mathrm{ann}(b) = \{0\}$ for all $b \in B$.

Lemma 3.19. *1. Every non-empty set can be the basis of some A-module.*

2. A module is free if and only if it has a basis.

The (proof of the) following lemma stands at the base of the whole idea of a free resolution (which we will see in Lecture 5).

Lemma 3.20 (Important). *Every A-module is a quotient of some free A-module.*

Proof. Exercise. Use the first isomorphism theorem. □

Theorem 3.21. *1. Every two bases of a free A-module have the same cardinality (and this cardinality is called the **rank** of the module).*

2. Two free A-modules are isomorphic if and only if they have the same rank.

Proof. For the first statement, let $B \subset M$ be a basis of a free module M. Let $\mathfrak{m}$ be a maximal ideal of A. The set $\{b + \mathfrak{m}M \mid b \in B\}$ has the same cardinality as B and is a basis of the $A/\mathfrak{m}$-vector space $M/\mathfrak{m}M$. Hence $\#B = \dim_{A/\mathfrak{m}} M/\mathfrak{m}M$. The second statement is left as an exercise. □

Definition 3.22. For any ring R, let $M_{m,n}(R)$ be the free R-module of matrices with m rows, n columns and entries in R. We have $M_{m,n}(R) \cong R^{m \cdot n}$. Write $M_n(R) := M_{n,n}(R)$.

Remarks 3.23.

- An element of $M_{n,m}(R)$ gives a module homomorphism

$$\begin{aligned} f_A \colon R^m &\longrightarrow R^n \\ b &\longmapsto Ab. \end{aligned}$$

- For matrices over R we still have the "determinant formula" $\det(AB) = \det(A)\det(B)$ and the Laplace expansion (along rows or columns).

Let $A \in M_n(R)$. Recall that the ***adjugate*** (or ***adjunct matrix***) of A, denoted A^{adj}, is the square matrix that in position (i,j) has the determinant of the square submatrix obtained from A by deleting the i-th column and the j-th row, multiplied by $(-1)^{i+j}$.

Theorem 3.24 (Cramer)**.** *For all $A \in M_n(R)$,*

$$AA^{\mathrm{adj}} = A^{\mathrm{adj}}A = \det(A)I_n,$$

where I_n is the $n \times n$ identity matrix.

An immediate consequence of this theorem is that if $\det(A)$ is an invertible element of the ring R, then A is invertible in $M_n(R)$. The converse is also true, for instance by the determinant formula.

Theorem 3.25 (McCoy)**.** *Let $A \in M_{n,m}(R)$. The map f_A is injective if and only if $n \geq m$ and 0 is the only element annihilating all $m \times m$ minors of A.*

Proof. ($\Leftarrow$) Suppose $Ab = 0$ for some $b \in R^m$. Let $\widetilde{m} := \det(\widetilde{A})$ be any minor. Then $\widetilde{A}b = 0$. By Cramer's theorem, $\widetilde{m}b = 0$. By assumption, $b = 0$.

($\Rightarrow$) Assume first that $m \leq n$. Suppose that $a \in R$ annihilates all $m \times m$ minors of A. We prove by downwards induction that for $k = m, \dots, 1$ we have the following: a annihilates all $k \times k$ minors of A. The first case of the induction is exactly our assumption. Next, suppose that a annihilates all $(k+1) \times (k+1)$ minors of A. Fix a $k \times k$ submatrix M in a $k \times (k+1)$ submatrix M'. Let M'_j be the matrix obtained from M' by removing the j-th column. In particular, $M'_{k+1} = M$. Denote

$$b := a \begin{pmatrix} \det(M'_1) \\ -\det(M'_2) \\ \vdots \\ (-1)^{k+1} \det(M'_{k+1}) \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Denoting by $a_{i,j}$ the (i,j)-entry of A, we have

$$(Ab)_i = \sum_{j=1}^{k+1} (-1)^j a_{i,j} (a \det(M'_j)) = (-1)^{k+1} a \det \begin{pmatrix} a_{1,1} & \cdots & a_{1,k+1} \\ \vdots & \ddots & \vdots \\ a_{k,1} & \cdots & a_{k,k+1} \\ a_{i,1} & \cdots & a_{i,k+1} \end{pmatrix}.$$

The right-hand side is zero for $i = 1, \dots, k$. Also, it is zero for $i = k+1, \dots, n$ by the induction hypothesis. Hence, $Ab = 0$, so that $b = 0$. In particular, $a\det(M) = a\det(M'_{k+1}) = 0$. Applying the claim for $k = 1$, we obtain that $aA = 0$, hence $A\begin{pmatrix} a \\ \vdots \\ a \end{pmatrix} = 0$, so that $a = 0$.

Assume now, by contradiction, that $m > n$. Then the matrix

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \in M_m(R)$$

defines an injective matrix. Its determinant is equal to zero, which contradicts the previously proven statement. Hence, we must have $n \geq m$. □

Theorem 3.26. *Let A be a ring.*

1. *If M and N are free A-modules and $f \colon M \to N$ is a surjective homomorphism, then* $\operatorname{rk}(M) \geq \operatorname{rk}(N)$.
2. *If M is a free A-module, $L \subset M$ is A-linearly independent, and $G \subset M$ generates M, then $\#L \leq \#G$.*
3. *If M and N are free A-modules and $f \colon M \to N$ is injective, then* $\operatorname{rk}(M) \leq \operatorname{rk}(N)$. *(In particular, if $A^m \to A^n$ is injective, then $m \leq n$.)*
4. *If M is a free A-modules and N is a free submodule of M, then* $\operatorname{rk}(N) \leq \operatorname{rk}(M)$.

Proof. 1. Let $\mathfrak{m} \in \operatorname{Max}(A)$ and let

$$\begin{aligned} \overline{f} \colon M/\mathfrak{m}M &\longrightarrow N/\mathfrak{m}N \\ a + \mathfrak{m}M &\longmapsto f(a) + \mathfrak{m}N. \end{aligned}$$

The map $\overline{f}$ is a surjective map of $A/\mathfrak{m}$-vector spaces. Hence, $\operatorname{rk}(M) = \dim(M/\mathfrak{m}M) \geq \dim(N/\mathfrak{m}N) = \operatorname{rk}(N)$.

2. *Case 1:* Let B be a basis of M. As in the previous point, we may show that $\#B \leq \#G$.

   Case 2: If B is finite, then we have $\#L \leq \#B$ by McCoy's theorem.

   Case 3: Assume B is infinite. A basic fact from set theory is that an infinite set has the same cardinality as the family of its finite subsets. Moreover, it also has the same cardinality if each finite subset is counted finitely many (or countably many) times. Clearly each element $\ell \in L$ gives a finite subset $b_\ell \subseteq B$ (consisting of the elements that appear in the basis presentation), and this subset appears at most $\#b_\ell$ times (by Case 2). Hence, $\#L \leq \#B$.

The remaining two points are left as an exercise. □

Remark 3.27. A submodule of a finitely generated module may not be finitely generated. Consider for instance a polynomial ring $A = k[x_1, x_2, \dots,]$ in infinitely many variables (which is finitely generated as an A-module by the polynomial 1), and the ideal $(x_1, x_2, \dots)$.

4 Graded rings and modules, and Nakayama's lemma

Definition 4.1. Let A be a ring. We call A a ***graded ring*** if there is a family $\{A_k\}_{k\in\mathbb{Z}}$ of (additive) subgroups of A satisfying the following conditions:

1. $A = \bigoplus_{k\in\mathbb{Z}} A_k$ as abelian groups—this means that $A = \sum_{k\in\mathbb{Z}} A_k$ and $A_i \cap \sum_{k\in\mathbb{Z}\setminus\{k\}} A_k = \{0\}$ for all $i \in \mathbb{Z}$, so that every element $a \in A$ has a unique decomposition $a = \sum_{k\in\mathbb{Z}} a_k$, where $a_k \in A_k$ for all indices k, and $a_k = 0$ for all but a finite number of indices k—, and

2. for all $i, j \in \mathbb{Z}$, we have $A_i A_j \subseteq A_{i+j}$.

The elements of A_k are called ***homogeneous elements of degree*** k. If we write $a = \sum_{k\in\mathbb{Z}} a_k$, where $a_k \in A_k$, the elements a_k are called the ***homogeneous components*** of a.

Remark 4.2. Sometimes it is natural to assume that $A_k = \{0\}$ for all $k < 0$, in which case we write $A = \bigoplus_{k\in\mathbb{N}} A_k$. We may call such graded rings "$\mathbb{N}$-graded", as opposed to "$\mathbb{Z}$-graded". Sometimes one also uses different kinds of gradings, for instance indexing the subgroups over $\mathbb{Z}_2$ or $\mathbb{Z}^n$, or over a general semigroup S.

Example 4.3. Let $A = R[x_1, \ldots, x_n]$ be the polynomial ring with coefficients in a ring R. Then A is "canonically" a graded ring, with A_k consisting of the homogeneous polynomials of degree k. However, there are other ways of grading A: fix $(a_1, \ldots, a_n) \in \mathbb{Z}^n_{>0}$, and let

$$A_k := \left\{ \sum_{\substack{\sum_{i=1}^n a_i b_i = k \\ b_i \in \mathbb{N}}} c_{b_1,\ldots,b_n} x_1^{b_1} \cdots x_n^{b_n} \right\}.$$

By choosing $a_1 = \cdots = a_n = 1$, we get the "canonical" grading, called ***standard grading***.

Lemma 4.4. *In any graded ring $A = \bigoplus_{k\in\mathbb{Z}} A_k$, the subgroup A_0 is a subring of A, and $1_A \in A_0$.*

Proof. By definition of graded ring, $A_0 A_0 \subseteq A_{0+0}$. Let us show that $1 = 1_A \in A_0$. We may decompose $1 = \sum_{k\in\mathbb{Z}} a_k$ into homogeneous components, with $a_k \in A_k$. Suppose b is a homogeneous element. We have $b = b1 = \sum_k b a_k$, so that $b = b a_0$. But then $c = c a_0$ for any $c \in A$, in particular for $c = 1$, so that $1 = a_0$. □

Proposition 4.5. *Let $A = \bigoplus_{k\in\mathbb{Z}} A_k$ be a graded ring. For an ideal $I \lhd A$, the following are equivalent:*

1. *the ideal I is generated by homogeneous elements,*

2. *if $a \in I$ and $a = \sum_{k\in\mathbb{Z}} a_k$ is the decomposition into homogeneous elements, then $a_k \in I$ for all $k \in \mathbb{Z}$.*

*An ideal satisfying these conditions is called a **homogeneous (or graded) ideal.***

Proof. ($1 \Rightarrow 2$) Suppose $I = (b_\lambda \mid \lambda \in \Lambda)$, where each b_λ is a homogeneous element of degree d_λ. Let $a = \sum_{i=1}^n b_{\lambda_i} r_{\lambda_i}$. Decompose $r_{\lambda_i} = \sum_{k\in\mathbb{Z}} r_{\lambda_i}^{(k)}$ into homogeneous components. Then $a = \sum_k a_k$, where $a_k = r_{\lambda_1}^{(k-d_{\lambda_1})} b_{\lambda_1} + \cdots + r_{\lambda_n}^{(k-d_{\lambda_n})} b_{\lambda_n}$ is the homogeneous component of degree k. Clearly $a_k \in I$.

($2 \Rightarrow 1$) We may take any generators and decompose them into homogeneous components. □

Lemma 4.6. *Let $A = \bigoplus_{k\in\mathbb{Z}} A_k$ be a graded ring, and let $I \lhd A$ be a homogeneous ideal. For all $k \in \mathbb{Z}$, denote $I_k := A_k \cap I$. Then A/I is a graded ring, with $(A/I)_k = A_k/I_k$.*

Corollary 4.7. *For any homogeneous ideals I and J of a graded ring A, we have:*

1. *If I is finitely generated, then I has a finite set of homogeneous generators.*
2. *The ideals $I+J$, IJ, $I \cap J$ and $I : J$ are homogeneous.*
3. *The image (along the projection map) of a homogeneous ideal of A is homogeneous in A/I. The inverse image of a homogeneous ideal of A/I is a homogeneous ideal of A.*

Lemma 4.8. *Let A be a graded ring, and let $p \in \operatorname{Spec}(A)$. Let p^* be the ideal of A generated by all the homogeneous elements in p. Then $p^* \in \operatorname{Spec}(A)$.*

Proof. Suppose $a, b \in A$ are such that $ab \in p^*$. We may decompose $a = \sum_i a_i$ and $b = \sum_i b_i$, for $a_i, b_i \in A_i$. By contradiction, assume that $a, b \notin p^*$. There exist minimal indices i_0 and j_0 such that $a_{i_0} \notin p^*$ and $b_{j_0} \notin p^*$. Since p^* is a homogeneous ideal, the homogeneous component of ab of degree $i_0 + j_0$, which is equal to $\sum_{\alpha+\beta=i_0+j_0} a_\alpha b_\beta$, is in p^*. By definition of i_0 and j_0, we conclude that $a_{i_0} b_{j_0} \in p^* \subseteq p$. Hence, $a_{i_0} \in p$ or $b_{j_0} \in p$. Thus, $a_{i_0} \in p^*$ or $b_{j_0} \in p^*$, which is a contradiction. □

Corollary 4.9. *Let A be a graded ring, and let $I \lhd A$ be a homogeneous ideal.*

1. *All minimal prime ideals of I are homogeneous.*
2. *We have*

$$\sqrt{I} = \bigcap_{\substack{p \in \operatorname{Spec}(A), \\ p \text{ homogeneous}, \\ p \supseteq I}} p.$$

In particular, $\operatorname{nil}(A)$ *is homogeneous and* A_{red} *is a graded ring.*

Proof. 1. If $p \in \operatorname{Spec}(A)$ is minimal for I, then, by Lemma 4.8, the ideal p^* is homogeneous, prime and such that $I \subseteq p^* \subseteq p$. Therefore $p = p^*$.

2. Follows from the previous part.

□

Definition 4.10. Let $A = \bigoplus_{k \in \mathbb{N}} A_k$ be a graded ring. Denote $A_+ := \bigoplus_{k>0} A_k$. Then A_+ is called the ***irrelevant ideal*** of A. We define the ***projective spectrum*** of A as

$$\operatorname{Proj}(A) := \{p \in \operatorname{Spec}(A) \mid p \text{ is homogeneous and } A_+ \not\subset p\}.$$

Remarks 4.11.

- The irrelevant ideal A_+ is an ideal.
- We consider the subspace topology on $\operatorname{Proj}(A)$, induced by the Zariski topology on $\operatorname{Spec}(A)$. A subset $F \subseteq \operatorname{Proj}(A)$ is closed if and only if there exists a homogeneous ideal $I \lhd A$ such that F is the set of all homogeneous prime ideals that contain I and do not contain A_+.

Definition 4.12. Let $A = \bigoplus_k A_k$ and $B = \bigoplus_k B_k$ be graded rings. We call a ring homomorphism $f : A \to B$ a ***graded homomorphism*** if $f(A_k) \subseteq B_k$ for all k, that is, if f preserves the degrees of the homogeneous elements.

Definition 4.13. Let $A = \bigoplus_{k \in \mathbb{Z}}$, and let M be an A-module. We call M a ***graded module*** if there is a family $\{M_k\}_{k \in \mathbb{Z}}$ of subgroups of M satisfying the following conditions:

1. $M = \bigoplus_{k \in \mathbb{Z}} M_k$ as abelian groups,

2. for all $i, j \in \mathbb{Z}$, we have $A_i M_j \subseteq M_{i+j}$.

If $M_k = \{0\}$ for all $k < 0$, we say M is ***positively graded***. The elements of M_k are called ***homogeneous elements of degree*** k. Every element $m \in M$ has a unique decomposition $m = \sum_{k\in\mathbb{Z}} m_k$, where $m_k \in M_k$, and $m_k \neq 0$ for a finite number of indices k. The elements m_k are called the ***homogeneous components*** of m.

Remark 4.14. Each M_k is an A_0-module.

4.1 Nakayama's lemma

For the rest of the section, A will be any ring, not necessarily graded. Recall that $\mathrm{Mod}_S(A)$ denotes the set of finitely generated A-modules, and $J(A)$ is the Jacobson radical of A, i.e., the intersection of all maximal ideals of A.

Lemma 4.15 (Nakayama). *1. Let $M \in \mathrm{Mod}_S(A)$ and $I \lhd A$ be such that $IM = M$. Then there exists $x \in I$ such that $(1+x)M = 0$.*

2. Let $M \in \mathrm{Mod}_S(A)$ and $I \lhd A$ be such that $I \subseteq J(A)$ and $IM = M$. Then $M = 0$.

3. Let $M \in \mathrm{Mod}(A)$, $N \lhd M$ and $I \lhd A$ be such that $I \subseteq J(A)$ and $M = N + IM$. Then $M = N$.

Proof. 1. Suppose $M = Am_1 + \cdots + Am_n$. Since $M \subseteq IM$, we have $m_i = \sum_{j=1}^n a_{ij} m_j$, for some $a_{ij} \in I$. Consider the matrices $Q = (a_{ij})$ and $C = I_n - Q$. By Cramer's theorem, $(\det C) m_j = 0$ for all $j \in \{1, \ldots, n\}$. We have $\det C = 1 + x$, for $x \in I$.

2. By the previous point, we have $(1+x)M = 0$ for some $x \in I \subseteq J(A)$. Hence $1 + x \in \mathcal{U}(A)$, and $M = 0$. Alternatively, one can prove this by induction on the number of generators of M.

3. Observe that

$$M/N = (N + IM)/N = (IM)/N = I(M/N),$$

and conclude by the previous point.

□

Theorem 4.16. *Let M be a finitely generated module and $f\colon M \to M$ be a surjective homomorphism. Then f is an isomorphism.*

Proof. Consider M as an $A[x]$-module, where $xm := f(m)$. By assumption, we have $(x)M = M$, so that by Nakayama's lemma there exists $P \in A[x]$ such that $(1+xP)M = 0$. For $u \in \ker(f)$, we have $0 = (1+xP)u = u + f(u)P = u$. □

Theorem 4.17. *Let $(A, \mathfrak{m}, k)$ be a local ring and $M \in \mathrm{Mod}_S(A)$. Let $\overline{M} := M/\mathfrak{m}M$, and $n := \dim_k \overline{M}$. Then:*

1. If $\{\overline{u_1}, \ldots, \overline{u_n}\}$ is a basis of $\overline{M}$ over k for some $u_1, \ldots, u_n \in M$, then $\{u_1, \ldots, u_n\}$ is a minimal system of generators of M.

2. Every minimal system of generators of M has n elements (and is achieved as in part 1).

3. If $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ are two minimal systems of generators of M and $v_i = \sum_{j=1}^n a_{ij} u_j$ for some $a_{ij} \in A$, then $\det(a_{ij}) \in \mathcal{U}(A)$, i.e., the matrix $(a_{ij}) \in M_n(A)$ is invertible.

Proof.

1. Let $N = Au_1 + \cdots + Au_n$. The natural composition $N \to M \to M/\mathfrak{m}M$ of inclusion and projection is surjective. Hence, $N + \mathfrak{m}M = M$. By Nakayama's lemma, we have $M = N$. The minimality follows from the fact that $\overline{u_1}, \ldots, \overline{u_n}$ is a basis.

2. If $\{u_1, \ldots, u_m\}$ is a minimal system of generators, then $\{\overline{u_1}, \ldots, \overline{u_m}\}$ generates $\overline{M}$ and is linearly independent. Therefore, $m = n$.

3. Let $\overline{a_{ij}}$ be the image of a_{ij} in $\overline{M}$. We have $\overline{v_i} = \sum_j \overline{a_{ij}} \cdot \overline{u_j}$ in $\overline{M}$. Thus the coefficients $\overline{a_{ij}}$ constitute a change of basis, and $\overline{a_{ij}} \in k \setminus \{0\}$. Since $\overline{\det((a_{ij}))} = \det((\overline{a_{ij}}))$, we have $\det((a_{ij})) \notin \mathfrak{m}$. Thus, $\det((a_{ij}))$ is invertible in A. Hence the matrix (a_{ij}) is invertible.

□

The following is the "graded version" of Nakayama's lemma.

Lemma 4.18 (Nakayama)**.** *Let $A = \bigoplus_{k \in \mathbb{Z}_{\geq 0}} A_k$ be a graded ring and consider the irrelevant ideal $A_+ = \bigoplus_{k \in \mathbb{Z}_{>0}} A_k$. Let M be a finitely generated graded A-module such that $A_+M = M$. Then $M = 0$.*

5 Exact sequences and resolutions

Definition 5.1. A sequence of A-module homomorphisms

$$\dots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \dots$$

is said to be ***exact at*** M_i if $\operatorname{im}(d_{i+1}) = \ker(d_i)$. The whole sequence is called an ***exact sequence*** if it is exact at every module.

We will consider both infinite and finite exact sequences. For finite sequences, we will not talk about exactness at the first and last module of the sequence, since there is only one map involved there.

Examples 5.2.

1. The sequence $M \xrightarrow{f} N \to 0$ is exact (which in this case just means exact at N) if and only if f is surjective.
2. The sequence $0 \to M \xrightarrow{f} N$ is exact if and only if f is injective.
3. An exact sequence of the form $0 \to M_1 \to M_2 \to M_3 \to 0$, with precisely three modules between two zero modules, is called a ***short exact sequence***.
4. For $M \in \operatorname{Mod}(A)$, the following are equivalent:
   - M is finitely generated;
   - M is (isomorphic to) a quotient of $A^q := \bigoplus_{i=1}^q A$, for some $q \in \mathbb{N}$;
   - there exists an exact sequence of the form $A^q \to M \to 0$, for some $q \in \mathbb{N}$.

Definition 5.3. An A-module M is ***finitely presented*** (or ***has finite presentation***) if there exists an exact sequence of the form $A^p \to A^q \to M \to 0$, for some $p, q \in \mathbb{N}$.

More explicitly, M is finitely presentend if the following conditions are satisfied:

- M is finitely generated, with $M = Am_1 + \dots + Am_q$ for some $m_1, \dots, m_q$, and
- the module

$$\left\{(a_1, \dots, a_q) \in A^q \mid \sum_{i=1}^q a_i m_i = 0\right\}$$

(which is the kernel of $A^q \to M$) is finitely generated (by p elements).

Remark 5.4. With the notation of Definition 5.1, the exactness at M_i implies that the composition $d_i \circ d_{i+1} \colon M_{i+1} \to M_{i-1}$ is the zero homomorphism. A sequence of homomorphisms satisfying this weaker condition at every module is called a ***chain complex***. This is equivalent to having $\operatorname{im}(d_{i+1}) \subseteq \ker(d_i)$ for all i, not necessarily with equality. One defines the ***i-th homology*** of the chain complex to be the quotient $H_i := \ker(d_i)/\operatorname{im}(d_{i+1})$. These quotients measure "how far" the chain complex is from being exact: in particular, it is exact if and only if $H_i = 0$ for all i.

Recall that the set $\operatorname{Hom}(M, N)$ of A-module homomorphisms has itself an A-module structure, by pointwise addition and multiplication by scalars. When we fix one "entry" of $\operatorname{Hom}(M, N)$, we get functors in the following way. (Knowing functors beforehand is not necessary for this course, as we will only see very few functors, and all of the algebraic kind. If you never heard of functors and categories, you may have a look at Appendix C.)

Definition 5.5. Let P be a fixed A-module. We define functors $\mathrm{Hom}(P,-)$ and $\mathrm{Hom}(-,P)$: to each module M, the former associates $\mathrm{Hom}(P,M)$ and the latter $\mathrm{Hom}(M,P)$. These functors also take as input homomorphisms and return homomorphisms. Schematically:

$$\begin{tikzcd}
\mathrm{Mod}(A) \arrow[rr, "\mathrm{Hom}(P,-)"] & & \mathrm{Mod}(A) & & \mathrm{Mod}(A) \arrow[rr, "\mathrm{Hom}(-,P)"] & & \mathrm{Mod}(A) \\
M \arrow[d, "f"'] \arrow[r, phantom, "\mapsto"] & {} & \mathrm{Hom}(P,M) \arrow[d, "f\circ-"'] & & M \arrow[d, "f"'] \arrow[r, phantom, "\mapsto"] & {} & \mathrm{Hom}(M,P) \\
N \arrow[r, phantom, "\mapsto"] & {} & \mathrm{Hom}(P,N), & & N \arrow[r, phantom, "\mapsto"] & {} & \mathrm{Hom}(N,P). \arrow[u, "-\circ f"']
\end{tikzcd}$$

Exercise 5.6. Let $P \in \mathrm{Mod}(A)$. Show the following:

1. For $f \in \mathrm{Hom}(M,N)$, the map $(f \circ -)\colon \mathrm{Hom}(P,M) \to \mathrm{Hom}(P,N)$ that associates to each $g \in \mathrm{Hom}(P,M)$ the composition $f \circ g$ is a module homomorphism. Similarly for $- \circ f$.

2. If $\ldots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \ldots$ is a chain complex, meaning that $\mathrm{im}(d_{i+1}) \subseteq \ker(d_i)$ for all i, then
$$\ldots \longrightarrow \mathrm{Hom}(P,M_{i+1}) \xrightarrow{d_{i+1}\circ -} \mathrm{Hom}(P,M_i) \xrightarrow{d_i\circ -} \mathrm{Hom}(P,M_{i-1}) \longrightarrow \ldots$$
and
$$\ldots \longrightarrow \mathrm{Hom}(M_{i-1},P) \xrightarrow{-\circ d_i} \mathrm{Hom}(M_i,P) \xrightarrow{-\circ d_{i+1}} \mathrm{Hom}(M_{i+1},P) \longrightarrow \ldots$$
are chain complexes.

3. The functors $\mathrm{Hom}(P,-)$ and $\mathrm{Hom}(-,P)$ are "left-exact functors", that is, if $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ is an exact sequence, then
$$0 \longrightarrow \mathrm{Hom}(P,M_1) \xrightarrow{f\circ -} \mathrm{Hom}(P,M_2) \xrightarrow{g\circ -} \mathrm{Hom}(P,M_3)$$
and
$$0 \longrightarrow \mathrm{Hom}(M_3,P) \xrightarrow{-\circ g} \mathrm{Hom}(M_2,P) \xrightarrow{-\circ f} \mathrm{Hom}(M_1,P)$$
are exact sequences.

4. Give an example where the functor $\mathrm{Hom}(P,-)$ does not preserve surjectivity.

5.1 Projective modules

Definition 5.7. Let A be a ring. An A-module P is called a ***projective module*** if for any two A-modules M and N, and for any surjective homomorphism $f\colon M \to N$ and any homomorphism $g\colon P \to N$, there exists a homomorphism $h\colon P \to M$ that makes the diagram

$$\begin{tikzcd}
 & P \arrow[d, "g"] \arrow[dl, dashed, "h"'] \\
M \arrow[r, two heads, "f"'] & N
\end{tikzcd}$$

commute, i.e., such that $g = f \circ h$.

Remarks 5.8.

- **Free modules are projective:** If P is a free module with basis $\{e_i\}_{i\in\Lambda}$, then any choice of elements $m_i \in M$, for $i \in \Lambda$, determines a unique $h\colon P \to M$, defined by $h(e_i) := m_i$. And one may pick m_i such that $f(m_i) = g(e_i)$.

- In some books, the diagram in the definition of a projective module is drawn as

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "h"'] \arrow[d, "g"] & \\
M \arrow[r, "f"'] & N \arrow[r] & 0,
\end{tikzcd}$$

and the surjectivity of f is phrased as exactness of the horizontal sequence.

Definition 5.9. A submodule $M_0 \lhd M$ is called a ***direct summand*** of M if there exists a submodule $M_1 \lhd M$ such that $M = M_0 \oplus M_1$.

Proposition 5.10. *For an A-module P, the following are equivalent:*

1. *P is projective;*

2. *P is a direct summand of a free A-module.*

Proof. Exercise. □

Examples 5.11.

- *A projective module that is not free.* Consider the ring $A := \mathbb{Z}\times\mathbb{Z}$, with component-wise operations, and the A-modules $P_1 := \mathbb{Z}\times(0)$ and $P_2 := (0)\times\mathbb{Z}$. Since $P_1 \oplus P_2 \cong A$, and A is a free A-module, P_1 is a projective A-module. But since $(0,x)\cdot P_1 = 0$ for all $x \in \mathbb{Z}$, the A-module P_1 is not free.

- The $\mathbb{Z}$-modules $\mathbb{Q}$ and $\mathbb{Z}/2\mathbb{Z}$ are not projective.

Recall that a matrix Q in the (non-commutative) ring $M_n(A)$ of $n\times n$ matrices with entries in A defines a homomorphism $f_Q\colon A^n \to A^n$, by setting $v \mapsto Qv$, for any column vector $v \in A^n$. A ***projection*** is a matrix Q that satisfies $Q^2 = Q$, or equivalently $f_Q \circ f_Q = f_Q$.

Proposition 5.12. *For a finitely generated A-module P, the following are equivalent:*

1. *P is projective;*

2. *P is the "image of a projection", i.e., there exist $n \in \mathbb{N}$ and $Q \in M_n(A)$ such that $Q^2 = Q$ and $P \cong f_Q(A^n)$.*

Proof. Exercise. □

Proposition 5.13. *For an A-module P, the following are equivalent:*

1. *P is projective;*

2. *the functor* $\mathrm{Hom}(P,-)$ *is an "exact functor", that is, if* $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ *is an exact sequence, then*

$$0 \longrightarrow \mathrm{Hom}(P,M_1) \xrightarrow{f\circ -} \mathrm{Hom}(P,M_2) \xrightarrow{g\circ -} \mathrm{Hom}(P,M_3) \longrightarrow 0$$

is an exact sequence.

Proof. Exercise. (Compare this with the left-exactness in Exercise 5.6.) □

We conclude this subsection by observing that, in the cases we are interested in the most in this course, the concepts of projective module and free module coincide.

Theorem 5.14 (Kaplansky). *Every projective module over a local ring is free.*

Proof for finitely generated modules. Suppose that M is a finitely generated projective module over a local ring $(A, \mathfrak{m}, k)$.

First, we show that there exists a finitely generated module N such that $M \oplus N = A^n$. We know that there exists N' such that $M \oplus N' = F$, where F is free, that is, F has a basis $(e_\lambda)_{\lambda \in \Lambda}$. We fix a finite set $L \subseteq \Lambda$ such that $M \subseteq F_0 := \bigoplus_{\lambda \in L} Ae_\lambda$. Then $F_0 = M + (N' \cap F_0)$, and actually $F_0 = M \oplus (N' \cap F_0)$. Since $N := N' \cap F_0 = F_0/M$, we know that N is finitely generated.

Now let $e_1, \dots, e_n$ be a basis of $M \oplus N$. We have $\overline{M} \oplus \overline{N} = k^n$, and there exist bases $\overline{b_1}, \dots, \overline{b_m}$ of $\overline{M}$ and $\overline{b_{m+1}}, \dots, \overline{b_n}$ of $\overline{N}$. We may write $b_i = \sum_{j=1}^n b_{ij} e_j$ for all i. We know that $\det((b_{ij})) \notin \mathfrak{m}$ (since after reduction this is a change-of-basis matrix), so (b_{ij}) is invertible. Hence, $b_1, \dots, b_n$ is a basis for $M \oplus N$. Thus $b_1, \dots, b_m$ is a basis for M. □

The following was a long-standing conjecture by Serre, settled independently by Quillen and Suslin:

Theorem 5.15 (Quillen–Suslin). *Let k be a field. Every finitely generated projective module over a polynomial ring $k[x_1, \dots, x_n]$ is free.*

5.2 Resolutions

Definition 5.16. Let A be a ring and $M \in \operatorname{Mod}(A)$. A ***resolution of*** M is an exact sequence of A-modules of the form

$$\dots \longrightarrow F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \longrightarrow 0.$$

If all the modules F_i are projective, this is called a ***projective resolution***. If all the modules F_i are free (so that they are in particular projective), this is called a ***free resolution***.

Remarks 5.17.

- In particular, the exactness at M means that the map d_0 is surjective.

- Some authors prefer to remove the module M from the resolution, starting from F_0 instead, or refer to what we call a resolution above as an "augmented resolution".

- **How to construct free resolutions.** The resolutions we will be interested in are free resolutions. They can be built as follows. If $\{m_i \mid i \in \Lambda_0\}$ is a system of generators of M, let $F_0 := \bigoplus_{i \in \Lambda_0} A$, and let $\{e_i \mid i \in \Lambda_0\}$ be a basis of F_0. The map

  $$\begin{aligned} d_0 \colon F_0 &\longrightarrow M \\ e_i &\longmapsto m_i \end{aligned}$$

  is a surjection, and by the first isomorphism theorem one has

  $$F_0/\ker(d_0) \cong M.$$

  Now, the map d_0 might also be injective, which happens if and only if $\ker(d_0) = 0$. In this case the module M is actually isomorphic to F_0 via d_0, which means that M is free and there are no non-trivial relations among the generators of M. If otherwise $\ker(d_0)$ is a non-zero module, let $\{g_i \mid i \in \Lambda_1\}$ be a system of generators of $\ker(d_0)$, describing the relations among the generators of M. Define then the next module in the resolution as $F_1 := \bigoplus_{i\in\Lambda_1} A$, and the map

$$\begin{aligned} d_1\colon F_1 &\longrightarrow F_0 \\ \eta_i &\longmapsto g_i, \end{aligned}$$

where $\{\eta_i \mid i \in \Lambda_1\}$ is a basis of the free module F_1. Then by construction one has $\operatorname{im}(d_1) = \ker(d_0)$, and again by the first isomorphism theorem

$$F_1/\ker(d_1) \cong \ker(d_0).$$

There are two cases again: if $\ker(d_1) = 0$, then the module $\ker(d_0)$ is free, isomorphic to F_1, and this is a satisfactory description of it; if otherwise $\ker(d_1) \neq 0$, then we keep going, constructing a free module F_2 with as many generators as $\ker(d_1)$ and a map $d_2\colon F_2 \to F_1$ that surjects onto $\ker(d_1)$. And so on… More schematically:

$$\begin{tikzcd}
\cdots \arrow[r] & F_3 \arrow[rr, "d_3"] \arrow[dr] & & F_2 \arrow[rr, "d_2"] \arrow[dr] & & F_1 \arrow[rr, "d_1"] \arrow[dr] & & F_0 \arrow[r, two heads, "d_0"] & M. \\
& & \ker(d_2) \arrow[ur, hook] & & \ker(d_1) \arrow[ur, hook] & & \ker(d_0) \arrow[ur, hook] & &
\end{tikzcd}$$

- In the setting of $k[x_1,\dots,x_n]$-modules, there are indeed algorithms to compute kernels, implemented in several computer algebra systems.
- If M is a finitely generated $k[x_1,\dots,x_n]$-module, the free modules F_i constructed at each step are themselves finitely generated, and if one considers systems of generators that are not redundant, then the procedure described above to construct a free resolution of M ends after a finite number of steps—that is, $F_i = 0$ for $i \gg 0$. These results were proven by Hilbert, and we will discuss at least part of them in Lectures 7 and 11.

Example 5.18. Let $A = k[x,y,z]$ and $I = (x^2, xy, y^3) \lhd A$. One may check that the sequence

$$0 \longrightarrow A^2 \xrightarrow{\begin{bmatrix} y & 0 \\ -x & y^2 \\ 0 & -x \end{bmatrix}} A^3 \xrightarrow{\begin{bmatrix} x^2 & xy & y^3 \end{bmatrix}} I \longrightarrow 0$$

is a free resolution of the A-module I, where matrices represent A-module homomorphisms as recalled before Proposition 5.12.

5.3 Injective modules

Consider the definition of a projective module with the diagram written in the second item of Remarks 5.8. By inverting all arrows, we get the "dual diagram"

$$\begin{tikzcd}
& P & \\
M \arrow[ur, dashed, "h"] & N \arrow[l, "f"] \arrow[u, "g"'] & 0. \arrow[l]
\end{tikzcd}$$

The assumption that the horizontal sequence is exact (at N) means that now f is injective. This gives us the following definition of an injective module, which is the dual concept to a projective module:

Definition 5.19. Let A be a ring. An A-module E is called an ***injective module*** if for any two A-modules M and N, and for any injective homomorphism $f\colon N \to M$ and any homomorphism $g\colon N \to E$, there exists a homomorphism $h\colon M \to E$ that makes the diagram

$$\begin{tikzcd}
& E \\
M \arrow[ur, dashed, "h"] & N \arrow[l, "f"] \arrow[u, "g"']
\end{tikzcd}$$

commute, i.e., such that $g = h \circ f$.

Similarly to the case of projective modules in Proposition 5.20, one may characterize injective modules in terms of exactness of a Hom-functor (the other one):

Proposition 5.20. *For an A-module E, the following are equivalent:*

1. *E is injective;*

2. *the functor* $\mathrm{Hom}(-,E)$ *is an "exact functor", that is, if* $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ *is an exact sequence, then*

$$0 \longrightarrow \mathrm{Hom}(M_3,E) \xrightarrow{-\circ g} \mathrm{Hom}(M_2,E) \xrightarrow{-\circ f} \mathrm{Hom}(M_1,E) \longrightarrow 0$$

is an exact sequence.

Definition 5.21. Let $M \in \mathrm{Mod}(A)$. An exact sequence of the form

$$0 \longrightarrow M \xrightarrow{d_0} E_0 \xrightarrow{d_1} E_1 \xrightarrow{d_2} E_2 \longrightarrow \dots$$

where all the A-modules E_i are injective, is called an ***injective resolution*** of M.

One may expect injective resolutions to be very similar to projective resolutions, since they are formally just a "dual notion". But it turns out that they are harder to construct than projective resolutions. However, in some contexts like the study of sheaf cohomology, they are the natural concept to consider. We will not consider injective modules and injective resolutions later in this course.

6 Localizations (i.e., "rings and modules of fractions")

Example 6.1. Consider the equivalence relation $\sim$ on $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ defined by

$$(a,b)\sim(c,d) \qquad \text{if} \qquad ad=bc.$$

The equivalence class $\overline{(a,b)}$ of $(a,b)\in\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ is usually denoted by $\frac{a}{b}$. This is a way of defining the rational numbers, provided that one has defined $\mathbb{Z}$ first:

$$\mathbb{Q}:=\big(\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})\big)/\sim\ .$$

The elementary-school addition and multiplication of fractions are well-defined operations on this quotient and make it into a ring, but note that it is not a "quotient ring" meant as in a ring modulo an ideal.

The goal of this section is to generalize the construction in the example above to more general rings. A special case of the procedure defined in this section is an important source of local rings: starting from a ring A, we will "localize at a prime ideal" $p\in\operatorname{Spec}(A)$, producing a local ring A_p. This is a central construction in algebraic geometry and a motivation for the study of local rings in commutative algebra.

Recall that a *multiplicative system* is a subset S of a ring A such that $1_A\in S$ and the product of any two elements of S is in S (see Definition 2.4).

Definition 6.2. Let A be a ring and $S\subseteq A$ be a multiplicative system. Consider the equivalence relation $\sim$ on the set $A\times S$ defined by

$$(a,s)\sim(b,s') \qquad \text{if} \qquad \exists_{t\in S}\, t(s'a-sb)=0.$$

The quotient $A_S:=(A\times S)/\sim$ is called the ***localization of*** A ***in*** S.[2] The equivalence class of (a,s) is written $\frac{a}{s}$ or a/s, and it is called a ***fraction***. We define two binary operations $+$ and $\cdot$ on A_S, which make it a ring:

$$\frac{a}{s}+\frac{b}{s'}:=\frac{as'+bs}{ss'}, \qquad \frac{a}{s}\cdot\frac{b}{s'}:=\frac{ab}{ss'}.$$

Lastly, we define a ring homomorphism

$$\begin{aligned} i_S\colon A &\longrightarrow A_S \\ a &\longmapsto \frac{a}{1}. \end{aligned}$$

Exercise 6.3. Show that:

- the relation $\sim$ is indeed an equivalence relation;
- the operations $+$ and $\cdot$ are well defined, and $(A_S,+,\cdot)$ is indeed a ring, with additive identity $\frac{0}{1}$ and unity $\frac{1}{1}$;
- the map i_S is indeed a ring homomorphism;
- the elements of S are mapped to units by i_S, that is, $i_S(S)\subseteq\mathcal{U}(A_S)$. Morally, what happens is that we introduce multiplicative inverses for the elements of S (the fractions $1/s$) in A_S.

[2] Some authors use the notation $S^{-1}A$ for A_S, exactly to stress the point, mentioned in Exercise 6.3, that the elements of S "become invertible" in A_S.

Proposition 6.4 (Universal property of the localization). *Let A be a ring, and let $S \subseteq A$ be a multiplicative system.*

(1) The pair (A_S, i_S) satisfies the following "universal property": Let B be a ring, and let $f\colon A \to B$ be a ring homomorphism with $f(S) \subseteq \mathcal{U}(B)$. Then there exists a unique ring homomorphism $g\colon A_S \to B$ that makes the diagram

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "i_S"'] & & B \\
& A_S \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

commute, i.e., $f = g \circ i_S$.

(2) The pair (A_S, i_S) is unique up to isomorphism in the following sense: if C is a ring and $h\colon A \to C$ is a ring homomorphism such that $h(S) \subseteq \mathcal{U}(C)$, and the pair (C, h) satisfies the same property as (A_S, i_S) in part (1) above, then $C \cong A_S$.

Proof. Part (1) is left as an exercise. As for part (2), let (C, h) be another pair satisfying the universal property, so that the property holds for both (A_S, i_S) and (C, h). In particular, we may choose the ring B and the map f in the universal property in turn as A_S and i_S and then as C and h, so that we get diagrams

$$\begin{tikzcd}
A \arrow[rr, "i_S"] \arrow[dr, "i_S"'] & & A_S \\
& A_S \arrow[ur, dashed, "\mathrm{id}_{A_S}"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[rr, "h"] \arrow[dr, "h"'] & & C \\
& C \arrow[ur, dashed, "\mathrm{id}_C"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
A \arrow[rr, "h"] \arrow[dr, "i_S"'] & & C \\
& A_S \arrow[ur, dashed, "g"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[rr, "i_S"] \arrow[dr, "h"'] & & A_S \\
& C. \arrow[ur, dashed, "g'"'] &
\end{tikzcd}$$

By gluing the two bottom diagrams along i_S, we get

$$\begin{tikzcd}
& C \\
A \arrow[ur, "h"] \arrow[r, "i_S"'] \arrow[dr, "h"'] & A_S \arrow[u, dashed, "g"'] \\
& C, \arrow[u, dashed, "g'"']
\end{tikzcd}$$

so that the composition $g \circ g'$ needs to be equal to id_C, by the diagram on the top right above. Similarly, $g' \circ g = \mathrm{id}_{A_S}$. This shows that g and g' are inverses of each other, hence isomorphisms between A_S and C. □

Remark 6.5. The universal property of the localization is useful in (at least) two ways:

- From a theoretical point of view, it is cleaner to prove some results by using the universal property instead of the explicit definition of localization.
- From a practical point of view, A_S is defined as a quotient. So, when one defined a map from A_S to some other ring, one needs to always check that the map is well defined. The universal property gives the well-definedness almost for free (by showing it once and for all in the proof above).

There are other objects that satisfy their own "universal property", in the same sense that if another object satisfies the same property, then the two objects are isomorphic. For instance, the universal property of the abelian group $\mathbb{Z}^n$ is the following: for any finitely generated abelian group G with generators $x_1,\dots,x_n$, there is a unique group homomorphism $\varphi\colon \mathbb{Z}^n \to G$ such that $\varphi(e_i) = x_i$ for all i, where e_i is the vector with 0s everywhere except 1 in the i-th entry. One can show that any group H that satisfies this property is isomorphic to $\mathbb{Z}^n$. Tensor products, in Lecture 10, satisfy their own universal property.

Exercise 6.6. Show that:

1. i_S is injective if and only if S contains no zero-divisors;
2. if $0 \in S$, then $A_S = \{0\}$.

Recall contraction and extension from Definition 1.9.

Theorem 6.7. *Let A be a ring and $S \subseteq A$ a multiplicative system. Consider contraction and extension with respect to the map $i_S\colon A \to A_S$.*

(1) For any ideal $I \lhd A$, the extension I^e, more often denoted IA_S, is

$$IA_S = \{a/s \mid a \in I, s \in S\} \lhd A_S.$$

(2) For any ideal $J \lhd A_S$, we have $J = J^{ce}$.

(3) For any ideal $I \lhd A$, we have $I^{ec} = \bigcup_{s\in S}(I : s)$.

(4) The map

$$\begin{aligned}\Phi\colon \{p \in \operatorname{Spec}(A) \mid p \cap S = \emptyset\} &\longrightarrow \operatorname{Spec}(A_S)\\ q &\longmapsto q^e\end{aligned}$$

is an inclusion-preserving bijection. (The same holds if we replace prime ideals by primary ideals.)

Proof. The first three statements are left as an exercise. We prove (4). First we show that $p^{ec} = p$. We already know that $p \subseteq p^{ec}$ holds in general. By part (3), we have $p^{ec} = \bigcup_{s\in S}(p : s)$. Hence, if $a \in p^{ec}$, then $as \in p$ for some $s \in S$. Since $s \notin p$, we have $a \in p$.

Next, note that the map Φ is well defined. If $p \cap S = \emptyset$, then by part (1), the ideal p^e is proper and prime: if $\frac{a}{s}\frac{b}{t} \in p^e$, then $\frac{ab}{st} = \frac{a'}{s'}$ for some $a' \in p$ and $s' \in S$; this means that $s_1(sta' - s'ab) = 0$ for some $s_1 \in S$, which implies that $s_1 s'ab \in p$. Thus $ab \in p$, so that $a \in p$ or $b \in p$, and therefore $\frac{a}{s} \in p^e$ or $\frac{b}{t} \in p^e$.

Because $p^{ec} = p$, the map Φ is injective. By part (2), it is surjective. □

Examples 6.8. 1. If A is an integral domain, then $A \setminus \{0\}$ is a multiplicative system. The localization $A_{A\setminus\{0\}}$ is called the ***fraction field*** of A. A special case of this is given in Example 6.1: $\mathbb{Q} = \mathbb{Z}_S$, with $S = \mathbb{Z} \setminus \{0\}$. Note that in this case the condition

$$\exists_{t\in S}\, t(s'a - sb) = 0$$

can be simplified to $s'a - sb = 0$.

2. (**Important.**) Let $p \in \operatorname{Spec}(A)$ and $S := A \setminus p$. Then we write $A_p := A_S$ and call this the ***localization of** A **at the prime** p*. The ring (A_p, pA_p) is local. Indeed, if $\frac{b}{t} \notin pA_p$, then $b \notin p$, so that $b \in S$, and then $\frac{b}{t} \in \mathcal{U}(A_p)$. From the previous theorem, we have

$$\operatorname{Spec}(A_p) \cong \{q \in \operatorname{Spec}(A) \mid q \subseteq p\}.$$

This generalizes the case of integral domains (because there (0) is a prime ideal) in the previous item.

3. Let $S = \{1, f, f^2, \ldots\}$, for $f \in A \setminus \operatorname{nil}(A)$. Then we denote $A_f := A_S$. Recall from Definition 2.15 that $D(f) = \{p \in \operatorname{Spec}(A) \mid f \notin p\}$. Then $\operatorname{Spec}(A_f) \cong D(f)$.

Note that, if (f) is a prime ideal, then $A_{(f)}$ and A_f are two different localizations.

Lemma 6.9. *Let A be a ring, let $I \lhd A$, and le $S \subseteq A$ be a multiplicative system. Denote by $\overline{S}$ the image of S in A/I along the projection. Then $A_S/IA_S \cong (A/I)_{\overline{S}}$.*

Proof. The isomorphism is

$$\begin{aligned} A_S/IA_S &\longrightarrow (A/I)_{\overline{S}} \\ \frac{a}{s} + IA_S &\longmapsto \frac{a+I}{s+I}. \end{aligned}$$

□

One can think of the result above as stating that localizing and taking quotients "commute":

$$\begin{tikzcd} A \arrow[r, mapsto, "\text{quotient}"] \arrow[d, mapsto, "\text{localize}"'] & A/I \arrow[d, mapsto, "\text{localize}"] \\ A_S \arrow[r, mapsto, "\text{quotient}"'] & A_S/IA_S \cong (A/I)_{\overline{S}}. \end{tikzcd}$$

Lemma 6.10. *Let A be a ring and $S \subseteq A$ a multiplicative system.*

1. *Let $T \supset S$ be another multiplicative system, and denote $T' := i_S(T)$, which is a multiplicative system inside A_S. Then $(A_S)_{T'} = A_T$.*

2. *Let $p \in \operatorname{Spec}(A)$ be such that $p \cap S = \emptyset$. Then $(A_S)_{pA_S} = A_p$.*

Proof. Exercise. □

6.1 Localization of modules

Exercise 6.11. Let A and B be rings, and $f \colon A \to B$ be a ring homomorphism. If M is a B-module, one may define an A-module structure on M by ***restriction of scalars***: if $\cdot_B$ is the multiplication by scalars in B, one defines the multiplication $\cdot_A$ by scalars in A as

$$a \cdot_A m := f(a) \cdot_B m.$$

Verify that M equipped with $\cdot_A$ is then an A-module.

Definition 6.12. Let A be a ring. Let $M \in \mathrm{Mod}(A)$ and $S \subseteq A$ be a multiplicative system. Consider the equivalence relation $\sim$ on the set $M \times S$ defined by

$$(m,s) \sim (n,s') \qquad \text{if} \qquad \exists_{t \in S}\, t(s'm - sn) = 0_M.$$

The quotient $M_S := (M \times S)/\!\sim$ is called the ***localization of*** M ***in*** S. The equivalence class of (m,s) is written $\frac{m}{s}$ or m/s, and it is called a ***fraction***. We define a binary operation $+$ on M_S and a multiplication by scalars in A_S, which make M_S an A_S-module:

$$\frac{m}{s} + \frac{n}{s'} := \frac{s'm + sn}{ss'}, \qquad \frac{a}{s} \cdot \frac{m}{s'} := \frac{am}{ss'}.$$

(In particular, by using the homomorphism $i_S \colon A \to A_S$, we get that M_S has an A-module structure by restriction of scalars.) Lastly, we define a homomorphism of A-modules

$$\begin{aligned} j_S \colon M &\longrightarrow M_S \\ m &\longmapsto \frac{m}{1}. \end{aligned}$$

Exactly as in the case of rings, the localization of a module in some particular multiplicative systems has a special notation:

- If $S = A \setminus p$ for $p \in \mathrm{Spec}(A)$, then we write $M_p := M_S$.
- If $S = \{1, x, x^2, \ldots\}$ for $x \in A \setminus \mathrm{nil}(A)$, then we write $M_x := M_S$.

Exercise 6.13. Show that:

- the relation $\sim$ is indeed an equivalence relation;
- the operations $+$ and $\cdot$ are well defined, and $(M_S, +, \cdot)$ is indeed an A_S-module, with (additive) identity $0_M/1_A$;
- the map j_S is indeed an A-module homomorphism.

Proposition 6.14 (Universal property of the localization)**.** *Let A be a ring, let $S \subseteq A$ be a multiplicative system, and let $M \in \mathrm{Mod}(A)$.*

(1) The pair (M_S, j_S) satisfies the following "universal property": Let $N \in \mathrm{Mod}(A)$ be such that the scalar multiplication $(-) \cdot s \colon N \to N$ by any fixed $s \in S$ is a bijection, and let $f \colon M \to N$ be an A-module homomorphism. Then there exists a unique A-module homomorphism $g \colon M_S \to N$ that makes the diagram

$$\begin{tikzcd}
M \arrow[rr, "f"] \arrow[dr, "j_S"'] & & N \\
& M_S \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

commute, i.e., $f = g \circ j_S$.

(2) The pair (M_S, j_S) is uniquely determined up to isomorphism by the property above.

Proof. Exercise. □

Definition 6.15. Let A be a ring and $S \subseteq A$ a multiplicative system. Let $M, N \in \mathrm{Mod}(A)$, and let $f\colon M \to N$ be a homomorphism of A-modules. Then we define the homomorphism of A_S-modules

$$\begin{aligned} f_S\colon M_S &\longrightarrow N_S \\ \frac{m}{s} &\longmapsto \frac{f(m)}{s}. \end{aligned}$$

We call f_S the ***localization of f in S***.

Proposition 6.16. 1. *The construction above is "functorial", in the sense that:*

- *for any $M \in \mathrm{Mod}(A)$ and multiplicative system $S \subseteq A$, one has $(\mathrm{id}_M)_S = \mathrm{id}_{M_S}$;*
- *for A-module homomorphisms $f\colon M \to N$ and $g\colon N \to P$, one has $(g \circ f)_S = g_S \circ f_S$.*

2. *Localization is an "exact functor", in the sense that if*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

is an exact sequence of A-modules, then

$$0 \longrightarrow M_S \xrightarrow{f_S} N_S \xrightarrow{g_S} P_S \longrightarrow 0$$

is an exact sequence of A_S-modules.

Proof. Exercise. For the second statement, it is enough to show that if $M \to N \to P$ is exact at N, then $M_S \to N_S \to P_S$ is exact at N_S. □

Corollary 6.17. *The localization of an injective (respectively, surjective) homomorphism is injective (respectively, surjective).*

To conclude this section, we give a couple of results that show how one may inspect "global" properties of a module or a homomorphism by checking that they hold "locally".

Definition 6.18. The ***support*** of $M \in \mathrm{Mod}(A)$ is

$$\mathrm{Supp}(M) := \{p \in \mathrm{Spec}(A) \mid M_p \neq 0\}.$$

Proposition 6.19 (Local properties)**.** *Let $M \in \mathrm{Mod}(A)$.*

1. *Let $x \in M$. If for every $\mathfrak{m} \in \mathrm{Max}(A)$ we have $x/1 = 0/1$ in $M_\mathfrak{m}$, then $x = 0$ in M.*

2. *We have*

$$M \neq 0 \quad \Leftrightarrow \quad \mathrm{Supp}(M) \neq \emptyset \quad \Leftrightarrow \quad \exists_{\mathfrak{m} \in \mathrm{Max}(A)} M_\mathfrak{m} \neq 0.$$

Proof. 1. The equality $x/1 = 0/1$ in $M_\mathfrak{m}$ means that there exists $s \in A \setminus \mathfrak{m}$ such that $sx = 0$ in M, which means that $\mathrm{ann}(x) \not\subseteq \mathfrak{m}$. On the other hand, by Krull's theorem, if $\mathrm{ann}(x) \cap \mathcal{U}(A) = \emptyset$, then there would be $\mathfrak{m} \in \mathrm{Max}(A)$ such that $\mathrm{ann}(x) \subseteq \mathfrak{m}$. So there is an invertible element annihilating x, which means that $x = 0$.

2. This follows from the previous part. Exercise.

□

Corollary 6.20. *Let $M, N \in \mathrm{Mod}(A)$ and $f \in \mathrm{Hom}_A(M, N)$. The following are equivalent:*

1. *f is injective (respectively, surjective);*

2. *for all $m \in \mathrm{Max}(A)$, the map $f_m\colon M_m \to N_m$ is injective (respectively, surjective).*

Proof. The implication $(1 \Rightarrow 2)$ holds by the exactness of the localization functor (second part of Proposition 6.16). For the converse implication, let $M' := \ker(f)$. Since localization is exact, we have $M'_\mathfrak{m} = \ker(f_\mathfrak{m}) = 0$. Hence $M' = 0$, by Proposition 6.19. Surjectivity is left as an exercise. □

7 Noetherian rings and modules

Proposition 7.1. *Let A be a ring. For $M \in \mathrm{Mod}(A)$, the following are equivalent:*

1. *every submodule of M is finitely generated;*
2. *every ascending chain of submodules of M stabilizes, that is, for any chain*

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \dots$$

of submodules of M, there exists $c \in \mathbb{N}$ such that $N_i = N_c$ for all $i \geq c$.

Proof. ($1 \Rightarrow 2$) By contradiction, let $N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots$ be an infinite strictly increasing chain of A-submodules of M. The union $N := \bigcup_{i=1}^{+\infty} N_i$ is an A-submodule of M, so that by assumption N is finitely generated, by some elements $m_1, \dots, m_k$. For each $i \in \{1, \dots, k\}$, there exists j_i such that $m_i \in N_{j_i}$, but then if we set $j := \max\{j_1, \dots, j_k\}$ we have $N \subseteq N_j$, which is a contradition, since $N_j \subsetneq N_{j+1} \subseteq N$.

($2 \Rightarrow 1$) By contradiction, let $N \lhd M$ not be finitely generated. For any $m_1 \in N$, we have $\langle m_1 \rangle \subsetneq N$, and for any $m_2 \in N \setminus \langle m_1 \rangle$, we have $\langle m_1 \rangle \subsetneq \langle m_1, m_2 \rangle \subsetneq N$. We may proceed this way and find a sequence $\{m_i\}_{i \in \mathbb{N}}$ of elements of N, which generate modules that form an infinite strictly increasing chain. □

Definition 7.2.
- Let A be a ring. An A-module M is called a ***Noetherian module*** if it satisfies the conditions in the proposition above.
- A ring A is called a ***Noetherian ring*** if it is a Notherian A-module (that is, if every ideal of A is finitely generated, or equivalently every ascending chain of ideals stabilizes).

Condition (2) in the proposition is usually referred to as the "ascending chain condition". There is a similar "descending chain condition", in which any chain of smaller and smaller submodules eventually stabilizes. Modules satisfying this other condition are called *Artinian modules*, and we will not discuss them in this course.

Examples 7.3.
- Every field k is a Noetherian ring: the only ideals are $k = (1)$ and (0).
- We know that $\mathbb{Z}$ and the polynomial ring $k[x]$ over a field k are PID's (as a consequence of the Euclidean algorithm), hence they are Noetherian rings.
- A ring that is *not* Noetherian is a polynomial ring $k[x_i \mid i \in \mathbb{N}]$ with infinitely many variables, because the chain of ideals

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \dots$$

does not stabilize. Note that the ring itself is finitely generated (by 1, like every ring).

- Consider the set

$$A := \left\{ a + xf \mid a \in \mathbb{Q}, f \in \mathbb{Q}[x,y] \right\} \subseteq \mathbb{Q}[x,y].$$

One may show that A is a subring of $\mathbb{Q}[x,y]$, with $\mathbb{Q}[x] \subsetneq A \subsetneq \mathbb{Q}[x,y]$. (As a consequence of Hilbert's Basis Theorem below, note that both $\mathbb{Q}[x]$ and $\mathbb{Q}[x,y]$ are Noetherian rings.) The ring A is *not* Noetherian: note that, since $y \notin A$, we have $xy \notin (x)$ in A, and thus we get the chain of ideals

$$(x) \subsetneq (x, xy) \subsetneq (x, xy, xy^2) \subsetneq (x, xy, xy^2, xy^3) \subsetneq \dots,$$

which does not stabilize.

We use the following terminology in the proof of Hilbert's basis theorem below:

Definition 7.4. Let A be a ring. For a polynomial $f = a_nx^n + a_{n-1}x^{n-1} + \dots a_1x + a_0$ in $A[x]$ with $a_n \neq 0$, we call $\mathrm{LT}(f) := a_nx^n$ the ***leading term*** of f and $\mathrm{LC}(f) := a_n$ the ***leading coefficient*** of f.

(In the literature these are also referred to as "initial term" and "initial coefficient".)

Theorem 7.5 (Hilbert's Basis Theorem)**.** *Let A be a Noetherian ring. Then $A[x]$ is a Noetherian ring. More generally, $A[x_1, \dots, x_n]$, for any $n \in \mathbb{N}$, is a Noetherian ring.*

Proof. Let $I \lhd A[x]$. We show that I is finitely generated. Choose a sequence of elements $f_1, f_2, \dots \in I$ as follows: Let f_1 be an element of least degree in I. For $i \geq 1$, if $(f_1, \dots, f_i) \subsetneq I$, let f_{i+1} be an element of least degree in $I \setminus (f_1, \dots, f_i)$. If $(f_1, \dots, f_i) = I$, stop choosing elements.

For each j, let $a_j := \mathrm{LC}(f_j)$. Since A is Noetherian, the ideal $J := (a_1, a_2, \dots)$ is finitely generated. Let m be the smallest index such that $(a_1, \dots, a_m) = J$. We will show that $(f_1, \dots, f_m) = I$. By contradiction, say this is not the case. Then in the process above we chose an element $f_{m+1} \in I \setminus (f_1, \dots, f_m)$. We may write $a_{m+1} = \sum_{j=1}^m r_ja_j$, for some $r_j \in A$. Since the degree of f_{m+1} is at least as large as the degrees of $f_1, \dots, f_m$, we may define the polynomial

$$g := \sum_{j=1}^{m} r_jf_jx^{\deg(f_{m+1}) - \deg(f_j)} \in (f_1, \dots, f_m).$$

Then $\mathrm{LT}(g) = (\sum_{j=1}^m r_ja_j)x^{\deg(f_{m+1})} = \mathrm{LT}(f_{m+1})$. Hence, the difference $f_{m+1} - g$ is in $I \setminus (f_1, \dots, f_m)$ and has strictly smaller degree than f_{m+1}, which contradicts the choice of f_{m+1}.

The statement with an arbitrary finite number of variables follows by induction, since $(A[x_1, \dots, x_{n-1}])[x_n] \cong A[x_1, \dots, x_{n-1}, x_n]$. □

Recall the formal definition of a polynomial with coefficients in A as a sequence $\mathbb{N} \to A$ which is eventually zero. One writes x for the sequence $(0, 1, 0, 0, \dots)$. With the same notation and operations, one may consider sequences $\mathbb{N} \to A$ that are not necessarily eventually zero, thereby obtaining ***formal power series***.

Definition 7.6. We write $A[[x]]$ for the ring of formal power series in the variable x.

One can think of $A[x]$ as a subring of $A[[x]]$. The "constant" series 1 is the unity of $A[[x]]$.

Proposition 7.7. *Let A be a ring.*

1. *A formal power series $f = a_0 + a_1x + a_2x^2 + \dots$ is a unit of $A[[x]]$ if and only if a_0 is a unit of A.*

2. *Let $(A, \mathfrak{m})$ be a local ring. Then the ring $A[[x]]$ is local.*

Proof. We leave the second part as an exercise and prove the first statement. Assume first that $f \in \mathcal{U}(A[[x]])$, so that there exists an inverse $g = b_0 + b_1x + b_2x^2 + \dots$ for f. By expanding $1 = fg = a_0b_0 + (a_0b_1 + a_1b_0)x + \dots$, clearly $a_0 \in \mathcal{U}(A)$. For the converse implication, let $a_0 \in \mathcal{U}(A)$. One may construct an inverse $g = b_0 + b_1x + \dots$ of f as follows: since we need $a_0b_0 = 1$, we set $b_0 := a_0^{-1}$; since we need $a_0b_1 + a_1b_0 = 0$, we set $b_1 := -a_1b_0a_0^{-1}$. And so on. □

Theorem 7.8. *If A is a Noetherian ring, then $A[[x]]$ is a Noetherian ring.*

Proof. The proof is similar to that of Hilbert's basis theorem. Exercise. □

7.1 Noetherianity and exactness

Proposition 7.9. *Let $0 \to M \to N \to P \to 0$ be an exact sequence of A-modules. Then N is Noetherian if and only if M and P are Noetherian.*

Proof. Exercise. □

Corollary 7.10. *Quotients and submodules of Noetherian A-modules are Noetherian.*

Proof. By Proposition 7.9, this follows by using the exact sequence $0 \to N \to M \to M/N \to 0$, for $N \lhd M$. □

Corollary 7.11. *Let A be a Noetherian ring.*

1. *Finitely generated free A-modules, that is, the modules (isomorphic to) A^n for $n \in \mathbb{N}$, are Noetherian.*

2. *Finitely generated A-modules are Noetherian.*

Proof.
1. The sequence $0 \to A \xrightarrow{\iota} A^n \xrightarrow{\pi} A^{n-1} \to 0$ is exact, where ι is the canonical embedding of the last summand A in $A^n = \bigoplus_{i=1}^n A$, and π is the projection on the first $n-1$ summands. By induction, the statement follows by Proposition 7.9.

2. A finitely generated A-module is (isomorphic to) a quotient of A^n, for some $n \in \mathbb{N}$.

□

In Section 5.2, we defined a *free resolution* of $M \in \mathrm{Mod}(A)$ as an exact sequence of the form

$$\ldots \longrightarrow F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \longrightarrow 0,$$

where all the F_i's are free A-modules. We saw how to construct a free resolution of a given module: first define $d_0 \colon F_0 \to M$ as a surjection. Then we define a map $d_1 \colon F_1 \to F_0$ so that $\mathrm{im}(d_1) = \ker(d_0)$. Similarly, we define $d_2 \colon F_2 \to F_1$ so that $\mathrm{im}(d_2) = \ker(d_1)$. And so on. *The idea at each step is to surject onto the kernel of the map defined in the previous step.* The kernel of a homomorphism is a submodule, hence we get the following:

Corollary 7.12. *Let A be a Noetherian ring, and let $M \in \mathrm{Mod}(A)$ be finitely generated. Then there exists a resolution of M where each free module is finitely generated.*

It is still not clear at this point whether a resolution ends, that is, whether one always a sufficiently large index p such that $F_i = 0$ for all $i > p$. This does not always happen, but for modules over polynomial rings it does happen that one always has such a "finite" resolution. This will be the content of Hilbert's Syzygy Theorem, in Lecture 11.

7.2 Irreducible ideals and primary decompositions

Definition 7.13. Let A be a ring. An ideal $I \lhd A$ is called an ***irreducible ideal*** if whenever $I = J_1 \cap J_2$ for some $J_1, J_2 \lhd A$, we have $I = J_1$ or $I = J_2$.

Proposition 7.14. *Let A be a Noetherian ring. Every proper irreducible ideal $I \lhd A$ is primary.*

Proof. Let $a, b \in A$ be such that $ab \in I$. By the Noetherianity of A, the chain of ideals

$$I : b \subseteq I : b^2 \subseteq I : b^3 \subseteq \cdots$$

stabilizes, so that in particular there is an $n \in \mathbb{N}$ such that $I : b^n = I : b^{n+1}$. We show that $I = (I + (a)) \cap (I + (b^n))$:

($\subseteq$) Trivial.

($\supseteq$) Let $x \in (I + (a)) \cap (I + (b^n))$, so that $x = i_1 + r_1 a$ and $x = i_2 + r_2 b^n$, for some $i_1, i_2 \in I$ and $r_1, r_2 \in A$. Then $r_2 b^n = i_1 - i_2 + r_1 a$, and $r_2 b^{n+1} = (i_1 - i_2)b + r_1 ab$ is an element of I. But this means that $r_2 \in I : b^{n+1} = I : b^n$, so that $r_2 b^n \in I$. Therefore $x \in I$.

Since I is irreducible, we have $I = I + (a)$, in which case $a \in I$, or $I = I + (b^n)$, in which case $b^n \in I$. Hence I is primary. □

Theorem 7.15. *Let A be a Noetherian ring and let $I \lhd A$ be a proper ideal. Then:*

1. *The ideal I is the intersection of finitely many irreducible ideals.*
2. *There exist primary ideals $Q_1, \dots, Q_s$ of A such that, if we write $p_i := \sqrt{Q_i}$, then*
   - *$I = Q_1 \cap \cdots \cap Q_s$,*
   - *if $i \neq j$, then $p_i \neq p_j$, and*
   - *the decomposition is irredundant, that is, for all $j \in \{1, \dots, s\}$, we have $I \subsetneq \bigcap_{i \neq j} Q_i$.*

Proof. (1) By contradiction, suppose that the family

$$\mathcal{P} := \{I \lhd A \mid I \text{ is } \textit{not} \text{ the intersection of finitely many irreducible ideals}\}$$

is not empty. By the Noetherianity of A, these exists $L \in \mathcal{P}$ which is maximal with respect to inclusion. This L is not irreducible (or else $L = L$ would be a decomposition). Then there exist ideals $J_1, J_2 \lhd A$ with $J_1 \supsetneq L \subsetneq J_2$ and $L = J_1 \cap J_2$. And $J_1, J_2 \notin \mathcal{P}$ by the maximality of L. So then we have decompositions $J_1 = H_1 \cap \cdots \cap H_{s_1}$ and $J_2 = K_1 \cap \cdots \cap K_{s_2}$, where the H_i's and K_i's are irreducible ideals. But then L is the intersection of finitely many irreducible ideals.

(2) By part (1), we may write $I = J_1 \cap \cdots \cap J_t$, where each J_i is irreducible, and by Proposition 7.14, proper irreducible ideals are primary. (Recall that the radical of a primary ideal is prime, by Proposition 2.18.) If J_i and J_k are such that $\sqrt{J_i} = \sqrt{J_k}$, then $J_i \cap J_k$ is primary. Replace $J' := J_i \cap J_k$ in the decomposition $I = J_1 \cap \cdots \cap J_t$. Repeat the process as many times as needed until all factors have pairwise distinct radical. The irredundance is achieved by removing the unnecessary factors. □

Definition 7.16. A decomposition into primary ideals as in part (2) of Theorem 7.15 is called a ***primary decomposition*** of I.

Example 7.17. Consider the ideal $I := (x^2, xy)$ in the polynomial ring $k[x,y]$, where k is a field. Then $(x^2, xy) = (x) \cap (x^2, y)$ is a decomposition into irreducible ideals, and

$$(x^2, xy) = (x) \cap (x^2, xy, y^2)$$

is a primary decomposition. The second factor is a primary ideal, and its radical is (x, y) (see Remark 8.2 below for more details).

8 More on primary decompositions

Proposition 2.18 shows that the radical of a primary ideal is prime, and in Remarks 2.19 there is an example of a non-primary ideal whose radical is prime.

Lemma 8.1. *Let $Q \lhd A$ be such that $\sqrt{Q} \in \operatorname{Max}(A)$. Then Q is primary.*

Proof. Exercise. □

Remark 8.2. For $\gamma = (\gamma_1, \dots, \gamma_n) \in \mathbb{N}^n$, denote $x^\gamma := x_1^{\gamma_1} \cdots x_n^{\gamma_n}$. Monomial ideals, that is, ideals generated by monomials, are easier to understand than arbitrary polynomial ideals. For monomial ideals it is easy to compute intersections and radicals (and other constructions):

- If $I = (x^{\alpha_1}, \dots, x^{\alpha_s})$ and $J = (x^{\beta_1}, \dots, x^{\beta_t})$, then $I \cap J = (\operatorname{lcm}(x^{\alpha_i}, x^{\beta_j}) \mid i = 1, \dots, s,\ j = 1, \dots, t)$.
- For $\gamma = (\gamma_1, \dots, \gamma_n) \in \mathbb{N}^n$, denote by $\sqrt{\gamma}$ the vector in $\mathbb{N}^n$ whose k-th entry is 1 if $\gamma_k > 0$, and 0 if $\gamma_k = 0$, for all $k = 1, \dots, n$. Then $\sqrt{(x^{\alpha_1}, \dots, x^{\alpha_s})} = (x^{\sqrt{\alpha_1}}, \dots, x^{\sqrt{\alpha_s}})$.

Theorem 7.15 shows that a proper ideal in a Noetherian ring has a primary decomposition. Primary decompositions are not unique, and there can be infinitely many:

Example 8.3. Consider the ideal $I := (x^2, xy)$ in the polynomial ring $k[x, y]$, where k is a field, as in Example 7.17. For any $m \in \mathbb{N}$,

$$(x^2, xy) = (x) \cap (x^2, xy, y^m)$$

is a primary decomposition of I. The second factor is primary by Lemma 8.1, as its radical is (x, y). Note that the following three things do not change, regardless of the decomposition:

- the factor (x),
- the number of factors used (always two),
- the radicals of the factors (respectively (x) and (x, y)).

8.1 Associated primes

Recall that, for $M \in \operatorname{Mod}(A)$ and $m \in M$, we set $\operatorname{ann}(m) := \{a \in A \mid am = 0\}$.

Lemma 8.4. *Let $M \neq 0$ be an A-module, and let $I \lhd A$, $I \neq A$. The following are equivalent:*

1. *there exists an injective A-module homomorphism $f\colon A/I \to M$;*
2. *there exists an $m \in M \setminus \{0\}$ such that* $\operatorname{ann}(m) = I$.

Proof. ($1 \Rightarrow 2$) Let $f\colon A/I \to M$ be an injective A-module homomorphism. Let $m := f(\overline{1})$. Then $a \in \operatorname{ann}(m)$ if and only if $am = 0$, and on the other hand $am = af(\overline{1}) = f(\overline{a})$. Since f is injective, this means that $a \in I$.

($2 \Rightarrow 1$) Let $m \in M \setminus \{0\}$ be such that $\operatorname{ann}(m) = I$. Consider the A-module homomorphism

$$g\colon A \longrightarrow M, \qquad a \longmapsto am.$$

We have $\ker(g) = \operatorname{ann}(m) = I$, and by the first isomorphism theorem $A/I \cong \operatorname{im}(g) \subseteq M$. □

Definition 8.5. Let $M \in \operatorname{Mod}(A)$. We call $p \in \operatorname{Spec}(A)$ an ***associated prime*** of M if it satisfies the conditions of the lemma above. We write $\operatorname{Ass}_A(M)$ or $\operatorname{Ass}(M)$ for the set of associated primes of M.

Lemma 8.6. *Let A be a Noetherian ring and $M \in \mathrm{Mod}(A)$. If $M \neq 0$, then $\mathrm{Ass}_A(M) \neq \emptyset$. More precisely, for all $m \in M \setminus \{0\}$, there exists $p \in \mathrm{Ass}_A(M)$ satisfying $\mathrm{ann}(m) \subseteq p$.*

Proof. Let $m \in M \setminus \{0\}$. Consider the family $\mathcal{F} := \{\mathrm{ann}(am) \mid a \in A \setminus \mathrm{ann}(m)\}$. The elements of $\mathcal{F}$ are proper ideals of A, and $\mathcal{F} \neq \emptyset$. By the Noetherianity of A, there is $J \in \mathcal{F}$ that is maximal with respect to inclusion. So $J = \mathrm{ann}(am)$, for some $a \in A$ such that $am \neq 0$. We show that J is prime. Let $b, c \in A$ be such that $bc \in J$. There are two cases:

- If $cam = 0$, then $c \in J$.
- If $cam \neq 0$, then note that $J = \mathrm{ann}(am) \subseteq \mathrm{ann}(cam) \in \mathcal{F}$, so that $J = \mathrm{ann}(cam)$, since J is maximal. Hence $b \in J$.

As J is proper, J is then a prime ideal. □

Denote $D_A(M) := \{a \in A \mid \exists_{m \in M \setminus \{0\}} am = 0\}$ the set of *zero-divisors* of $M \in \mathrm{Mod}(A)$.

Corollary 8.7. *If A is a Noetherian ring and $M \in \mathrm{Mod}(A)$, then $D_A(M) = \bigcup_{p \in \mathrm{Ass}_A(M)} p$.*

Proposition 8.8. *Let A be a Noetherian ring. Let $M \neq 0$ be a finitely generated A-module. There exists a chain of submodules $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$ such that, for all i, there is some $p_i \in \mathrm{Spec}(A)$ satisfying $M_i/M_{i-1} \cong A/p_i$ (as A-modules).*

Proof. Since $M \neq 0$, by Lemma 8.6, there exists $p_1 = \mathrm{ann}(m_1) \in \mathrm{Ass}_A(M)$. Define $M_1 := \langle m_1 \rangle$. Consider the map

$$A \longrightarrow M, \qquad a \longmapsto am_1,$$

whose kernel is $\mathrm{ann}(m_1) = p_1$ and whose image is M_1, so that $A/p_1 \cong M_1$ by the first isomorphism theorem, and of course $M_1 = M_1/M_0$. If $M_1 = M$, then we are done. Otherwise, M/M_1 is not the zero module, so that there exists $p_2 \in \mathrm{Ass}_A(M/M_1)$, with $p_2 = \mathrm{ann}(\overline{m_2})$, for some $\overline{m_2} \in (M/M_1) \setminus \{\overline{0}\}$. Define $M_2 := M_1 + \langle m_2 \rangle$. Then $M_2/M_1 = \langle \overline{m_2} \rangle$, and similarly to the previous step we may consider the homomorphism

$$A \longrightarrow M/M_1, \qquad a \longmapsto a\overline{m_2},$$

whose kernel is p_2 and whose image is M_2/M_1, so that $A/p_2 \cong M_2/M_1$. If $M_2 = M$, then we are done. Otherwise, we proceed in the same way, and eventually this process will terminate, since M is Noetherian. □

Lemma 8.9. *Let A be any ring. Let $0 \to N \xrightarrow{f} M \xrightarrow{g} T \to 0$ be a short exact sequence of A-modules. Then $\mathrm{Ass}_A(N) \subseteq \mathrm{Ass}_A(M) \subseteq \mathrm{Ass}_A(N) \cup \mathrm{Ass}_A(T)$.*

Proof. The first inclusion is clear, as the composition of injective homomorphisms is injective. So we now show the second inclusion. Let $p \in \mathrm{Ass}_A(M)$, so that $p = \mathrm{ann}(m)$ for some $m \in M \setminus \{0\}$. Consider two cases:

- If $m \in \mathrm{im}(f)$, then there is some $n \in N$ satisfying $f(n) = m$, so that
$$am = 0 \quad \Leftrightarrow \quad af(n) = 0 \quad \Leftrightarrow \quad f(an) = 0 \quad \Leftrightarrow \quad an = 0,$$
and $p = \mathrm{ann}(n) \in \mathrm{Ass}_A(N)$.
- If $m \notin \mathrm{im}(f) = \ker(g)$, then $g(m) \neq 0$. In general, $\mathrm{ann}(m) \subseteq \mathrm{ann}(g(m))$. If equality holds, then $p \in \mathrm{Ass}_A(T)$. If instead $\mathrm{ann}(m) \subsetneq \mathrm{ann}(g(m))$, then there exists some $b \in A$ such that $bg(m) = 0$ and $bm \neq 0$. In particular $bm \in \ker(g) = \mathrm{im}(f)$, so that $bm = f(n)$ for some $n \in N$. But then $\mathrm{ann}(n) = \mathrm{ann}(bm)$, and lastly we show that $\mathrm{ann}(bm) = \mathrm{ann}(m)$, so that $p \in \mathrm{Ass}_A(N)$. The inclusion $(\supseteq)$ is trivial, so conversely let $a \in \mathrm{ann}(bm)$. Then $ab \in \mathrm{ann}(m) = p$, and since p is prime this means that $b \in p$, in which case $bm = 0$, a contradiction, or $a \in p$, which means that $a \in \mathrm{ann}(m)$.

In both cases, $p \in \mathrm{Ass}_A(N) \cup \mathrm{Ass}_A(T)$. □

Associated primes are "compatible" with taking localizations:

Lemma 8.10. *Let A be a Noetherian ring, $M \in \mathrm{Mod}(A)$, $S \subseteq A$ a multiplicative system and $p \in \mathrm{Spec}(A)$ with $p \cap S = \emptyset$. Then*

$$p \in \mathrm{Ass}_A(M) \quad \Leftrightarrow \quad pA_S \in \mathrm{Ass}_{A_S}(M_S).$$

Proof. Exercise. For the implication ($\Rightarrow$), show that if $p = \mathrm{ann}_A(m)$, then $pA_S = \mathrm{ann}_{A_S}(m/1)$. For the implication ($\Leftarrow$), if $pA_S = \mathrm{ann}_{A_S}(\frac{m}{s}) = \mathrm{ann}_{A_S}(\frac{m}{1})$, start by showing that $\mathrm{ann}_A(m) \subseteq p$. Note that p is finitely generated, by the Noetherianity of A. □

Recall, from Definition 2.10, that for an ideal $I \lhd A$, the inclusion-minimal elements of $V(I)$ are called the *minimal primes* of I. Recall, from Definition 6.18, that for a module $M \in \mathrm{Mod}(A)$, the *support* of M is the set $\mathrm{Supp}(M) = \{p \in \mathrm{Spec}(A) \mid M_p \neq 0\}$.

Lemma 8.11. *Let A be a Noetherian ring and $I \lhd A$. If $p \in \mathrm{Spec}(A)$ is minimal prime of I, then $p \in \mathrm{Ass}_A(A/I)$.*

Proof. We first show that $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$ for $M \in \mathrm{Mod}(A)$: indeed, if $p \in \mathrm{Ass}(M)$, then there is an injection $A/p \to M$, and this stays an injection $A_p/pA_p \to M_p$ after localizing, by the exactness of the localization. Next, we show that the minimal elements of $\mathrm{Ass}(M)$ and $\mathrm{Supp}(M)$ are the same, and it is enough to show that a minimal element $p \in \mathrm{Supp}(M)$ belongs to $\mathrm{Ass}(M)$: since $M_p \neq 0$,

$$\emptyset \neq \mathrm{Ass}_{A_p}(M_p) = \{qA_p \mid q \in \mathrm{Ass}_A(M)\} \subseteq \{qA_p \mid q \in \mathrm{Supp}(M)\} = \{pA_p\},$$

so that $p \in \mathrm{Ass}_A(M)$ by Lemma 8.10.

Now consider $M = A/I$. The set $\mathrm{Supp}(A/I)$ consists of the prime ideals containing I, so that the minimal elements of $\mathrm{Supp}(A/I)$ are exactly the minimal primes of I. □

Definition 8.12. Let A be a ring. We say that $Q \lhd A$ is p-***primary*** if Q is primary and $\sqrt{Q} = p$.

Lemma 8.13. *Let A be a Noetherian ring. Let $Q \lhd A$ and $p \in \mathrm{Spec}(A)$. Then*

$$\mathrm{Ass}_A(A/Q) = \{p\} \qquad \Leftrightarrow \qquad Q \text{ is } p\text{-primary.}$$

Proof. Exercise. Use Proposition 2.18, Corollary 8.7 and Lemma 8.11. □

Lemma 8.14. *Let A be a ring and $p \in \mathrm{Spec}(A)$. Let $Q \lhd A$ be p-primary. If $x \in A \setminus Q$, then the colon ideal $Q : x$ is p-primary.*

Proof. Exercise. □

Theorem 8.15. *Let A be a Noetherian ring. Let $M \neq 0$ be a finitely generated A-module. Then $\#\mathrm{Ass}_A(M) < +\infty$.*

Proof. By Proposition 8.8, there exists a chain of submodules $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$ such that, for all i, there exists $p_i \in \mathrm{Spec}(A)$ for which $M_i/M_{i-1} \cong A/p_i$. For each i, we may consider the short exact sequence $0 \to M_{i-1} \to M_i \to M_i/M_{i-1} \to 0$. By Lemma 8.9, we then have

$$\begin{aligned} \mathrm{Ass}_A(M_i) &\subseteq \mathrm{Ass}_A(M_{i-1}) \cup \mathrm{Ass}_A(M_i/M_{i-1}) \\ &\subseteq \mathrm{Ass}_A(M_{i-1}) \cup \mathrm{Ass}_A(A/p_i) = \mathrm{Ass}_A(M_{i-1}) \cup \{p_i\}, \end{aligned}$$

where the equality holds by Lemma 8.13. Hence, $\mathrm{Ass}_A(M) \subseteq \{p_1, \ldots, p_n\}$. □

Theorem 8.16. *Let A be a Noetherian ring and $I \lhd A$ a proper ideal. Let $I = Q_1 \cap \cdots \cap Q_s$ be a primary decomposition as in Theorem 7.15 (that is, the decomposition is irredundant and, if we set $p_i := \sqrt{Q_i}$, then $p_i \neq p_j$ whenever $i \neq j$). Then*

$$\mathrm{Ass}_A(A/I) = \{p_1, \ldots, p_s\}.$$

Proof. Given two A-modules M_1 and M_2, by using Lemma 8.9 on the short exact sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ (and on the similar sequence where M_1 and M_2 are swapped), one has $\mathrm{Ass}_A(M_1 \oplus M_2) = \mathrm{Ass}_A(M_1) \cup \mathrm{Ass}_A(M_2)$. In general, given A-modules $M_1, \ldots, M_s$, we have $\mathrm{Ass}_A(\bigoplus_{i=1}^s M_i) = \bigcup_{i=1}^s \mathrm{Ass}_A(M_i)$. We now prove the equality in the statement:

($\subseteq$) Consider the A-module homomorphism

$$\begin{aligned} \varphi \colon A &\longrightarrow \bigoplus_{i=1}^{s} A/Q_i \\ a &\longmapsto (\overline{a}, \ldots, \overline{a}), \end{aligned}$$

where each $\overline{a}$ denotes the equivalence class of a in the appropriate quotient. Since $\ker(\varphi) = Q_1 \cap \cdots \cap Q_s = I$, there is an injection $A/I \longrightarrow \bigoplus_{i=1}^s A/Q_i$. But then

$$\mathrm{Ass}_A(A/I) \subseteq \mathrm{Ass}_A\Big(\bigoplus_{i=1}^{s} A/Q_i\Big) = \bigcup_{i=1}^{s} \mathrm{Ass}_A(A/Q_i) = \{p_1, \ldots, p_s\},$$

as we have $\mathrm{Ass}_A(A/Q_i) = \{p_i\}$ by Lemma 8.13.

($\supseteq$) By the irredundance of the decomposition, we have $I \subsetneq Q_2 \cap \cdots \cap Q_s$, so that there exists $x \in (Q_2 \cap \cdots \cap Q_s) \setminus I$. Define

$$\psi \colon A \longrightarrow A/I, \quad a \longmapsto \overline{ax}.$$

Then

$$\ker \psi = I : x = \Big(\bigcap_{i=1}^{s} Q_i\Big) : x = \bigcap_{i=1}^{s} (Q_i : x) = Q_1 : x,$$

since $x \in Q_2 \cap \cdots \cap Q_s$. There is then an injection $A/(Q_1 : x) \to A/I$, by the first isomorphism theorem, so that $\mathrm{Ass}_A(A/(Q_1 : x)) \subseteq \mathrm{Ass}_A(A/I)$. By Lemma 8.14, since $x \notin Q_1$, the colon ideal $Q_1 : x$ is p_1-primary, so that $\mathrm{Ass}_A(A/(Q_1 : x)) = \{p_1\}$.

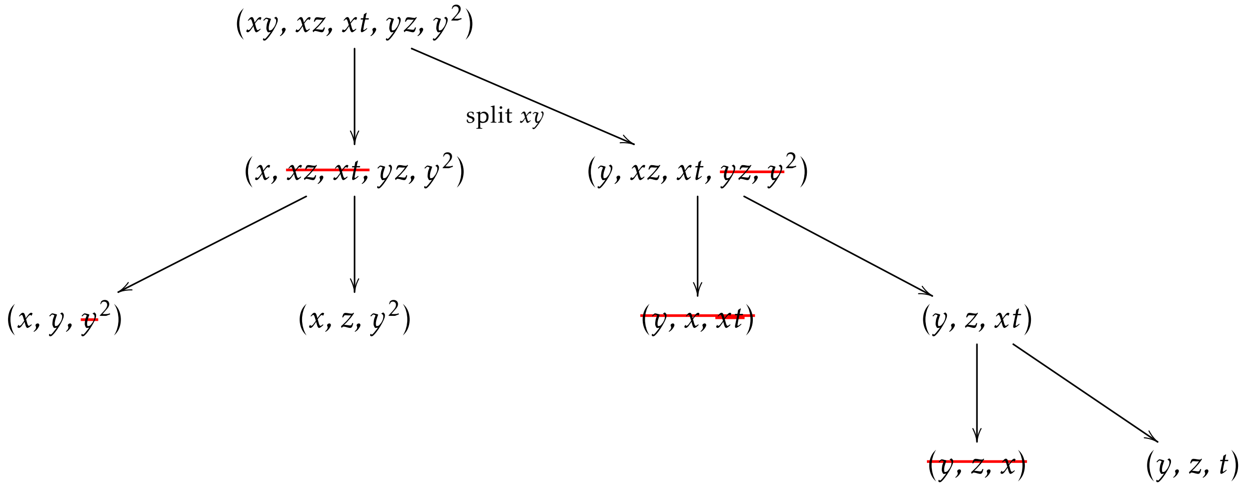
□

Definition 8.17. Let $M \in \mathrm{Mod}(A)$. A submodule $N \lhd M$ is called a ***primary submodule*** if $\#\mathrm{Ass}_A(M/N) = 1$.

Remark 8.18.

- One may repeat essentially the same steps for submodules as we did for ideals, obtaining a very similar theory of primary decompositions for modules.
- If A is a *graded* Noetherian ring and $I \lhd A$ is a homogeneous ideal, there is a theory of primary decompositions with homogeneous factors. In particular the associated primes are homogeneous ideals.
- One may consider a *fine* grading on $A := k[x_1, \ldots, x_n]$, indexed on $\mathbb{N}^n$. For each i, one sets $\deg(x_i) = e_i$, where e_i is the i-th vector of the standard basis, so that, for $\alpha \in \mathbb{N}^n$, the α-th homogeneous component is $A_\alpha = \langle x^\alpha \rangle$, where $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. With respect to this grading, the homogeneous ideals of I are exactly the monomial ideals, i.e., ideals generated by monomials. Also with respect to this grading, one has a primary decomposition as in the previous item above.

Example 8.19. Consider the monomial ideal $I = (xy, xz, xt, yz, y^2)$ in the polynomial ring $k[x,y,z,t]$. In practice, finding a primary decomposition for a monomial ideal is easy, as we simply need to "split" products of distinct variables as follows:



where we cancel unnecessary generators and unnecessary factors in the intersection (because they contain some other factor). All in all, we get the decomposition

$$I = (x, y) \cap (x, z, y^2) \cap (y, z, t),$$

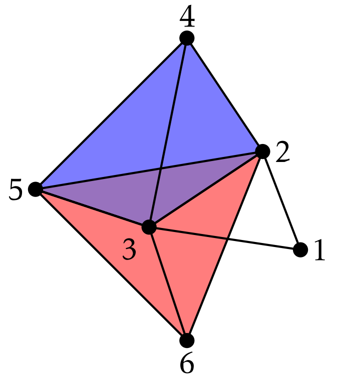
and the radicals are respectively $p_1 = (x,y)$, $p_2 = (x,z,y)$ and $p_3 = (y,z,t)$. They are already pairwise distinct, so we do not need to intersect any of them as in the second part of the proof of Theorem 7.15. As we saw in Lemma 8.11, the minimal primes of I amount for some of associated primes of A/I. The other associated primes of A/I are called ***embedded primes***, and they are generally more difficult to understand. They are the ones whose corresponding factor that can change in a primary decomposition, giving rise to infinitely many primary decompositions as in Example 8.3. In this example, p_1 and p_3 are minimal, but p_2 is not, as $p_1 \subsetneq p_2$. Hence, p_2 is an embedded prime.

8.2 Applications of primary decompositions

Primary decompositions in combinatorics

Monomial ideals, that is, ideals generated by monomials, have a very combinatorial structure, and as we exemplified in Remark 8.2 and Example 8.19, some computations are easier with monomial ideals. They arise for instance in the theory of Gröbner bases, where an arbitrary polynomial ideal I is approached by first studying a monomial ideal, the *initial ideal* of I (generated by the leading monomials of all elements of I). A famous procedure called *polarization* (introduced by Hartshorne) allows to reduce the study of an arbitrary monomial ideal to that of a *squarefree monomial ideal*, that is, an ideal generated by monomials where each variable appears with exponent ≤ 1.

Squarefree monomial ideals in the polynomial ring $k[x_1,\ldots,x_n]$, with n variables, are in bijection with the simplicial complexes on n vertices. Formally, a simplicial complex on the groud set $\{1,\ldots,n\}$ is a collection Δ of subsets of $\{1,\ldots,n\}$ such that if $\sigma \in \Delta$ and $\tau \subseteq \sigma$, then $\tau \in \Delta$. So for instance if $n = 6$, a simplicial complex Δ may be consisting of $\{1,2\}$, $\{1,3\}$, $\{2,3,4,5\}$, $\{2,3,5,6\}$ and all the subsets of these sets, and in more practical terms this simplicial complex looks like this:



The above-mentioned bijection is called the *Stanley–Reisner correspondence*, and it is more than just a bijection: many combinatorial properties of the simplicial complex are translated into algebraic properties of the associated squarefree monomial ideal. Finite simple graphs and their edge ideals below are the simplest objects in this framework:

Definition 8.20. A ***finite simple graph*** $G = (V, E)$ consists of a finite set V, whose elements are called the ***vertices*** of G, and a set E whose elements are subsets of cardinality 2 of V, called the ***edges*** of G. (That is, a finite simple graph consists of vertices and some of them are connected to each other, with no direction for the edges, no loops and no multiple edges between any two given vertices.) Given a finite simple graph $G = (V, E)$ with vertex set $V = \{1, \dots, n\}$, we define the ***edge ideal*** of G as

$$I_G := (x_i x_j \mid \{i, j\} \in E) \quad \subset \quad k[x_1, \dots, x_n],$$

where k is some fixed field.

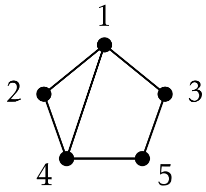
We state it below only for graphs for simplicity, but an analogous result holds in general for arbitrary simplicial complexes:

Proposition 8.21. *Let $G = (V, E)$ be a finite simple graph on $V = \{1, \dots, n\}$. Let $\mathcal{N}$ be the set of non-edges of G, that is, all the subsets of V of cardinality 2 that are not elements of E. Then the "standard" primary decomposition of the edge ideal I_G is*

$$I_G = \bigcap_{F \in \mathcal{N}} (x_i \mid i \in \{1, \dots, n\} \setminus F).$$

The (more general version for arbitrary simplicial complexes of the) proposition above is used in practice to compute what is called the *Alexander dual* of a squarefree monomial ideal.

Example 8.22. Consider the graph



The set of non-edges of G is $\mathcal{N} = \{\{1,5\}, \{2,3\}, \{2,5\}, \{3,4\}\}$, and the standard primary decomposition of I_G is

$$I_G = (x_2, x_3, x_4) \cap (x_1, x_4, x_5) \cap (x_1, x_3, x_4) \cap (x_1, x_2, x_5).$$

Primary decompositions in geometry

Let k be a field and consider the polynomial ring $A := k[x_1,\dots,x_n]$. In classical algebraic geometry, one considers the sets of solutions of polynomial equation systems

$$\begin{cases} f_1(x_1,\dots,x_n) = 0 \\ f_2(x_1,\dots,x_n) = 0 \\ \qquad\vdots \end{cases}$$

and because A is Noetherian, any arbitrary system of such polynomial equations has the same set of solutions as a system with only a finite number of polynomial equations $f_1 = 0,\dots,f_r = 0$. The set of solutions

$$Z(f_1,\dots,f_r) := \left\{a = (a_1,\dots,a_n) \in k^n \mid f_1(a) = 0,\dots,f_r(a) = 0\right\}$$

is called an *(affine) algebraic set*, or an *affine variety*, or some variations of these, depending on the source. If for an ideal $I \lhd A$ one defines

$$Z(I) := \{x \in k^n \mid f(x) = 0 \text{ for all } f \in I\},$$

and I is generated by $f_1,\dots,f_r$, then it turns that $Z(I) = Z(f_1,\dots,f_r)$. An algebraic set is called an *irreducible algebraic set* if it cannot be written as a union of two proper algebraic subsets. A primary decomposition $I = Q_1 \cap \cdots \cap Q_s$ of an ideal corresponds to a decomposition $Z(I) = Z(Q_1) \cup \cdots \cup Z(Q_s)$ of the associated algebraic set into irreducible algebraic sets.

Recall that, as mentioned in Example 8.19, the associated primes of A/I consist of the minimal primes of I and some additional primes, called *embedded primes*. In this context of classical algebraic geometry, the minimal primes are more meaningful. In modern algebraic geometry (such as scheme theory, mentioned in Sections 2.1 and 12.2 and the very end of Appendix C), also embedded primes actually appear.

Primary decompositions and PDEs

Every polynomial with real or complex coefficients can be interpreted as a linear differential operator with constant coefficients. This operator is obtained by simply replacing x_i by the differential operator $\frac{\partial}{\partial x_i}$. Every ideal $I \lhd \mathbb{C}[x_1,\dots,x_n]$ can thus be interpreted as a system of linear PDEs with constant coefficients. The set of solutions to this system is related to a primary decomposition of the ideal I. In this context, both minimal and embedded primes play a role.

The details are out of the scope of this course, so we refer to Chapter 3 of *Invitations to Nonlinear Algebra*, one of the recommended textbooks. We just quote some of the first results in this direction:

Lemma 8.23. *Let $I \lhd \mathbb{C}[x_1,\dots,x_n]$. A point $(a_1,\dots,a_n) \in \mathbb{C}^n$ lies in the algebraic set $Z(I)$ if and only if the exponential function $\exp(a_1x_1 + \cdots + a_nx_n)$ is a solution of the system of PDEs given by I.*

A *zero-dimensional ideal* I is an ideal whose algebraic set $Z(I)$ is zero-dimensional in the geometric sense, that is, $Z(I)$ consists of finitely many points. For two ideals I and J, we denote $I : J^\infty := \bigcup_{n\geq 1}(I : J^n)$ the *saturation of I with respect to J*.

Theorem 8.24. *Let $I \lhd \mathbb{C}[x_1,\dots,x_n]$ be a zero-dimensional ideal, and let $\mathcal{P}$ be the system of PDEs given by I. There exist non-zero polynomial solutions to $\mathcal{P}$ if and only if the maximal ideal $\mathfrak{m} = (x_1,\dots,x_n)$ is associated to I. In that case, the polynomial solutions to $\mathcal{P}$ are precisely the solutions to the system of PDEs given by the $\mathfrak{m}$-primary factor in a primary decomposition of I. More explicitly, the $\mathfrak{m}$-primary factor is $(I : (I : \mathfrak{m}^\infty))$.*

9 Hilbert's theorem on the finite generation of invariants

Invariant theory is the original motivation for some of the theorems by Hilbert, such as the Basis Theorem, that became (and still are) the cornerstones of commutative algebra.

9.1 A-algebras

Definition 9.1. Let A be a ring. An ***A-algebra*** is a pair (B,φ), where B is a ring and $\varphi\colon A \to B$ is a ring homomorphism. A ***subalgebra*** of (B,φ) consists of a subring $C \subseteq B$ with $\operatorname{im}(\varphi) \subseteq C$. A ***homomorphism of A-algebras*** from (B_1,φ_1) to (B_2,φ_2) is a ring homomorphism $\psi\colon B_1 \to B_2$ that makes the diagram

$$\begin{tikzcd}
A \arrow[rr, "\varphi_2"] \arrow[dr, "\varphi_1"'] & & B_2 \\
& B_1 \arrow[ur, "\psi"'] &
\end{tikzcd}$$

commute.

Examples 9.2.

- A typical case is when $A \subseteq B$ is a subring and $\varphi\colon A \hookrightarrow B$ is the inclusion.
- For any ring A, the polynomial ring $A[x_1,\dots,x_n]$ is an A-algebra.
- A quotient A/I is an A-algebra, via the projection.
- Given a multiplicative system $S \subseteq A$, the localization A_S is an A-algebra, via the homomorphism $i_S\colon A \to A_S$. One may re-state the universal property of the localization (Proposition 6.4) in terms of A-algebras.
- Every ring B is a $\mathbb{Z}$-algebra in a unique way, with

$$\begin{aligned}\varphi\colon \mathbb{Z} &\longrightarrow B\\ n &\longmapsto n\cdot 1_B := \underbrace{1_B + \cdots + 1_B}_{n \text{ times}}.\end{aligned}$$

  This is analogous to abelian groups being exactly the $\mathbb{Z}$-modules.

- Let A be a subring of B, and consider the evaluation map $A[x] \to B$ at a fixed $b \in B$. This is a homomorphism of A-algebras.

Remark 9.3. Slightly different definitions of an A-algebra are often given in the literature, such as:

- "a ring B that contains A as a subring": this is the case when $\varphi\colon A \hookrightarrow B$ is the inclusion;
- "a ring B that is also an A-module": the A-module structure is given by restriction of scalars via the map φ (see Exercise 6.11).

Definition 9.4. Let $A \subseteq B$ be an inclusion of rings. Let $b_1,\dots,b_t \in B$. The smallest A-subalgebra of B containing $b_1,\dots,b_t$ (and this exists because the intersection of subalgebras is a subalgebra) is called the ***subalgebra generated by*** $b_1,\dots,b_t$ and it is

$$A[b_1,\dots,b_t] := \Big\{ \sum_{\text{finite}} a_v b_1^{v_1}\cdots b_t^{v_t} \mid v = (v_1,\dots,v_t) \in \mathbb{N}^t,\, a_v \in A \Big\}.$$

That is, $A[b_1,\dots,b_t]$ consists of the polynomials of $A[x_1,\dots,x_t]$ evaluated at $(b_1,\dots,b_t)$.

Examples 9.5.

- Thinking of $\mathbb{R}$ as a $\mathbb{Z}$-algebra, the $\mathbb{Z}$-subalgebra of $\mathbb{R}$ generated by $\sqrt[3]{2}$ is $\mathbb{Z}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \mid a_0, a_1, a_2 \in \mathbb{Z}\}$.
- The polynomial ring $\mathbb{Q}[x]$ is a $\mathbb{Q}$-algebra. The polynomial $2x^{10} = 2(x^3)^2(x^4)$ is in the subalgebra $\mathbb{Q}[x^3, x^4]$, and the polynomial x^2 is not.

Definition 9.6. Let $A \subseteq B$ be an inclusion of rings. We call B a ***finitely generated*** A***-algebra*** if there exist $b_1, \dots, b_t \in B$ such that $B = A[b_1, \dots, b_t]$.

Remark 9.7. Note the difference between being finitely generated as an algebra or as an A-module. For instance,

$$\mathbb{Q}[x] \text{ is } \begin{cases} \text{a } \mathbb{Q}[x]\text{-module, with basis } \{1\}, \\ \text{a } \mathbb{Q}\text{-vector space, with basis } \{x^i\}_{i\in\mathbb{N}}, \\ \text{a } \mathbb{Q}\text{-algebra, generated by } x. \end{cases}$$

Theorem 9.8 (Universal property of the polynomial ring).

1. *Let B be a finitely generated A-algebra, with generators $b_1, \dots, b_n$. There exists a unique A-algebra homomorphism $f : A[x_1, \dots, x_n] \to B$ such that $f(x_i) = b_i$ for all $i \in \{1, \dots, n\}$.*
2. *Let C be an A-algebra that is generated by n elements $c_1, \dots, c_n$ and such that for any A-algebra B generated by $b_1, \dots, b_n$, there exists a unique A-algebra homomorphism $f : C \to B$ such that $f(c_i) = b_i$ for all $i \in \{1, \dots, n\}$. Then $C \cong A[x_1, \dots, x_n]$.*

Proof. Exercise. □

Corollary 9.9. *Any finitely generated A-algebra is (isomorphic to) a quotient of $A[x_1, \dots, x_n]$, for some $n \in \mathbb{N}$.*

9.2 Invariants

For the rest of the section, let $S := k[x_1, \dots, x_n]$ be the polynomial ring in n variables over a field k of characteristic 0. An invertible matrix $g = (g_{ij}) \in \mathrm{GL}_n(k)$ induces a k-algebra automorphism

$$\begin{aligned} \hat{g} \colon S &\longrightarrow S \\ x_i &\longrightarrow \sum_{j=1}^{n} g_{ji} x_j \end{aligned}$$

which is a linear change of variables. For a constant $\lambda \in k$, we have $\hat{g}(\lambda) = \lambda$, and for an arbitrary polynomial $F \in S$, we have $\hat{g}(F(x_1, \dots, x_n)) = F(\hat{g}(x_1), \dots, \hat{g}(x_n))$. This defines a group isomorphism $\mathrm{GL}_n(k) \to \mathrm{Aut}_k(S)$, where $\mathrm{Aut}_k(S)$ is the group of automorphisms of S as a graded k-algebra (that is, k-algebra isomorphisms $S \to S$ that preserve the degree of homogeneous elements).

Definition 9.10. Let G be a group. A k***-linear representation of*** G (on $\mathrm{GL}_n(k)$) is a group homomorphism $\alpha \colon G \to \mathrm{GL}_n(k)$. A polynomial $f \in S = k[x_1, \dots, x_n]$ is ***invariant with respect to*** α (or with respect to G, if α is understood from the context) if

$$\widehat{\alpha(y)}(f) = f \qquad \text{for all } y \in G.$$

Remark 9.11. Often G will simply be a subgroup of $\mathrm{GL}_n(k)$, and $\alpha \colon G \hookrightarrow \mathrm{GL}_n(k)$ will be the inclusion. In this case f is invariant if

$$\hat{g}(f) = f \qquad \text{for all } g \in G.$$

Definition 9.12. We write $S^G := \{f \in S \mid f \text{ is invariant}\}$, where α is implicit.

Remark 9.13.

- The set S^G is a k-subalgebra of S. We have $k \subseteq S^G \subseteq S$.
- The k-algebra S^G is graded: if we decompose a polynomial $f \in S$ into homogeneous components $f = \sum_{i=0}^{d} f_i$, then
$$f \in S^G \qquad \Leftrightarrow \qquad \forall_{i \in \{0,\dots,d\}}\ f_i \in S^G.$$
- Note that S is an S^G-module by restriction of scalars (see Exercise 6.11).

Theorem 9.14 (Hilbert's finiteness theorem)**.** *Let G be a finite group. Then S^G is finitely generated as a k-algebra, that is, there exist $f_1,\dots,f_t \in S^G$ such that $S^G = k[f_1,\dots,f_t]$.*

Proof. Define the map

$$\begin{aligned} \mathcal{R}\colon S &\longrightarrow S^G \\ f &\longmapsto \frac{1}{\#G}\sum_{x\in G}\widehat{\alpha(x)}(f), \end{aligned}$$

called the ***Reynolds operator***. This is well-defined: for any $y \in G$, as the map $x \mapsto yx$ is a bijection $G \to G$, we have

$$\widehat{\alpha(y)}\Big(\frac{1}{\#G}\sum_{x\in G}\widehat{\alpha(x)}(f)\Big) = \frac{1}{\#G}\sum_{x\in G}\widehat{\alpha(y)}\Big(\widehat{\alpha(x)}(f)\Big) = \frac{1}{\#G}\sum_{x\in G}\widehat{\alpha(yx)}(f) = \frac{1}{\#G}\sum_{x\in G}\widehat{\alpha(x)}(f).$$

Verify as an exercise that:

- $f \in S^G$ if and only if $\mathcal{R}(f) = f$,
- $\mathcal{R}(f+h) = \mathcal{R}(f) + \mathcal{R}(h)$ for all $f, h \in S$,
- $\mathcal{R}(fh) = f\mathcal{R}(h)$, for all $f \in S^G$ and all $h \in S$.

These properties amount to say that $\mathcal{R}$ is an S^G-module homomorphism that makes the diagram

$$\begin{tikzcd} S^G \arrow[r, hook] \arrow[rr, bend right, "\mathrm{id}"'] & S \arrow[r, two heads, "\mathcal{R}"] & S^G \end{tikzcd}$$

commute. (This means that for every ideal $I \lhd S^G$, we have $IS \cap S^G = I$, and in the literature this is expressed by saying that S^G is a *pure subring* of S.) Let J be the ideal of S generated by the polynomials f that are invariant, homogeneous and of positive degree. By Hilbert's Basis Theorem 7.5, the ideal J is finitely generated.[3] More precisely, there exist invariant homogeneous polynomials $f_1,\dots,f_t$ of positive degree such that $J = (f_1,\dots,f_t)$. We will prove that $S^G = k[f_1,\dots,f_t]$.

The inclusion ($\supseteq$) is clear, so we show ($\subseteq$). Let $F \in S^G$ be homogeneous, and we show that $F \in k[f_1,\dots,f_t]$ by induction on $\deg(F)$. If $\deg(F) = 0$, this is trivial. So let $\deg(F) > 0$. Then $F \in J$, so that there exist $h_1,\dots,h_t \in S$ that are homogeneous and such that $F = \sum_{i=1}^{t} h_i f_i$ (and we may assume that $h_i = 0$ if $\deg(f_i) > \deg(F)$). By the properties of the Reynolds operator listed above, we have $F = \mathcal{R}(F) = \sum_{i=1}^{t} f_i \mathcal{R}(h_i)$. But $\deg \mathcal{R}(h_i) < \deg(F)$ for all i, so that $\mathcal{R}(h_i) \in k[f_1,\dots,f_t]$ by induction hypothesis. So we are done. □

[3] This step in the proof was the motivation for Hilbert's basis theorem.

Example 9.15. Consider the subgroup $G \subset \mathrm{GL}_n(k)$ consisting of the $n \times n$ permutation matrices. An invariant polynomial $f \in S^G$ is called a ***symmetric polynomial***, because being invariant in this case means that $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$ for any permutation σ of $\{1, \ldots, n\}$. A famous result known as *Newton's theorem* states that S^G is generated as a k-algebra by the ***elementary symmetric polynomials***

$$\begin{aligned} E_1 &:= x_1 + \cdots + x_n \\ E_2 &:= \sum_{1 \le i < j \le n} x_i x_j, \\ &\vdots \\ E_n &:= x_1 \cdots x_n \end{aligned}$$

(that is, E_d is the sum of all degree-d monomials consisting of distinct variables). An alternative set of generators $P_1, \ldots, P_n$ for S^G, since we are assuming that $\mathrm{char}(k) = 0$, consists of the sums of powers of the variables: for each $d \in \mathbb{N}$, set

$$P_d := x_1^d + \cdots + x_n^d.$$

One may express the elementary symmetric polynomials in terms of the power sums and vice versa, by the so-called *Newton's identities*:

$$E_d = \frac{1}{d} \sum_{i=1}^{d} (-1)^{i-1} E_{d-i} P_i, \qquad P_d = (-1)^{d-1} d E_d + \sum_{i=1}^{d-1} (-1)^{d-1-i} E_{k-i} P_i.$$

Example 9.16. Let $S = k[x_1, \ldots, x_n]$ as above. Consider the map

$$\mathbb{Z}_2 \longrightarrow \mathrm{GL}_n(k), \qquad \overline{0} \longmapsto I, \quad \overline{1} \longmapsto -I,$$

where I is the identity matrix.Then $S^{\mathbb{Z}_2} = \{f \in S \mid f(x_1, \ldots, x_n) = f(-x_1, \ldots, -x_n)\}$. Suppose that $\mathrm{char}(k) \neq 2$. Then the polynomials in $S^{\mathbb{Z}_2}$ are those that have only monomials of even degree, so that $S^{\mathbb{Z}_2} = k[x_i x_j \mid 1 \le i \le j \le n]$. This is called the ***Veronese ring*** of order 2 of $S = k[x_1, \ldots, x_n]$. For $n = 2$, for instance, we have $S^{\mathbb{Z}_2} = k[x_1^2, x_1x_2, x_2^2]$, and by considering the surjective map $\varphi\colon k[y_{11}, y_{12}, y_{22}] \to k[x_1^2, x_1x_2, x_2^2]$ defined by $y_{11} \mapsto x_1^2$, $y_{12} \mapsto x_1x_2$ and $y_{22} \longmapsto x_2^2$, we may write

$$S^{\mathbb{Z}^2} \cong k[y_{11}, y_{12}, y_{22}]/\ker(\varphi) = k[y_{11}, y_{12}, y_{22}] \Big/ \left(\det \begin{bmatrix} y_{11} & y_{12} \\ y_{12} & y_{22} \end{bmatrix} \right).$$

Theorem 9.17 (Noether's Degree Bound). *Let G be a finite group. Then S^G is generated by homogeneous invariants of degree $\le \#G$.*

See Section 11.1 of the book *Invitation to Nonlinear Algebra* for a proof.

10 Tensor products

From a commutative algebra perspective, tensors are a sort of "non-commutative polynomials". One reason why the tensor product $M \otimes N$ of two A-modules M and N is theoretically interesting is that the module of *bilinear* maps (a strange concept) from $M \times N$ to a third module P is isomorphic to the module of *linear* maps (that is, A-module homomorphisms, a concept we are familiar with) from $M \otimes N$ to P. In this course, one important feature is that the tensor product with a fixed module N, that is, the map $M \mapsto M \otimes N$, is a nice functor $\mathrm{Mod}(A) \to \mathrm{Mod}(A)$.

Definition 10.1. Let A be a ring and $M, N, P \in \mathrm{Mod}(A)$. A function $f\colon M \times N \to P$ is A-***bilinear*** if, for all $m \in M$ and all $n \in N$, the functions

$$f(m,-)\colon N \longrightarrow P \qquad \text{and} \qquad f(-,n)\colon M \longrightarrow P$$

are A-module homomorphisms. The set $\mathrm{Bil}(M,N,P)$ of bilinear functions $M \times N \to P$ is an A-module, with pointwise addition and multiplication by scalars.

Remarks 10.2.

- Bilinear maps are not linear (that is, A-module homomorphisms) in general: for instance the scalar multiplication $A \times M \to M$ is bilinear but in general not linear.
- Let $f\colon M \times N \to P$ be bilinear and let $g\colon P \to Q$ be linear. Then $g \circ f\colon M \times N \to Q$ is bilinear.
- Let $g_1\colon M_1 \to M$ and $g_2\colon N_1 \to N$ be linear, and let $f\colon M \times N \to P$ be bilinear. Then $f \circ (g_1 \times g_2)\colon M_1 \times N_1 \to P$ is bilinear.

Definition 10.3. For any set X, define $F_X := \left\{ f\colon X \to A \mid \#\{x \in X \mid f(x) \neq 0\} < +\infty \right\}$. Then F_X is an A-module, with pointwise addition and multiplication by scalars. Moreover, F_X is free as an A-module, with basis $\{e_x\}_{x \in X}$, where we define

$$e_x\colon X \longrightarrow A, \qquad y \longmapsto \begin{cases} 0 & \text{if } y \neq x, \\ 1 & \text{if } y = x. \end{cases}$$

For instance, if $M, N \in \mathrm{Mod}(A)$, then $F_{M \times N}$ is a free module, and a general element of $F_{M \times N}$ is of the form $a_1 e_{(m_1,n_1)} + a_2 e_{(m_2,n_2)} + \cdots + a_r e_{(m_r,n_r)}$. (This is a huge module.)

Definition 10.4. Let $M, N \in \mathrm{Mod}(A)$. Consider the submodule D of $F_{M \times N}$ generated by all the elements of the form

$$e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)}, \qquad e_{(am,n)} - a e_{(m,n)},$$

$$e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)}, \qquad e_{(m,an)} - a e_{(m,n)},$$

for $m_1, m_2, m \in M$, $n_1, n_2, n \in N$ and $a \in A$. The ***tensor product of*** M ***and*** N ***(over*** A***)*** is the quotient

$$M \otimes_A N := F_{M \times N}/D.$$

(We omit the A if it is clear from the context.) For $m \in M$ and $n \in N$, we denote $m \otimes n := \overline{e_{(m,n)}}$ the equivalence class in $M \otimes N$, and we call $m \otimes n$ the ***tensor product of*** m ***and*** n. Elements of the form $m \otimes n$ are called ***elementary tensors***.

Remarks 10.5.

- The tensor product $M \otimes N$ does not only consist of elementary tensors. A general element of $M \otimes N$ is an A-linear combination of elementary tensors, that is, an element of the form $a_1(m_1 \otimes n_1) + a_2(m_2 \otimes n_2) + \cdots + a_r(m_r \otimes n_r)$.

- Because D is generated by the elements listed above, in $M\otimes N$ we have the equalities
$$(m_1+m_2)\otimes n = m_1\otimes n + m_2\otimes n, \qquad (an)\otimes n = a(m\otimes n),$$
$$m\otimes (n_1+n_2) = m\otimes n_1 + m\otimes n_2, \qquad m\otimes (an) = a(m\otimes n),$$
where $\otimes$ takes precedence over $+$, for all $m_1, m_2, m \in M$, $n_1, n_2, n\in N$ and $a\in A$.

Lemma 10.6. *If $h\colon U\to V$ is an A-module homomorphism and $U_1 \lhd U$ is a submodule such that $U_1\subseteq \ker(h)$, then the map*
$$h'\colon U/U_1 \longrightarrow V, \qquad \overline{u}\longmapsto h(u)$$
is an A-module homomorphism.

Proof. Exercise. □

Definition 10.7. Define the bilinear (by the equalities in the previous remark!) map
$$\begin{aligned}\varphi\colon M\times N &\longrightarrow M\otimes N\\ (m,n)&\longmapsto m\otimes n.\end{aligned}$$

As it was the case for the universal property of the localization, the following universal property allows to prove results more elegantly than using the explicit definition of $M\otimes N$ given above, and in practice it helps in defining maps from $M\otimes N$ (which is not totally trivial, as $M\otimes N$ is constructed explicitly as a quotient).

Proposition 10.8 (Universal property of the tensor product). *1. The pair $(M\otimes N,\varphi)$ has the following property: for every A-module P and every bilinear map $f\colon M\times N\to P$, there exists a unique A-module homomorphism $g\colon M\otimes N\to P$ that makes the diagram*

$$\begin{tikzcd} M\times N \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & P \\ & M\otimes N \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

commute, that is, $g\circ\varphi = f$.

2. The pair $(M\otimes N,\varphi)$ is unique in the following sense. Let (T,φ') be another pair satisfying the same property, that is, let $T\in \mathrm{Mod}(A)$ and $\varphi'\colon M\times N\to T$ be a bilinear map such that for every $P\in\mathrm{Mod}(A)$ and for every bilinear map $f\colon M\times N\to P$, there exists a unique A-module homomorphism $g\colon T\to P$ that makes the diagram

$$\begin{tikzcd} M\times N \arrow[rr, "f"] \arrow[dr, "\varphi'"'] & & P \\ & T \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

commute. Then $T\cong M\otimes N$.

Proof. We prove part (1) and leave part (2) as an exercise. Let $P\in\mathrm{Mod}(A)$ and let $f\colon M\times N\to P$ be a bilinear map. By the universal property of free modules, there exists a unique homomorphism $h\colon F_{M\times N}\to P$ such that $h(e_{(m,n)}) = f(m,n)$, for all $(m,n)\in M\times N$. Note that the submodule D of Definition 10.4 is contained in $\ker(h)$. Therefore, by Lemma 10.6, there is an induced homomorphism (called h' in the lemma) from the quotient $F_{M\times N}/D = M\otimes N$

$$g\colon M\otimes N \longrightarrow P \quad \text{such that} \quad m\otimes n \longmapsto f(m,n).$$

The diagram in the statement commutes. In order to show that g is unique, note that the elementary tensors $m\otimes n$ generate $M\otimes N$ as an A-module. Let $g_1\colon M\otimes N \to P$ be another homomorphism that makes the diagram commute. Then we necessarily have

$$g_1(m\otimes n) = g_1\circ\varphi((m,n)) = f(m,n) = g(m\otimes n),$$

and consequently $g = g_1$ on the whole $M\otimes N$. □

Corollary 10.9. *The A-module $\mathrm{Bil}(M,N,P)$ of bilinear maps $M\times N\to P$ is isomorphic to the A-module $\mathrm{Hom}(M\otimes N,P)$ of linear maps $M\otimes N\to P$. Explicitly,*

$$\mathrm{Hom}(M\otimes N,P)\longrightarrow \mathrm{Bil}(M,N,P), \qquad \alpha\longmapsto \alpha\circ\varphi$$

is an isomorphism.

Examples 10.10.

- For any $M,N\in\mathrm{Mod}(A)$, and for any $n\in N$, we have $0\otimes n = 0$. Indeed, $0\otimes n = (0+0)\otimes n = 0\otimes n + 0\otimes n$. Similarly, $m\otimes 0 = 0$ for all $m\in M$.
- If $I,J\lhd A$ are coprime ideals (that is, $I+J=A$), then $A/I\otimes_A A/J = 0$. Exercise. (It is enough to check that all the elementary tensors are zero.) So for instance $\mathbb{Z}_2\otimes_{\mathbb{Z}}\mathbb{Z}_3 = 0$.
- Let $M'\lhd M$ and $N'\lhd M$, and let $x\in M'$ and $y'\in N'$. It is possible that $x\otimes y\neq 0$ in $M'\otimes N'$, but $x\otimes y = 0$ in $M\otimes N$. For example, take $A=M=\mathbb{Z}$, and $M' = 2\mathbb{Z}\lhd\mathbb{Z}$, and take $N'=N=\mathbb{Z}/2\mathbb{Z}$. Then $2\otimes 1 = 0$ in $M\otimes N$, but $2\otimes 1\neq 0$ in $M'\otimes N'$.

Lemma 10.11. *If $M=\langle m_1,\dots,m_s\rangle$ and $N=\langle n_1,\dots,n_t\rangle$ are finitely generated A-modules, then $M\otimes N = \langle m_i\otimes n_j \mid i=1,\dots,s,\ j=1,\dots,t\rangle$.*

Proof. We know that $M\otimes N$ is generated by all elementary tensors of the form $m\otimes n$. If $m=\sum_{i=1}^s a_i m_i$ and $n=\sum_{j=1}^t b_j n_j$, then $m\otimes n = \sum_{i=1}^s\sum_{j=1}^t a_i b_j (m_i\otimes n_j)$. □

Observe that the lemma above does not imply that, if $\{m_1,\dots,m_s\}$ and $\{n_1,\dots,n_t\}$ are minimal systems of generators for M and N, then $\{m_i\otimes n_j\}_{i,j}$ is a minimal system of generators for $M\otimes N$. Consider for instance $\mathbb{Z}_2\otimes\mathbb{Z}_3 = 0$.

Lemma 10.12. *For $M,N\in\mathrm{Mod}(A)$, we have $M\otimes N\cong N\otimes M$.*

Proof. We want to show that the map $m\otimes n\mapsto n\otimes m$ defines an isomorphism. (Always remember that not all elements of $M\otimes N$ are of the form $m\otimes n$.)

One may check that the function $M\times N\to N\otimes M$ defined by $(m,n)\mapsto n\otimes m$ is bilinear. By the universal property, there exists then a unique linear map $g_1\colon M\otimes N\to N\otimes M$ such that $m\otimes n\mapsto n\otimes m$. Similarly, there is a linear map $g_2\colon N\otimes M\to M\otimes N$ such that $n\otimes m\mapsto m\otimes n$. Since the elementary tensors generate the tensor product, one deduces that $g_2\circ g_1 = \mathrm{id}$ and $g_1\circ g_2 = \mathrm{id}$, so that the maps g_1 and g_2 are isomorphisms. □

Lemma 10.13. *For any $M\in\mathrm{Mod}(A)$, we have $A\otimes M\cong M$.*

Proof. Exercise. □

Definition 10.14. For A-modules $M_1,\dots,M_n,P$, a function $f\colon M_1\times\cdots\times M_n\to P$ is called an *n-(multi)linear map* if, for any $i\in\{1,\dots,n\}$, if we fix $m_1\in M_1,\dots,m_{i-1}\in M_{i+1},m_{i+1}\in M_{i+1},\dots,m_n\in M_n$, then the map

$$f(m_1,m_2,\dots,m_{i-1},-,m_{i+1},\dots,m_n)\colon M_i\longrightarrow N$$

is an A-module homomorphism. Denote by $\mathrm{Mult}(M_1,\dots,M_n,P)$ the set of such functions. This is an A-module, with the usual pointwise sum and multiplication by scalars.

One may construct the ***tensor product*** $M_1\otimes\cdots\otimes M_n$ similarly to the case of the tensor product of two modules, as a quotient of $F_{M_1\times\cdots\times M_n}$. The elements of the form $m_1\otimes\cdots\otimes m_n$ are called ***elementary tensors*** and they generate $M_1\otimes\cdots\otimes M_n$ as an A-module. The general element of $M_1\otimes\cdots\otimes M_n$ is a finite sum $\sum_{j=1}^s a_j m_{1j}\otimes m_{2j}\otimes\cdots\otimes m_{nj}$, with $m_{ij}\in M_i$ for all i. Again similarly to the tensor product of two modules, one defines in general the multilinear map

$$\varphi\colon M_1\times\cdots\times M_n\longrightarrow M_1\otimes\cdots\otimes M_n,\qquad (m_1,\dots,m_n)\longmapsto m_1\otimes\cdots\otimes m_n.$$

The general version of Proposition 10.8, for tensor products of n modules, is the following:

Proposition 10.15 (Universal property of tensor product). 1. *For any module P and for any n-multilinear map $f\colon M_1\times\cdots\times M_n\to P$, there exists a unique A-module homomorphism $g\colon M_1\otimes\cdots\otimes M_n\to P$ that makes the diagram*

$$\begin{tikzcd}
M_1\times\cdots\times M_n \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & P \\
& M_1\otimes\cdots\otimes M_n \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

commute. In particular $\mathrm{Hom}(M_1\otimes\cdots\otimes M_n,P)\cong\mathrm{Mult}(M_1,\dots,M_k,P)$ *as A-modules.*

2. *If the pair (T,φ'), where $\varphi'\colon M_1\times\cdots\times M_n\to T$ is an n-multilinear map, satisfies the same property as $(M_1\otimes\cdots\otimes M_n,\varphi)$ above, then $T\cong M_1\otimes\cdots\otimes M_n$.*

Remarks 10.16. 1. As it was the case for the tensor product of two modules, the elementary tensors are special elements of $M_1\otimes\cdots\otimes M_n$. The general element is a linear combination of elementary tensors.

2. If $M_1,\dots,M_n$ are finitely generated, then $M_1\otimes\cdots\otimes M_n$ is finitely generated (for instance by the elementary tensors).

3. If each M_i is a free module of rank r_i, then $M_1\otimes\cdots\otimes M_n$ is free of rank $r_1\cdots r_k$. Vector spaces are always free, but arbitrary modules are in general not free. If you know tensor products for vector spaces, this is one of the main differences.

Lemma 10.17. *For any $M_1,M_2,M_3\in\mathrm{Mod}(A)$, we have $(M_1\otimes M_2)\otimes M_3\cong M_1\otimes M_2\otimes M_3\cong M_1\otimes(M_2\otimes M_3)$.*

Proof. Exercise. Use the universal property in a similar way to Lemma 10.12. □

10.1 Functorial properties of the tensor product

Definition 10.18. Let $M_1, M_2, N \in \mathrm{Mod}(A)$, and let $f\colon M_1 \to M_2$ be an A-module homomorphism. Then we define the A-module homomorphism

$$\begin{aligned} f \otimes N \colon M_1 \otimes N &\longrightarrow M_2 \otimes N \\ m \otimes n &\longmapsto f(m) \otimes n. \end{aligned}$$

(Check as an exercise that this is indeed well-defined and a homomorphism.)

Definition 10.19. For a fixed $N \in \mathrm{Mod}(A)$, we define the following functor

$$\begin{tikzcd} \mathrm{Mod}(A) \arrow[rr, "(-)\otimes N"] & & \mathrm{Mod}(A) \\ M_1 \arrow[d, "f"'] \arrow[r, phantom, "\mapsto"] & {} & M_1 \otimes N \arrow[d, "f\otimes N"] \\ M_2 \arrow[r, phantom, "\mapsto"] & {} & M_2 \otimes N \end{tikzcd}$$

$$\begin{tikzcd} M_1 \arrow[d, "f"'] & \mapsto & M_1 \otimes N \arrow[d, "f\otimes N"'] \\ {} & \mapsto & {} \\ M_2 & \mapsto & M_2 \otimes N \end{tikzcd}$$

and similarly $N \otimes (-)$, which gives an isomorphic result by Lemma 10.12.

Proposition 10.20. 1. *For any fixed $N \in \mathrm{Mod}(A)$, the construction above is functorial, that is:*

- *for any $M \in \mathrm{Mod}(A)$, we have $\mathrm{id}_M \otimes N = \mathrm{id}_{M\otimes N}$;*
- *for A-module maps $f\colon M \to N$ and $g\colon N \to P$, we have $(g\circ f)\otimes N = (g\otimes N)\circ(f\otimes N)$.*

2. *The functor $(-)\otimes N$ is a **right-exact functor**, that is, if $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is an exact sequence of A-modules, then*

$$M_1 \otimes N \xrightarrow{f\otimes N} M_2 \otimes N \xrightarrow{g\otimes N} M_3 \otimes N \longrightarrow 0$$

is an exact sequence of A-modules.

Proof. Exercise. □

Definition 10.21. Let $N \in \mathrm{Mod}(A)$ be such that the functor $(-)\otimes N$ is exact (or equivalently, such that $N\otimes(-)$ is exact), which means that if $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is an exact sequence of A-modules, then $0 \to M_1 \otimes N \xrightarrow{f\otimes N} M_2 \otimes N \xrightarrow{g\otimes N} M_3 \otimes N \to 0$ is an exact sequence of A-modules. Then N is called a ***flat module***.

As the name suggests, flat modules have applications in algebraic geometry (that are out of the scope of this course).

The Tor-functors

In Section 5.2, we defined a *free resolution* of $M \in \operatorname{Mod}(A)$ as an exact sequence of the form

$$\ldots \longrightarrow F_3 \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

where all the F_i's are free A-modules.

Definition 10.22. A sequence of A-module homomorphisms

$$\mathcal{C}: \quad \ldots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \ldots$$

is called a ***(chain) complex*** if $\operatorname{im}(d_{i+1}) \subseteq \ker(d_i)$ for all i, or equivalently if $d_i \circ d_{i+1} = 0$ for all i. The A-module $H_i(\mathcal{C}) := \ker(d_i)/\operatorname{im}(d_{i+1}$ is called the ***i-th homology*** of the complex $\mathcal{C}$.

Resolutions are exact complexes, that is, where $H_i = 0$ for all i.

From now on, all functors considered will be covariant, that is, they do not invert the direction of the arrows.

Definition 10.23. A functor $F\colon \operatorname{Mod}(A) \to \operatorname{Mod}(A)$ is called an ***additive functor*** if, for all $M, N \in \operatorname{Mod}(A)$, the map

$$\operatorname{Hom}_A(M,N) \longrightarrow \operatorname{Hom}_A(F(M),F(N)), \qquad f \longmapsto F(f)$$

is a homomorphism of abelian groups.

Remark 10.24. The functors we consider in this course, that is, tensor product, Hom and localization, are all additive. By definition, any functor F "preserves compositions", in the sense that if f and g are composable homomorphisms, then $F(g \circ f) = F(g) \circ F(f)$. Note that additive functors map the zero map to the zero map, so that they map a chain complex $\mathcal{C}$ to a chain complex $F(\mathcal{C})$, since $F(d_i) \circ F(d_{i+1}) = F(d_i \circ d_{i+1}) = F(0) = 0$. In particular, a resolution is mapped to a chain complex (with possibly non-zero homology) by such functors.

See Appendix D if you are not familiar with homomorphisms of chain complexes and homotopy.

Theorem 10.25. *Let $F\colon \operatorname{Mod}(A) \to \operatorname{Mod}(A)$ be a right-exact additive functor. Let $M \in \operatorname{Mod}(A)$ and let $\mathcal{P}$ and $\mathcal{Q}$ be two free resolutions of M. Then $F(\mathcal{P})$ and $F(\mathcal{Q})$ have the same homology.*

Proof sketch. Say that the given resolution $\mathcal{P}$ in the statement is $\cdots \to P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} M \to 0$ and the resolution $\mathcal{Q}$ is $\cdots \to Q_1 \xrightarrow{q_1} Q_0 \xrightarrow{q_0} M \to 0$. By the Comparison Theorem D.5, there exist homomorphisms $\varphi\colon \mathcal{P} \to \mathcal{Q}$ and $\psi\colon \mathcal{Q} \to \mathcal{P}$ such that $\psi \circ \varphi \sim \operatorname{id}_{\mathcal{P}}$ and $\varphi \circ \psi \sim \operatorname{id}_{\mathcal{Q}}$. So in particular, for all $n \in \mathbb{N}$, we have A-module maps $s_n\colon P_n \to P_{n+1}$ such that

$$\psi_n \circ \varphi_n - \operatorname{id}_{P_n} = p_{n+1} \circ s_n + s_{n-1} \circ p_n,$$

and since F is additive, this implies that

$$F(\psi_n) \circ F(\varphi_n) - \operatorname{id}_{F(P_n)} = F(p_{n+1}) \circ F(s_n) + F(s_{n-1}) \circ F(p_n),$$

so that $F(\mathcal{P})$ and $F(\mathcal{Q})$ are homotopy equivalent, and hence they have the same homology by Proposition D.4. (See Appendix D and for instance the book *Introduction to homological algebra* by Weibel for more details.) □

Definition 10.26. Let M and N be two A-modules. Consider any free resolution $\mathcal{F}$ of M. The homology of the complex $\mathcal{F} \otimes N$ does not depend on the choice of $\mathcal{F}$, by Theorem 10.25. The i-th homology $H_i(\mathcal{F} \otimes N)$ is denoted by $\operatorname{Tor}_i(M,N)$.

(This is a special case of the more general concept of a *derived functor*.)

Theorem 10.27. *For $M, N \in \operatorname{Mod}(A)$, we have $\operatorname{Tor}_i(M,N) \cong \operatorname{Tor}_i(N,M)$ for all i.*

Proof. Exercise. □

10.2 Tensor algebra and exterior algebra of a module

For $M \in \mathrm{Mod}(A)$ and $n \in \mathbb{N}$, denote $M^{\otimes n} := M \otimes \cdots \otimes M$, with n factors. For any two exponents $s, t \in \mathbb{N}$, define the "concatenation product"

$$\begin{aligned} M^{\otimes s} \times M^{\otimes t} &\longrightarrow M^{\otimes(s+t)} \\ (m_1 \otimes \cdots \otimes m_s,\ n_1 \otimes \cdots \otimes n_t) &\longmapsto m_1 \otimes \cdots \otimes m_s \otimes n_1 \otimes \cdots \otimes n_t. \end{aligned}$$

One may check that this map is bilinear.

Definition 10.28. The ***tensor algebra*** of $M \in \mathrm{Mod}(A)$ is

$$T_A(M) := \bigoplus_{n=0}^{+\infty} M^{\otimes n},$$

where we set $M^{\otimes 0} := A$ and $M^{\otimes 1} := M$. This is of course an A-module, since it is a direct sum of A-modules, but it is also an A-algebra, with multiplication given by the concatenation defined above. We also write $T(M)$ for $T_A(M)$.

Remarks 10.29.

- Recall that in a direct sum at most finitely many entries are non-zero. An element of $T(M)$ looks like

$$(3,\ m,\ m_1 \otimes m_2 + m_3 \otimes m_4,\ 0,\ m_5 \otimes m_6 \otimes m_7 \otimes m_8,\ 0,\ 0,\ \dots)$$

(assuming that 3 makes sense in A).

- The elements of M, thought of as $M^{\otimes 1}$, generate $T_A(M)$ as an A-algebra.
- The tensor algebra $T(M)$ is in general *not* commutative: if $m, n \in M = M^{\otimes 1}$, then in general $m \cdot_{T(M)} n = m \otimes n \neq n \otimes m = n \cdot_{T(M)} m$.

Examples 10.30.

- By Lemma 10.13, we know that $A \otimes A \cong A$, and in general $A^{\otimes n} \cong A$, by induction. As a result, we get the isomorphism

$$T_A(A) \cong A[x],$$

where x corresponds to the element 1 of $A^{\otimes 1}$. This is a *very special case*.

- Let us consider $T_A(A^2)$. By combining Lemma 10.13 with some of the homework exercises, we have for instance

$$(A^2)^{\otimes 3} = A^2 \otimes A^2 \otimes A^2 \cong A^{2^3} = A^8,$$

and in general $(A^2)^{\otimes n} \cong A^{2^n}$. If we denote by e_1 and e_2 some basis elements for A^2, so that $A^2 = \langle e_1, e_2 \rangle$, then for instance we have $(A^2)^{\otimes 2} = \langle e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2 \rangle$. In conclusion, $T_A(A^2)$ is isomorphic to the *"non-commutative polynomial ring"* $A[e_1, e_2]$.

- Similarly, $T_A(A^n)$ is isomorphic to the *"non-commutative polynomial ring"* $A[e_1, \dots, e_n]$.

Definition 10.31. Let $M \in \mathrm{Mod}(A)$ and define the ideal $J := (m_1 \otimes m_2 + m_2 \otimes m_1 \mid m_1, m_2 \in M)$. The ***exterior algebra of*** M is the quotient

$$\bigwedge M := T_A(M)/J.$$

(The symbol $\wedge$ is read "wedge".) The equivalence class of $m_1 \otimes \cdots \otimes m_r \in T_A(M)$ in $\bigwedge M$ is denoted $m_1 \wedge \cdots \wedge m_r$. The submodule $\bigwedge^n M := \langle m_1 \wedge \cdots \wedge m_n \mid m_1, \dots, m_n \in M \rangle$, for $n \in \mathbb{N}$, is called the ***n-th exterior power*** of M. We have $\bigwedge M = \bigoplus_{n=0}^{+\infty} \bigwedge^n M$.

Remarks 10.32.

- The algebra $T_A(M)$ is not commutative in general, so one has to be careful: most ideals will be right of left ideals, but not bilateral. But the ideal J defined above is indeed bilateral.
- The exterior algebra $\bigwedge M$ is an A-algebra. Like $T_A(M)$, it is in general not commutative, but almost: $\bigwedge M$ is *anti-commutative*, that is, $m_1 \wedge m_2 = -m_2 \wedge m_1$ for all $m_1, m_2 \in M$.
- If we repeat the same construction as in Definition 10.4 but this time we consider $N = M$ and $D' := D + \langle e_{(m_1,m_2)} + e_{(m_2,m_1)} \mid m_1, m_2 \in M\rangle$, then we get $\bigwedge^2 M = F_{M\times M}/D'$.
- Consider the ideal $J' := (m_1 \otimes m_1 \mid m_1 \in M)$ in $T_A(M)$. Then $J \subseteq J'$, as $m_1 \otimes m_2 + m_2 \otimes m_1 = (m_1+m_2)\otimes(m_1+m_2) - (m_1\otimes m_1 + m_2 \otimes m_2)$ is the difference of two elements of J'. Now consider $m_2 = m_1$ and observe that $2(m_1 \otimes m_1) = m_1 \otimes m_1 + m_1 \otimes m_1 \in J$. Hence, if $2 \in \mathcal{U}(A)$, then $m_1 \otimes m_1 \in J$, and $J = J'$.

Assume for the rest of the section that $2 \in \mathcal{U}(A)$, so that $J = J'$ as in the remark above. Then $m \wedge m = 0$ for all $m \in M$.

Remark 10.33. If $M = \langle m_1, \dots, m_t\rangle$ is a finitely generated A-module, then

$$\bigwedge^n M = \langle m_{i_1} \wedge \cdots \wedge m_{i_n} \mid 1 \le i_1, \dots, i_n \le t\rangle = \langle m_{i_1} \wedge \cdots \wedge m_{i_n} \mid 1 \le i_1 < \cdots < i_n \le t\rangle.$$

So in particular $\bigwedge^{t+1} M = \bigwedge^{t+2} M = \cdots = 0$, and $\bigwedge M = \bigoplus_{n=0}^{t} \bigwedge^n M$.

Definition 10.34. Let $M, P \in \operatorname{Mod}(A)$. An n-multilinear map $f\colon M \times \cdots \times M \to P$ is ***alternating*** if $f(m_1, \dots, m_n) = (-1)^{\operatorname{sign}(\sigma)} f(m_{\sigma(1)}, \dots, m_{\sigma(n)})$ for any permutation $\sigma \in S_n$. (Equivalently, if $f(m_1, \dots, m_{i-1}, m_i, m_{i+1}, m_{i+2}, \dots, m_n) = -f(m_1, \dots, m_{i-1}, m_{i+1}, m_i, m_{i+2}, \dots, m_n)$ for all i.)

Proposition 10.35 (Universal property of the exterior powers)**.** *Let $M \in \operatorname{Mod}(A)$. The exterior power $\bigwedge^n M$ satisfies the following universal property: for any $P \in \operatorname{Mod}(A)$ and for any alternating map $f\colon M \times \cdots \times M \to P$, there exists a unique A-module map $g\colon \bigwedge^n M \to P$ that makes the diagram*

$$\begin{tikzcd}
M \times \cdots \times M \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & P \\
& \bigwedge^n M \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

commute, where $\varphi(m_1, \dots, m_n) := m_1 \wedge \cdots \wedge m_n$.

Examples 10.36.

- Consider $M = A^2 = \langle e_1, e_2\rangle$. We describe $\bigwedge A^2$. First of all $\bigwedge^n A^2 = 0$ for $n > 2$, by Remark 10.33. The nonzero summands are $\bigwedge^0 A^2 = A$, $\bigwedge^1 A^2 = A^2$ and $\bigwedge^2 A^2 = \langle e_1 \wedge e_2\rangle$. Observe that $e_1 \wedge e_2$ is linearly independent: let $a \in A$ be such that $ae_1 \wedge e_2 = 0$ and consider the diagram

$$\begin{tikzcd}
A^2 \times A^2 \arrow[rr, "\det"] \arrow[dr, "\varphi"'] & & A \\
& \bigwedge^2 A^2 \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

  where g is such that $g(e_1 \wedge e_2) = 1$. Then $a = a1 = ag(e_1 \wedge e_2) = g(ae_1 \wedge e_2) = 0$. Thus, $\bigwedge A^2$ is a free A-module, with basis $\{1, e_1, e_2, e_1 \wedge e_2\}$.

- In general, $\bigwedge A^t$ is a free A-module of rank 2^t. If we write $A^t = \langle e_1, \dots, e_t\rangle$, then an A-algebra, $\bigwedge A^t = A[e_1, \dots, e_t]$, with the relations

$$e_i^2 = 0, \qquad e_i \wedge e_j = -e_j \wedge e_i.$$

11 Hilbert functions and Hilbert's sygygy theorem

For the whole section, let $S := k[x_1, \ldots, x_n]$ be the polynomial ring in n variables over a field k. Recall that S is a graded ring (in the standard way), and by Hilbert's Basis Theorem 7.5, S is Noetherian.

Hilbert's Finiteness Theorem 9.14 shows that the algebra of invariants S^G, consisting of polynomials that are invariant under the action of some group G (at least in case G is finite and $\mathrm{char}(k) = 0$, but it holds in much greater generality) is a finitely generated k-algebra. By Theorem 9.8, S^G is then isomorphic to a quotient of some polynomial ring, modulo an ideal. Such a quotient is a module over that polynomial ring.

Besides studying the finiteness of generating sets, Hilbert was interested in another numerical measure of how large a ring of invariant is, and that is now called the "Hilbert function". This was later generalized to more general modules and is defined below. Consider the standard grading of $S = \bigoplus_{i=0}^{+\infty} S_i$, where S_i consists of the polynomials that are homogeneous in the usual sense and of degree i, so that in particular $S_0 = k$.

Definition 11.1. Let $M = \bigoplus_{i \in \mathbb{Z}} M_i$ be a finitely generated graded S-module.[4] The ***Hilbert function of*** M is the function

$$H_M \colon \mathbb{Z} \longrightarrow \mathbb{N}, \qquad H_M(t) := \dim_k(M_t),$$

where the dimension of M_t is taken as a k-vector space.

(The fact that the definition makes sense is left as an exercise.)

The following is another one of the cornerstone results for commutative algebra (together with the basis theorem, the syzygy theorem below, and the Nullstellensatz in Lecture 12) published by Hilbert in a couple of landmark papers in the 1890's .

Theorem 11.2 (Hilbert)**.** *Let M be a finitely generated graded S-module. Then the Hilbert function of M eventually agrees with a polynomial. More precisely, there exists a polynomial $P_M \in k[x]$ of degree $\leq n-1$, called the* **Hilbert polynomial of** *M, that satisfies $H_M(t) = P_M(t)$ for all sufficiently large t.*

We prove this result in Section 11.2. The main ingredient will be the so-called Syzygy Theorem, also by Hilbert.

Remark 11.3. Of course it does not make sense to ask that the equality $H_M(t) = P_M(t)$ holds for *all* indices t: for instance if $M = S$ then we have $H_S(t) = 0$ for $t < 0$ and $H_S(t) > 0$ for $t \geq 0$, and there is no polynomial with the same behavior.

11.1 Hilbert's syzygy theorem

In Section 5.2, we defined a *free resolution* of $M \in \mathrm{Mod}(A)$ as an exact sequence of the form

$$\ldots \longrightarrow F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \longrightarrow 0,$$

where all the F_i's are free A-modules. We saw how to construct a free resolution of a given module: first define $d_0 \colon F_0 \to M$ as a surjection. Then we define a map $d_1 \colon F_1 \to F_0$ so that $\mathrm{im}(d_1) = \ker(d_0)$. Similarly, we define $d_2 \colon F_2 \to F_1$ so that $\mathrm{im}(d_2) = \ker(d_1)$. And so on. *At each step we construct a surjection onto the kernel of the map constructed in the previous step.*

[4] Recall that being graded means in particular that $S_i M_j \subseteq M_{i+j}$ for all i, j.

Remark 11.4. The algorithm above is implemented in computer algebra systems (involving Gröbner basis methods) and can be run to get a free resolution of a given finitely generated S-module. However, one does not know what to expect a priori. There are very few classes of modules for which an explicit description of a resolution, with closed formulas, is given. The maximal ideal $(x_1,\dots,x_n) \lhd S$ happens to be in one of these classes, and a resolution for it is described in Definition 11.17 below.

Definition 11.5. Let M be an S-module. We call ***projective dimension of*** M, denoted $\operatorname{projdim}(M)$, the smallest $p \in \mathbb{N}$ such that there exists a free resolution of M of the form

$$0 \longrightarrow F_p \longrightarrow F_{p-1} \longrightarrow \dots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

with $F_i \neq 0$ for all $i \in \{0,\dots,p\}$, if such an n exists. Otherwise, we set $\operatorname{projdim}(M) = +\infty$.

Fun Fact 11.6. Consider $S = \mathbb{R}[x,y,z]$ and its field of fractions $S_{(0)}$. A result from the 1960's states that the projective dimension of $S_{(0)}$ as an S-module is either 2 or 3, and it is equal to 2 if and only if the continuum hypothesis holds.

Theorem 11.7 (Hilbert's Syzygy Theorem)**.** *Let $S = k[x_1,\dots,x_n]$. Let M be a finitely generated graded S-module. Then* $\operatorname{projdim}(M) \leq n$.[5]

The proof of this theorem originally given by Hilbert was constructive. In the following subsection we see a different proof by Cartan and Eilenberg (the "founders" of homological algebra), which consists of some homological juggling.

11.1.1 Graded and minimal resolutions, and proof of the syzygy theorem

Definition 11.8. Let $M = \bigoplus_{i\in\mathbb{Z}} M_i$ be a graded S-module.

- For $d \in \mathbb{Z}$, we define M ***shifted by*** d, denoted $M(d) = \bigoplus_{i\in\mathbb{Z}} M(d)_i$, to be the same module as M, but with a different grading, where

$$M(d)_i := M_{d+i}.$$

- Given another graded S-module $N = \bigoplus_{i\in\mathbb{Z}} N_i$, a module homomorphism $f\colon M \to N$ is called a ***graded homomorphism*** if $f(M_i) \subseteq N_i$, for all $i \in \mathbb{Z}$.

- A free resolution of M in which all the free modules are graded and all the homomorphisms are graded is called a ***graded resolution*** of M.

Remark 11.9. Shifting a module does not change anything about its algebraic structure, only the degrees of the elements. The reason for shifting is that many natural maps arise as multiplication by some high-degree elements, which of course does not preserve the degree. So, for instance if $S = k[x]$, then the multiplication by x^2 is a graded map $S(-2) \to S$. Also, we will take direct sums of copies of S that are shifted by possibly different degrees. For instance, the element (x^2, x^4) is homogeneous of degree 10 in $S(-8) \oplus S(-6)$.

Lemma 11.10. *The kernel of a graded homomorphism is a graded submodule.*

Proof. Exercise. □

[5] The word "syzygy" is used in astronomy to refer to a certain alignment of heavenly bodies. In commutative algebra, "syzygy" is essentially just a word for an element in the kernel of $d_i\colon F_i \twoheadrightarrow \ker(d_{i-1})$. The analogy is that the elements of F_i have to "align" suitably to go to zero.

Proposition 11.11. *Let M be a finitely generated graded S-module. Then M has a graded free resolution where all the free modules are finitely generated.*

Proof. We construct $\cdots \to F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$ essentially as in the third item of Remarks 5.17. Start from a finite system of homogeneous generators $m_1,\dots,m_t$ of M, and denote $a_i := \deg(m_i)$. Define d_0 to be the graded map

$$F_0 := \bigoplus_{i=1}^{t} S(-a_i) \longrightarrow M, \qquad e_i \longmapsto m_i,$$

where e_i is the i-th element of a basis of F_0. Now the kernel of d_0 is generated by finitely many homogeneous elements, and again we define F_1 by shifting accordingly, so that the natural map $d_1 \colon F_1 \to F_0$ is graded. And so on... □

Example 11.12. A module can have different resolutions. Let $S = k[x,y]$ and $I = (x^2,xy,y^3)$. Then the complexes

$$0 \to S(-5) \xrightarrow{\begin{bmatrix} y^2 \\ -x \\ -1 \end{bmatrix}} S(-3)\oplus S(-4)\oplus S(-5) \xrightarrow{\begin{bmatrix} y & 0 & y^3 \\ -x & -y^2 & 0 \\ 0 & x & -x^2 \end{bmatrix}} S(-2)^2\oplus S(-3) \xrightarrow{\begin{bmatrix} x^2 & xy & y^3 \end{bmatrix}} S \to S/I \to 0$$

and

$$0 \longrightarrow S(-3)\oplus S(-4) \xrightarrow{\begin{bmatrix} y & 0 \\ -x & -y^2 \\ 0 & x \end{bmatrix}} S(-2)^2 \oplus S(-3) \xrightarrow{\begin{bmatrix} x^2 & xy & y^3 \end{bmatrix}} S \longrightarrow S/I \longrightarrow 0$$

are two graded resolutions of S/I.

Definition 11.13. Let $S = k[x_1,\dots,x_n]$ and let M be a finitely generated graded S-module. A graded resolution

$$\cdots \longrightarrow F_i \xrightarrow{d_i} F_{i-1} \xrightarrow{d_{i-1}} \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \longrightarrow 0$$

of M is called a ***minimal resolution*** if $\operatorname{im}(d_i) \subseteq (x_1,\dots,x_n)F_{i-1}$ for all $i \geq 1$ (which means that no invertible elements, i.e., non-zero constants, appear in the matrices describing the maps in the resolution).

Proposition 11.14. *Every finitely generated graded S-module has a minimal resolution.*

Proof. (We implicitly use some unstated consequences of the graded version of Nakayama's lemma, similar to those stated near the end of Section 4.1.)

Denote $\mathfrak{m} := (x_1,\dots,x_n)$. Let $m_1,\dots,m_{\beta_0}$ be a minimal system of homogeneous generators of M, and choose $F_0 = A^{\beta_0}$ with

$$d_0 \colon F_0 \longrightarrow M, \qquad e_i \longmapsto m_i.$$

Then $\ker(d_0) \subseteq \mathfrak{m}F_0$, because by the right-exactness of $(-)\otimes S/\mathfrak{m}$ we have the exact sequence

$$\begin{tikzcd}
\ker(d_0)\otimes_S S/\mathfrak{m} \arrow[r] \arrow[d, equal] & F_0\otimes_S S/\mathfrak{m} \arrow[r] \arrow[d, equal] & M\otimes_S S/\mathfrak{m} \arrow[r] \arrow[d, equal] & 0 \\
\ker(d_0)/\mathfrak{m}\ker(d_0) & F_0/\mathfrak{m}F_0 & M/\mathfrak{m}M &
\end{tikzcd}$$

and $\dim_k(F_0/\mathfrak{m}F_0) = \dim_k(M/\mathfrak{m}M) = \beta_0$. So, however we choose $d_1\colon F_1 \twoheadrightarrow \ker(d_0) \subseteq F_0$, it will be true that $\operatorname{im}(d_1) \subseteq F_0$.

Like M, also $\ker(d_0)$ has a minimal system of finitely many, say β_1, homogeneous generators, and we choose $F_1 = S^{\beta_1}$ and define $d_1\colon F_1 \twoheadrightarrow \ker(d_0)$, so that $\ker(d_1) \subseteq \mathfrak{m}F_1$. Proceeding in this way, by taking *minimal* systems of generators, we get a minimal resolution of M. □

Example 11.15. Of the two resolutions in Example 11.12, the first one is not minimal: indeed, the third column in the second matrix is a combination of the first two, which means that that generator is redundant. We may also detect this by the presence of the invertible element -1 in the left-most matrix. Instead, the second resolution *is* minimal. (In general, it is possible to "trim" a non-minimal resolution by removing unnecessary parts and get a minimal one.)

Remark 11.16. Recall what the exterior powers of a free module look like: if $e_1,\dots,e_n$ is a basis of S^n, then

$$\bigwedge^i S^n = \langle e_{j_1} \wedge \cdots \wedge e_{j_i} \mid 1 \le j_1 < \cdots < j_i \le n\rangle$$

for $i \in \{0,\dots,n\}$, so that $\bigwedge^i S^n \cong A^{\binom{n}{i}}$. (See Remark 10.33 and Examples 10.36.)

Definition 11.17. Denote by $e_1,\dots,e_n$ a basis of the free S-module S^n. The ***Koszul complex*** (for the module $S/(x_1,\dots,x_n)$) is the sequence

$$\mathcal{K}\colon\quad 0 \longrightarrow \bigwedge^n S^n \xrightarrow{\partial_n} \bigwedge^{n-1} S^n \longrightarrow \cdots \longrightarrow \bigwedge^2 S^n \xrightarrow{\partial_2} \bigwedge^1 S^n \xrightarrow{\partial_1} \bigwedge^0 S^n \xrightarrow{\partial_0} S/(x_1,\dots,x_n) \longrightarrow 0,$$

where the maps ∂_i are defined as follows:

- we identify $\bigwedge^0 S^n$ with S, and define ∂_0 as the projection;
- we identify $\bigwedge^1 S^n$ with S^n and set $\partial_0(e_j) = x_j$, for all $j \in \{1,\dots,n\}$;
- for $i > 0$, we set

$$\partial_i(e_{j_1} \wedge \cdots \wedge e_{j_i}) = \sum_{p=1}^{i} (-1)^{p+1} x_{j_p} e_{j_1} \wedge \cdots \wedge \widehat{e_{j_p}} \wedge \cdots \wedge e_{j_i},$$

  where $\widehat{e_{j_p}}$ means that e_{j_p} is omitted in the product. We shift the gradings suitably to make all the maps graded. (This indeed specializes to the case of $i = 1$ above.)[6]

Example 11.18. Consider $S = k[x,y,z]$. Then $\mathcal{K}$ is the complex $0 \longrightarrow K_3 \xrightarrow{\partial_3} K_2 \xrightarrow{\partial_2} K_1 \xrightarrow{\partial_1} K_0 \to S/(x,y,z)$, where K_0 has basis $\{1\}$, K_1 has basis $\{e_1,e_2,e_3\}$, K_2 has basis $\{e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3\}$ and K_3 has basis $\{e_1 \wedge e_2 \wedge e_3\}$, and on the basis elements, the maps behave as follows:

$$\begin{aligned} \partial_1(e_1) &= x & \qquad \partial_2(e_1 \wedge e_2) &= xe_2 - ye_1 \\ \partial_1(e_2) &= y & \partial_2(e_1 \wedge e_3) &= xe_3 - ze_1 \\ \partial_1(e_3) &= z & \partial_2(e_2 \wedge e_3) &= ye_3 - ze_2 \end{aligned}$$

[6] This construction can be generalized to any sequence of elements $f_1,\dots,f_q \in S$, not just the variables of S. We still always get a complex, but the complex will be exact if and only if $f_1,\dots,f_q$ is what is called a *regular sequence*. Going through this whole homological business is the standard way to show that any permutation of a regular sequence is still a regular sequence in rings where some version of Nakayama's lemma holds (e.g., standard graded or local rings).

$$\partial_3(e_1 \wedge e_2 \wedge e_3) = xe_2 \wedge e_3 - ye_1 \wedge e_3 + ze_1 \wedge e_2.$$

In matrix notation, $\mathcal{K}$ is then the complex

$$0 \to K_3 \xrightarrow{\begin{bmatrix} z \\ -y \\ x \end{bmatrix}} K_2 \xrightarrow{\begin{bmatrix} -y & -z & 0 \\ x & 0 & -z \\ 0 & x & y \end{bmatrix}} K_1 \xrightarrow{\begin{bmatrix} x & y & z \end{bmatrix}} K_0 \to S/(x,y,z) \to 0.$$

Theorem 11.19. *The Koszul complex $\mathcal{K}$ is a minimal graded resolution for $k = S/(x_1,\dots,x_n)$.*

Proof sketch. The fact that $\mathcal{K}$ is a chain complex (i.e., $\partial_i \circ \partial_{i+1}$ for all i) is easily checked. The minimality and the fact that $\mathcal{K}$ is graded are clear. What is not so clear is why $\mathcal{K}$ is a resolution, that is, exactness at each module. We denote by $H_i(\mathcal{K})$ the homology at $\bigwedge^i S^n$. First of all, the fact that $H_0(\mathcal{K}) = 0$ is simply by construction. For the homology $H_i(\mathcal{K})$ for $i > 0$, the proof is by induction on the number of variables n. More precisely, we still consider the same ring S, but start with the ideal generated by just one variable (x_1). The associated Koszul complex, forgetting the shifts, is then simply

$$\mathcal{K}_1 : \quad 0 \to S \xrightarrow{\cdot x_1} S \to S/(x_1) \to 0,$$

and this is clearly exact. For two generators, again ignoring the shifts, we get the Koszul complex

$$\mathcal{K}_2 : \quad 0 \to S \xrightarrow{\begin{bmatrix} -x_2 \\ x_1 \end{bmatrix}} S^2 \xrightarrow{\begin{bmatrix} x_1 & x_2 \end{bmatrix}} S \to S/(x_1,x_2) \to 0.$$

And again this is exact. For the induction step, let $\overline{\mathcal{K}}$ be the Koszul complex associated to the ideal $(x_1,\dots,x_{n-1})$. By a general fact in homological algebra (see for instance Lemma 14.5 of the book *Graded Syzygies* by Irena Peeva), there are induced homomorphisms between the homologies of these complexes: first of all, there is an exact sequence

$$\begin{tikzcd}
H_1(\overline{\mathcal{K}}) \arrow[r] \arrow[d, equal] & H_1(\mathcal{K}) \arrow[r] & H_0(\overline{\mathcal{K}}) \arrow[r, "\cdot x_n"] \arrow[d, equal] & H_0(\overline{\mathcal{K}}) \arrow[d, equal] \\
0 & & S/(x_1,\dots,x_{n-1}) & S/(x_1,\dots,x_{n-1})
\end{tikzcd}$$

and since x_n is not a zero-divisor of the S-module $S/(x_1,\dots,x_{n-1})$, this means that $H_1(\mathcal{K}) = 0$. For $i > 0$, there are is a similar exact sequence, again by the same lemma,

$$H_i(\overline{\mathcal{K}}) \longrightarrow H_i(\mathcal{K}) \longrightarrow H_{i-1}(\overline{\mathcal{K}}),$$

where the first and third term are zero by induction. But then $H_i(\mathcal{K}) = 0$. □

Proposition 11.20. *Let $\mathcal{F} : \cdots \to F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$ be a minimal resolution of a finitely generated graded S-module M, with $F_i \cong S^{\beta_i}$. Then*

$$\beta_i = \dim_k(\mathrm{Tor}_i(M,k)),$$

where k is thought of as the S-module $S/(x_1,\dots,x_n)$.

Proof. Write $\mathfrak{m} := (x_1,\dots,x_n)$. By definition, $\mathrm{Tor}_i(M,k)$ is the i-th homology of the complex $\mathcal{F} \otimes_S k$, which can be rewritten as the upper row of the diagram

$$\begin{tikzcd}
\cdots \arrow[r] & F_i/\mathfrak{m}F_i \arrow[r, "\overline{d_i}"] \arrow[d, equal] & F_{i-1}/\mathfrak{m}F_{i-1} \arrow[r] \arrow[d, equal] & \cdots \arrow[r] & F_0/\mathfrak{m}F_0 \arrow[r, "\overline{d_0}"] \arrow[d, equal] & M/\mathfrak{m}M \arrow[r] & 0 \\
 & k^{\beta_i} & k^{\beta_{i-1}} & & k^{\beta_0} & &
\end{tikzcd}$$

by a homework problem. Since the resolution $\mathcal{F}$ is minimal, the matrices of the maps d_i contain only entries in $\mathfrak{m}$, so that the induced maps $\overline{d_i}$ are all zero. But then the i-th homology is the whole vector space k^{β_i}. □

Definition 11.21. The numbers $\beta_i = \beta_i(M)$ of the proposition above (which are uniquely determined by the module M) are called the ***Betti numbers of*** M.

We are now ready to prove Hilbert's Syzygy Theorem:

Proof of Theorem 11.7. Let M be a finitely generated graded S-module, with $S = k[x_1,\dots,x_n]$ as usual. We will show that $\mathrm{projdim}(M) \leq n$. By Proposition 11.20, we know that $\beta_i(M) = \dim_k(\mathrm{Tor}_i(M,k))$. It is clear that $\mathrm{projdim}(M) \leq \sup\{i \in \mathbb{N} \mid \beta_i(M) \neq 0\}$. By definition, $\mathrm{Tor}_i(M,k)$ is the i-th homology of $\mathcal{F} \otimes_S k$, where $\mathcal{F}$ is any resolution of M. By Theorem 10.27, we know that we can alternatively compute $\mathrm{Tor}_i(M,k)$ as the i-th homology of $M \otimes_S \mathcal{G}$, where $\mathcal{G}$ is any resolution of $k = S/(x_1,\dots,x_n)$. By Theorem 11.19, we know that the Koszul complex $\mathcal{K}$ is a resolution of k, and it contains exactly n modules, so certainly the i-th homology of $M \otimes_A \mathcal{K}$ will be zero for $i > n$, so that $\beta_i(M) = 0$ for $i > n$. □

11.2 Proof that the Hilbert function is eventually a polynomial

Lemma 11.22. *Let* $0 \to M_p \xrightarrow{d_p} M_{p-1} \to \cdots \to M_2 \xrightarrow{d_2} M_1 \xrightarrow{d_1} M_0 \to 0$ *be an exact sequence of graded* S*-modules, where the all the maps* d_i *are graded. Then, for all* t,

$$\sum_{i=0}^{p} (-1)^i H_{M_i}(t) = 0,$$

that is, the Hilbert function is "additive", with an alternating sign, on exact sequences.

Proof. We prove the result by induction on p. The cases $p = 0, 1$ are trivial, so we start from $p = 2$, namely we have a short exact sequence $0 \to N \to M \to P \to 0$. We need to show that $H_M(t) = H_N(t) + H_P(t)$. This holds because, for each t, we have a short exact sequence of vector spaces

$$0 \longrightarrow N_t \longrightarrow M_t \longrightarrow P_t \longrightarrow 0,$$

and this implies that $\dim(M_t) = \dim(N_t) + \dim(P_t)$. Exercise.

For general p, we obtain two exact sequences from the given one, both shorter than that:

$$0 \to M_p \to M_{p-1} \to \cdots \to M_2 \to \mathrm{im}(d_2) \to 0 \qquad \text{and} \qquad 0 \to \ker(d_1) \to M_1 \to M_0 \to 0.$$

By induction, since $\mathrm{im}(d_2) = \ker(d_1)$, we conclude. □

We are now ready to present Hilbert's proof of Theorem 11.2.

Proof of Theorem 11.2. Recall that $S = k[x_1, \ldots, x_n]$. If $M = S(d)$ for some d, then

$$H_{S(d)}(t) = H_S(t+d) = \binom{t+d+n-1}{n-1},$$

which agrees for $t \geq -(d+n-1)$ with the polynomial

$$\begin{aligned} Q(t) &= \frac{1}{(n-1)!}\Big(t + (d+n-1)\Big) \cdot \Big(t + (d+n-2)\Big) \cdots (t+d+2) \cdot (t+d+1) \\ &= \frac{1}{(n-1)!} t^{n-1} + (\text{terms of degree} < n-1 \text{ in } t). \end{aligned}$$

If F is a finitely generated graded free S-module, then F is a direct sum of finitely many modules of the form $S(d)$, so $H_F(t)$ is a finite sum of functions of the form $H_{S(d)}(t)$. Now let M be any finitely generated graded S-module. By the Syzygy Theorem 11.7, M has a finite graded free resolution of the form $0 \to F_p \to F_{p-1} \to \cdots \to F_1 \to F_0 \to M \to 0$. Thus, by Lemma 11.22,

$$H_M(t) = \sum_{i=0}^{p} (-1)^i H_{F_i}(t)$$

is a sum of functions that eventually agree with polynomials of degree $\leq n-1$. □

Remark 11.23. In practice, people do not use Hilbert's method via resolutions to compute Hilbert functions, but instead reduce to monomial ideals. Macaulay proved that the Hilbert function of an arbitrary ideal is attained by a monomial ideal (of a special kind), and characterized combinatorially the feasible Hilbert functions. These results were Macaulay's motivation for the introduction of the notion of monomial order that later became the foundation of the Gröbner machinery. (See for instance Section 15.10 of *Commutative Algebra with a View toward Algebraic Geometry* by Eisenbud for this and more general results.)

In Section 12.1, we give some examples of the geometric meaning of the Hilbert polynomial.

12 Algebra and geometry

We saw that there are two flavors of rings that are particularly nice: local rings and graded rings. From an algebraic point of view, they are easy to produce:

- By localizing any ring A at a prime ideal $p \in \operatorname{Spec}(A)$, we get the local ring (A_p, pA_p). We may localize A-modules at p, thus getting A_p-modules, and this procedure is functorial and preserves exactness.

- Polynomial rings are graded naturally in the standard way, or by picking arbitrary degrees for the variables. We did not see it in the course, but there is a procedure called *homogenization* that, given any polynomial $f \in k[x_1, \ldots, x_n]$, produces a homogeneous polynomial $f^{\mathrm{hom}} \in k[x_1, \ldots, x_n, z]$ in a polynomial ring with one extra variable: if $f = \sum_{i=0}^{d} f_i$ is a decomposition into homogeneous components with $\deg(f) = d$, then one sets
$$f^{\mathrm{hom}} := \sum_{i=0}^{d} f_i z^{d-i}.$$
Moreover, one defines $I^{\mathrm{hom}} := (f^{\mathrm{hom}} \mid f \in I) \lhd k[x_1, \ldots, x_n, z]$ for any ideal $I \lhd k[x_1, \ldots, x_n]$.

- Another algebraic construction is the following. Given any ring R and ideal $I \lhd R$, one defines the *associated graded ring of R with respect to I* as
$$\mathrm{gr}_I R := R/I \,\oplus\, I/I^2 \,\oplus\, I^2/I^3 \,\oplus\, \cdots.$$
More generally, one can do this for a module with a *filtration*. (In the case of a ring R, the given filtration consists of the descending chain $I \supset I^2 \supset I^3 \supset \cdots$.)

In the following section, we will see that local rings and homogeneous ideals arise naturally in classical algebraic geometry. And the algebraic constructions above have a geometric meaning.

12.1 Classical algebraic geometry: Hilbert's Nullstellensatz

Let k be a field, and denote $S := k[x_1, \ldots, x_n]$ for the whole section. For $f \in S$ and $a = (a_1, \ldots, a_n) \in k^n$, we write $f(a) = f(a_1, \ldots, a_n)$.

Definition 12.1. For an ideal $I \lhd S$, define
$$\mathcal{Z}(I) := \{a \in k^n \mid \forall_{f \in I} f(a) = 0\}$$
the ***algebraic set associated to*** I. For a subset $X \subseteq k^n$, define
$$\mathcal{I}(X) := \{f \in S \mid \forall_{a \in X} f(a) = 0\}$$
the ***vanishing ideal of*** X.

Remark 12.2. Each of the following properties is easily checked:

1. The set $\mathcal{I}(X)$ is always an ideal of S.

2. $\mathcal{I}(\emptyset) = (1) = S$.

3. $\mathcal{Z}(S) = \emptyset$.

4. $\mathcal{Z}(0) = k^n$.

5. For $J \lhd S$, we have $\mathcal{Z}(\mathcal{I}(\mathcal{Z}(J))) = \mathcal{Z}(J)$.

6. For $X \subseteq k^n$, we have $\mathcal{I}(\mathcal{Z}(\mathcal{I}(X))) = \mathcal{I}(X)$.

7. For $J \lhd S$, we have $\sqrt{J} \subseteq \mathcal{I}(\mathcal{Z}(J)) = \sqrt{\mathcal{I}(\mathcal{Z}(J))}$.

8. For $J_1, J_2 \lhd S$, we have $\mathcal{Z}(J_1) \subseteq \mathcal{Z}(J_2) \Leftrightarrow \mathcal{I}(\mathcal{Z}(J_1)) \supseteq \mathcal{I}(\mathcal{Z}(J_2))$.

9. The previous equivalence holds for equality instead of inclusion.

10. For $J_1, J_2 \lhd S$, we have $\mathcal{Z}(J_1 \cap J_2) = \mathcal{Z}(J_1) \cup \mathcal{Z}(J_2)$.

11. For a family $\{J_\lambda\}_{\lambda \in \Lambda}$ of ideals of S, we have $\mathcal{Z}(\sum_{\lambda \in \Lambda} J_\lambda) = \bigcap_{\lambda \in \Lambda} \mathcal{Z}(J_\lambda)$.

Corollary 12.3. *The family of all algebraic sets $\mathcal{Z}(I)$, for varying $I \lhd S$, is the family of closed sets of a topology on k^n, called the **(classical) Zariski topology on** k^n.*

In the following we think of the elements of $S = k[x_1, \dots, x_n]$ as polynomial functions.

Definition 12.4. Let $X \subseteq k^n$ be any set. A ***polynomial function on*** X is the restriction of a polynomial function on k^n to X. If we identify two polynomial functions when they agree on all the points of X, we get the ring $A(X) := S/\mathcal{I}(X)$, called the ***coordinate ring of*** X (so called because it is generated as a k-algebra by the "coordinate functions" x_i on X).

Recall that an ideal I is called a ***radical ideal*** if $I = \sqrt{I}$. (The inclusion ($\subseteq$) always holds.) Moreover, for any ring A, the quotient A/I is reduced (i.e., it does not contain nonzero nilpotents) if and only if I is a radical ideal.

Remark 12.5. The coordinate rings $A(X)$ are reduced, or equivalently the vanishing ideals $\mathcal{I}(X)$ are radical.

Proof. Let $f \in \sqrt{\mathcal{I}(X)}$, so that $f^d \in \mathcal{I}(X)$ for some d. Observe that $f^d(a) = f(a)^d$ for any $a \in k^n$. Since k is a field, if $f(a)^d = a$, then $f(a) = 0$, so that $f \in \mathcal{I}(X)$. □

The following is a consequence of the properties listed above:

Corollary 12.6. *The function*

$$\begin{aligned} \Phi \colon \{\textit{algebraic sets in } k^n\} &\longrightarrow \{\textit{radical ideals in } S\} \\ X &\longmapsto \mathcal{I}(X) \end{aligned}$$

is an inclusion-reversing injection.

The following result, together with the Basis Theorem, the Syzygy Theorem, and Theorem 11.2 (stating that the Hilbert function eventually agrees with a polynomial) is the last of the big theorems proven by Hilbert in the 1890's that lay the foundation for commutative algebra (and its interaction with geometry):

Theorem 12.7 (Nullstellensatz)**.** *Let k be algebraically closed. Then $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$ for any $J \lhd S$.*

We will not see a proof of this result, but only several consequences of it.

Corollary 12.8. *If k is algebraically closed, then the inclusion-reversing injection*

$$\Phi\colon \{\textit{algebraic sets in } k^n\} \longrightarrow \{\textit{radical ideals in } S\}$$
$$X \longmapsto \mathcal{I}(X)$$

is a bijection.

Corollary 12.9. *If k is algebraically closed, then $\mathcal{Z}(I) = \emptyset$ if and only if $1 \in I$.*

Proof. The "if" part always holds. For the "only if", we have $\sqrt{I} = \mathcal{I}(\emptyset) = S$, where the first equality holds by the Nullstellensatz. By Lemma 1.16, this implies that $I = S$. □

Corollary 12.10. *Let k be an algebraically closed field and let $\mathfrak{m} \in \operatorname{Max}(S)$. Then $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$, for some $a_1, \ldots, a_n \in k$. The function*

$$k^n \longrightarrow \operatorname{Max}(k[x_1, \ldots, x_n])$$
$$a = (a_1, \ldots, a_n) \longmapsto \mathfrak{m}_a := (x_1 - a_1, \ldots, x_n - a_n)$$

is a bijection.

Proof. If $a \in \mathcal{Z}(\mathfrak{m})$, then $\mathcal{I}(a) \supseteq \mathcal{I}(\mathcal{Z}(\mathfrak{m})) = \sqrt{\mathfrak{m}} = \mathfrak{m}$, and since $\mathfrak{m}$ is maximal, equality holds. Furthermore, $\mathcal{I}(a) \supseteq \mathfrak{m}_a$, and since $\mathfrak{m}_a$ is maximal, again equality holds. □

Example 12.11. The ideal $(x^2 + 1) \lhd \mathbb{R}[x]$ is radical, for instance because $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ is reduced. The field $\mathbb{R}$ is not algebraically closed, and this example shows that the Nullstellensatz and all the corollaries that followed fail for $k = \mathbb{R}$. However, there are some results in real algebraic geometry that hold for the reals (see for instance Chapter 6 of *Invitation to Nonlinear Algebra*, also for a "Positivstellensatz").

The rest of this section will be a bit vague.

Remark 12.12. There exists an "Effective Nullstellensatz" that gives bounds for the degrees of the polynomials involved in checking the membership to a radical ideal, but these bounds are practically useless. In some cases they are sharp, and there is ongoing research about special cases of this.

Definition 12.13. A ***morphism of algebraic sets*** (also called a "polynomial map" or "regular map", depending on the authors) from $X \subseteq k^n$ to $Y \subseteq k^m$ is a function of the form

$$F\colon X \longrightarrow Y, \qquad a = (a_1, \ldots, a_n) \longmapsto (f_1(a), \ldots, f_m(a)),$$

for some $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$. Given a morphism $F\colon X \to Y$ as above, we may define the homomorphism of k-algebras

$$F^\#\colon k[y_1, \ldots, y_m]/\mathcal{I}(Y) \longrightarrow k[x_1, \ldots, x_n]/\mathcal{I}(X), \qquad y_i \longmapsto f_i.$$

Remark 12.14. This defines an equivalence of categories between the category of algebraic sets and the category of finitely generated reduced k-algebras.

Definition 12.15. The quotient $\mathbb{P}^n_k := (k^{n+1} \setminus \{(0, \ldots 0\})/\sim$, where

$$(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n) \quad \text{if} \quad \exists_{\lambda \in k}(a_0, a_1, \ldots, a_n) = \lambda(b_0, b_1, \ldots, b_n)$$

(that is, nonzero tuples are identified if they are proportional) is called the ***n-dimensional projective space***. We denote by $[a_0, \ldots, a_n]$ or $(a_0 : \cdots : a_n)$ the class of $(a_0, \ldots, a_n)$.

Remark 12.16. The value of a given polynomial is not well-defined on projective space: for instance the points (a_0, a_1) and $(2a_0, 2a_1)$ give the same point in $\mathbb{P}^1_{\mathbb{C}}$, but a complex polynomial takes in general different values at them. However, the *vanishing* of a *homogeneous* polynomial is well-defined at projective points. This is why in projective geometry one studies homogeneous ideals. The "homogenization" procedure described at the beginning of this section, consisting in adding a variable z, is essentially a way to "projectivize" any polynomial or ideal, by embedding a "non-projective" space k^n into $\mathbb{P}^n_k$. Conversely, one may "dehomogenize", by setting $z = 1$. These procedure is reasonably well-behaved and described precisely algorithmically in terms of Gröbner bases.

This is how homogeneous ideals arise in geometry.

Remark 12.17. Just like some of the fundamental results above hold only for k algebraically closed, many important results in geometry (for instance Bézout's Theorem, which states that two curves of degree d_1 and d_2, respectively, have $d_1 d_2$ points in common, counted with multiplicity) hold only in projective geometry.

Fun Fact 12.18. Let X be a projective algebraic set in projective space, let I be the ideal of X, and consider the quotient S/I. By Theorem 11.2, the Hilbert function of S/I eventually agrees with a polynomial $P_{S/I} \in k[x]$, the *Hilbert polynomial* of S/I. It turns out that this polynomial carries a lot of geometric data about X. Under some assumptions, one may define the dimension of X as the longest possible chain of Zariski-closed sets nested in X, and then the dimension of X is equal to the degree d of $P_{S/I}$. The *degree* of X is the number of points in the intersection of X with a general plane of complementary dimension in projective space. The degree of X is equal to leaving coefficiet of $P_{S/I}$ multiplied by d factorial.

12.2 Modern algebraic geometry: schemes

Two following two main facts in classical algebraic geometry change when passing to schemes:

- In classical algebraic geometry, if k is an algebraically closed field, the points of k^n correspond bijectively to the maximal ideals of $k[x_1, \dots, x_n]$. (See Corollary 12.8.)
- In classical algebraic geometry, the correspondece between algebra and geometry is somewhat limited the geometric side:

$$\{\text{algebraic sets}\} \longleftrightarrow \{\text{finitely generated reduced } k\text{-algebras}\}.$$

In scheme theory, the points correspond to (actually, they literally are) *all* prime ideals of $k[x_1, \dots, x_n]$. To any ring A, one associates the spectrum $\operatorname{Spec}(A)$, and that is the topological space of interest. Equipped with its *structure sheaf* $\mathcal{O}_{\operatorname{Spec}(A)}$, the space $\operatorname{Spec}(A)$ is an *affine scheme*. (See the end of Appendix C.)

Example 12.19. For $S = k[x_1, \dots, x_n]$, the corresponding space $\operatorname{Spec}(S)$ still contains all the maximal ideals $\mathfrak{m}_a = (x_1 - a_1, \dots, x_n - a_n)$, which correspond to the "classical" points k^n, but there are more points.

To a ring homomorphism $A \to B$, we saw in Theorem 2.16 that the corresponding map $\overline{f}\colon \operatorname{Spec}B \to \operatorname{Spec}A$ is a continuous map. It is actually a morphism of schemes, because it is well-behaved with respect to the structure sheaves of these affine schemes. This defines an equivalence of categories which is now too poor on the algebraic side:

$$\{\text{affine schemes}\} \longleftrightarrow \{\text{rings}\}.$$

A Appendix: General topology

General topology (also called “point-set topology”) is an abstract kind of geometry, whose main object of study is topological spaces.

Definition A.1. A ***topological space*** is a pair (X,τ), where X is a set and τ is a family of subsets of X satisfying the following properties:

1. $\emptyset \in \tau$ and $X \in \tau$;

2. if I is any index set and for all $i \in I$ we have $U_i \in \tau$, then $\bigcup_{i\in I} U_i \in \tau$;

3. if $U \in \tau$ and $V \in \tau$, then $U \cap V \in \tau$.

With these assumptions we say that τ is a ***topology on*** X. The elements of τ are called the ***open sets*** of the topology τ (or of X, if τ is understood from the context). The complements in X of the elements of τ are called the ***closed sets*** of τ.

Remark A.2. One may describe a topology τ on X by giving the open sets, or alternatively by giving the closed sets, that is, a family $\mathcal{C}$ of subsets of X satisfying the following properties:

1. $X \in \mathcal{C}$ and $\emptyset \in \mathcal{C}$;

2. if $F \in \mathcal{C}$ and $G \in \mathcal{C}$, then $F \cup G \in \mathcal{C}$;

3. if I is any index set and for all $i \in I$ we have $F_i \in \mathcal{C}$, then $\bigcap_{i\in I} F_i \in \mathcal{C}$.

Examples A.3.

1. The most trivial topology on any set X is $\tau = \{\emptyset, X\}$. That is, only $\emptyset$ and X are open. The closed sets are $X = X \setminus \emptyset$ and $\emptyset = X \setminus X$.

2. The other extreme case is $\tau = 2^X$, that is, every possible set is open. Every subset of X is the complement of some open set, and it is therefore also a closed set.

3. Consider $X = \{1,2\}$. The smallest example of a non-trivial topology is given by $\tau = \{\emptyset, \{1\}, \{1,2\}\}$. The closed sets are then X, $\{2\}$ and $\emptyset$.

4. Consider $X = \mathbb{R}$. The set consisting of open intervals (including $\emptyset$) and their arbitrary unions forms a topology, called the Euclidean topology. A set is then “open” or “closed” in the sense introduced above if it is open/closed in the sense you are used to. For instance, the union of intervals $[0,1] \cup [2,5]$ is a closed set in this topology.

5. Consider again $X = \mathbb{R}$. The set
$$\tau_s := \{(a,+\infty) \mid a \in \mathbb{R}\} \cup \{\emptyset, \mathbb{R}\}$$
is a topology on $\mathbb{R}$. Every set that is open in this topology is also open in the Euclidean topology, but the converse is not true—this topology is ***strictly coarser*** than the Euclidean topology. (The letter s stands for “semicontinuity”.)

6. Given a metric space (X,d), the set consisting of arbitrary unions of open balls constitutes a topology on X. Not all topologies arise this way; the ones that do are called ***metrizable topologies***.

Definition A.4. Let (X,τ) be a topological space. A ***base*** for τ is a family $\mathcal{B}$ of open sets such that any $U \in \tau$ is a union of elements of $\mathcal{B}$.

Examples A.5.

1. Any topology is a base for itself.

2. In a metrizable topology, such as the Euclidean topology, the set of open balls is a base.

3. Consider the Euclidean topology on the plane $\mathbb{R}^2$. The "open squares"

$$]a,b[\times]c,d[:=\{(x,y)\mid a<x<b \text{ and } c<y<d\},$$

where $]a,b[$ denotes the open interval with extremes a and b, form a base for the Euclidea topology.

4. Consider the set $X=\{1,2,3,4,5\}$. The set

$$\tau=\Big\{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\},X\Big\}$$

is a topology on X, and $\{\{1\},\{2\},\{3\},X\}$ is a base for τ.

Definition A.6. Let (X,τ) and (Y,σ) be two topological spaces. A function $f\colon X\to Y$ is ***continuous*** if the preimage along f of every open set is open, that is, for all $U\in\sigma$, we have $f^{-1}(U)\in\tau$.

Examples A.7. 1. The "continuous functions" of calculus or the course Metric Spaces are continuous in the sense introduced above.

2. The identity map from (X,τ) to (X,τ) is continuous, for any topological space (X,τ).

3. Consider $X=\mathbb{R}$ and two topologies: the Euclidean topology τ_{Eucl} and the topology τ_s introduced above. The identity $\mathrm{id}_{\mathbb{R}}\colon(\mathbb{R},\tau_{\text{Eucl}})\to(\mathbb{R},\tau_s)$ is continuous, but the same identity in the opposite direction $\mathrm{id}_{\mathbb{R}}\colon(\mathbb{R},\tau_s)\to(\mathbb{R},\tau_{\text{Eucl}})$ is not continuous.

4. In general, $\mathrm{id}_X\colon(X,\tau)\to(X,\tau')$ is continuous if and only if $\tau'\subseteq\tau$.

Lemma A.8. *Let (X,τ) and (Y,σ) be two topological spaces. For a function $f\colon X\to Y$, the following are equivalent:*

- *f is continuous;*
- *the preimage along f of every closed set is closed.*

Definition A.9. Let (X,τ) be a topological space. An ***open cover*** of (X,τ) is a subset $\{U_i\}_{i\in\Lambda}$ of τ such that $\bigcup_{i\in\Lambda}U_i=X$. A ***finite subcover*** of $\{U_i\}_{i\in\Lambda}$ is a finite subset $\{U_i\}_{i\in\Lambda'}\subseteq\{U_i\}_{i\in\Lambda}$ such that $\bigcup_{i\in\Lambda'}U_i=X$. We say that the topological space (X,τ) is ***quasi-compact*** if every open cover of X has a finite subcover.

Examples A.10. 1. Any finite topological space is trivially quasi-compact.

2. The Euclidean line $(\mathbb{R},\tau_{\text{Eucl}})$ is *not* quasi-compact: the set $\{(-a,a)\mid a\in\mathbb{R}\}$ is an open cover of $\mathbb{R}$ that does not have a finite subcover.

3. The quasi-compact subsets in $(\mathbb{R},\tau_{\text{Eucl}})$ are exactly those that are closed and bounded, for instance the union of three closed bounded intervals.

4. The previous two points can be generalized to $\mathbb{R}^n$, or to more general metrizable spaces.

Remark A.11. If $\mathcal{B}$ is a base of a topological space (X,τ), the following are equivalent:

- (X,τ) is quasi-compact;

- every open cover of X consisting of elements of $\mathcal{B}$ has a finite subcover.

Definition A.12. Let (X,τ) be a topological space.

- We say that (X,τ) is T_0 if the following condition holds: for any two points x and y, there is an open set U for which either $x \in U$ and $y \notin U$, or $x \notin U$ and $y \in U$.

- We say that (X,τ) is T_1 if the following condition holds: for any two points x and y, there is an open set U for which $x \in U$ and $y \notin U$.

Remark A.13. If a topological space is T_1, then it is T_0.

Examples A.14.

1. The Euclidean real line $(\mathbb{R}, \tau_{\text{Eucl}})$ is T_1, and therefore also T_0.
2. The real line with the semicontinuity topology τ_s introduced above is T_0 but not T_1.
3. The space $(\{1,2\},\tau)$, with $\tau = \{\emptyset, \{1\}, \{1,2\}\}$ is T_0 but not T_1.
4. The last space given in Examples A.5 is not T_0.

Lemma A.15. *A space is T_1 if and only if "the points are closed", that is, the singleton $\{x\}$ is closed for any element x in the space.*

B Appendix: Zorn's lemma

Definition B.1. A ***partially ordered set*** (often abbreviated as ***poset***) is a pair $(P,\leq)$, where P is a set and $\leq$ is an order relation on P, that is, a binary relation on P satisfying the following properties:

- (reflexivity) for all $a \in P$, we have $a \leq a$,

- (anti-symmetry) for all $a,b \in P$, if $a \leq b$ and $b \leq a$, then $a = b$,

- (transitivity) for all $a,b,c \in P$, if $a \leq b$ and $b \leq c$, then $a \leq c$.

A ***chain*** is a sequence of elements $\{a_i\}_{i\in\mathbb{N}}$ satisfying

$$a_0 \leq a_1 \leq a_2 \leq a_3 \leq a_4 \leq a_5 \leq \dots$$

An ***upper bound*** for a subset $Q \subseteq P$ is an element $x \in P$ such that $q \leq x$ for all $q \in Q$. We say $y \in P$ is a ***maximal element*** if the only element $z \in P$ such that $y \leq z$ is $z = y$.

Examples B.2.

- The classical example is $\leq = \subseteq$, the inclusion of sets. That is, for a given fixed set X, we take the power set $P = 2^X$, and the poset is $(2^X, \subseteq)$.

- For a given ring R, the set $P = \{I \mid I \triangleleft R, I \neq R\}$ is a poset, again with respect to inclusion. The maximal ideals of R are exactly the maximal elements in this poset, according to the definition of "maximal" above.

- For a topological space (X,τ), we may consider the poset $(\tau, \subseteq)$. This is a fundamental poset in the construction of sheaves, in algebraic geometry and differential geometry.

Lemma B.3 (Zorn)**.** *Let $(P,\leq)$ be a partially ordered set. If every chain in P has an upper bound in P, then P contains at least one maximal element.*

C Appendix: Functors

Category theory is a very abstract branch of math that was born around the 1950's. The main idea is that in every branch one studies "objects" and "arrows between these objects":

- sets and functions,
- groups and group homomorphisms,
- rings and ring homomorphisms,
- modules and module homomorphisms,
- topological spaces and continuous maps, . . .

By noticing similarities between some results in algebraic number theory and algebraic topology, Samuel Eilenberg and Saunders Mac Lane first formulated the definition of a category. The goal is a unifying theory in which one can prove general results that apply to very different branches of math, and in which very different branches can "talk to each other", by translating, say, geometric problems in the category of topological spaces into algebraic statements in the category of groups. Informally, a category $\mathcal{C}$ is given by:

- a collection of objects $\mathrm{Ob}(\mathcal{C})$, and
- a collection of arrows (called *morphisms*) $\mathrm{Mor}(\mathcal{C})$ going from an object to another, with a "composition rule" that is associative (and in the cases listed above, this composition is the usual composition of functions). Formally, "going from one object to another" means that there exist functions

  $$\text{domain}\colon \mathrm{Mor}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}) \qquad \text{and} \qquad \text{codomain}\colon \mathrm{Mor}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}),$$

  but let's not get too technical here... For every object $C \in \mathrm{Ob}(C)$, there exists a unique morphism $\mathrm{id}_C\colon C \to C$, such that $\mathrm{id}_C \circ f = f$ for all $f\colon C' \to C$, and $g \circ \mathrm{id}_C = g$ for all $g\colon C \to C''$. (In the cases listed above, this is the usual identity function.)

Definition C.1. Given two categories $\mathcal{C}$ and $\mathcal{D}$, a ***functor*** $F\colon \mathcal{C} \to \mathcal{D}$ consists of two functions, both usually denoted with the same symbol F, $\mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ and $\mathrm{Mor}(\mathcal{C}) \to \mathrm{Mor}(\mathcal{D})$, that satisfy the following:

1. for all $C \in \mathrm{Ob}(\mathcal{C})$, we have $F(\mathrm{id}_C) = \mathrm{id}_{F(C)}$;
2. for all morphisms $f\colon C \to C'$ and $g\colon C' \to C''$ in $\mathcal{C}$, we have $F(g \circ f) = F(g) \circ F(f)$.

Examples C.2. 1. The simplest example is a *forgetful functor*. A group is a pair $(G,*)$, and a homomorphism of groups is simply a function $f\colon G \to G$ satisfying a special property. The forgetful functor from the category of groups to the category of sets simply "forgets" the operations:

$$\begin{tikzcd}
\textbf{Groups} \arrow[rr, "F"] & & \textbf{Sets} \\
(G,*_G) \arrow[dd, "f"'] & \mapsto & G \arrow[dd, "f"'] \\
 & \mapsto & \\
(H,*_H) & \mapsto & H.
\end{tikzcd}$$

There are similar functors from the categories of rings, modules and topological spaces to the category of sets.

2. The functors mentioned in this course, namely Hom, localization, and tensor product, all go from a category of modules Mod(A) to that same category, or anyway to another category of modules (for instance over the localized ring A_S). For instance,

$$\begin{tikzcd}
\mathrm{Mod}(A) \arrow[rr, "\text{localize in } S"] & & \mathrm{Mod}(A_S) \\
M \arrow[d, "f"'] & \mapsto & M_S \arrow[d, "f_S"'] \\
 & \mapsto & \\
N & \mapsto & N_S.
\end{tikzcd}$$

3. A more interesting functor is studied in your first course in homotopy, from the category of (pointed) topological spaces to the category of groups: to any topological space, with a fixed point, you can associate its *fundamental group*. By studying the fundamental groups of two topological spaces you may for instance find out that the spaces are not homeomorphic, and that might be too hard to do by simple geometric means.

4. A poset $(P, \leq)$ is an example of category not mentioned above: the objects are the elements of P, and for any $x, y \in P$, there is a morphism $x \to y$ exactly if $x \leq y$. The presence of the identity morphisms $\mathrm{id}_x \colon x \to x$ is given by the assumption that $\leq$ is reflexive, and the "composition" of two morphisms $x \to y$ and $y \to z$, namely $x \to z$, is given by the assumption that $\leq$ is transitive. (So in particular notice that we do not need the anti-symmetry of $\leq$ to define this category.)

   A central example of such a "poset category" is when the poset is the collection of open sets of a fixed topological space X, ordered by inclusion. A (contravariant) functor from this poset category to the category of sets is called a *sheaf of sets on X*, and a (contravariant) functor from this poset category to the category of groups is called a *sheaf of groups on X*, and so on. This construction is fundamental in modern algebraic geometry. Informally, an ***affine scheme*** consists of the topological space Spec(A), for some ring A, equipped with a specific sheaf of rings $\mathcal{O}_A$ on Spec(A), the functor that is defined as follows on the distinguished open sets $D(a)$:

$$\begin{tikzcd}
\mathbf{OpenSets}(\mathrm{Spec} A) \arrow[rr, "\mathcal{O}_A"] & & \mathbf{Rings} \\
D(a) \arrow[dd] & \mapsto & A_a \\
 & \mapsto & \\
D(b) & \mapsto & A_b, \arrow[uu]
\end{tikzcd}$$

   where the arrow $D(a) \to D(b)$ means that $D(a) \subseteq D(b)$, and the ring homomorphism $A_b \to A_a$ is further localization. Note that the arrow on the right goes upwards, which is what the "contravariance" of the functor means.

D Appendix: Homological algebra

A sequence of A-module homomorphisms

$$\mathcal{C}: \quad \ldots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \ldots$$

is called a ***(chain) complex*** if $\operatorname{im}(d_{i+1}) \subseteq \ker(d_i)$ for all i, or equivalently if $d_i \circ d_{i+1} = 0$ for all i. The A-module $H_i(\mathcal{C}) := \ker(d_i)/\operatorname{im}(d_{i+1}$ is called the ***i-th homology*** of the complex $\mathcal{C}$.

Definition D.1. A *homomorphism of chain complexes* between two complexes of A-modules

$$\ldots \to P_{i+1} \xrightarrow{p_{i+1}} P_i \xrightarrow{p_i} P_{i-1} \to \ldots \qquad \text{and} \qquad \ldots \to Q_{i+1} \xrightarrow{q_{i+1}} Q_i \xrightarrow{q_i} Q_{i-1} \to \ldots$$

is a sequence of A-module maps $(\varphi_i\colon P_i \to Q_i)_{i\in\mathbb{Z}}$ such that all the squares in the diagram

$$\begin{tikzcd}
\ldots \arrow[r] & P_{i+1} \arrow[r, "p_{i+1}"] \arrow[d, "\varphi_{i+1}"'] & P_i \arrow[r, "p_i"] \arrow[d, "\varphi_i"'] & P_{i-1} \arrow[r] \arrow[d, "\varphi_{i-1}"'] & \ldots \\
\ldots \arrow[r] & Q_{i+1} \arrow[r, "q_{i+1}"'] & Q_i \arrow[r, "q_i"'] & Q_{i-1} \arrow[r] & \ldots
\end{tikzcd}$$

commute, that is, $q_i \circ \varphi_i = \varphi_{i-1} \circ p_i$ for all i.

When the chain complexes are resolutions, as in our case, we will have $\varphi_i = 0$ for all $i < 0$.

Remark D.2. By the commutativity of the squares, $\varphi_i(\ker(p_i)) \subseteq \ker(q_i)$ and $\varphi_n(\operatorname{im}(p_{i+1})) \subseteq \operatorname{im}(q_{i+1})$ for all i, so that φ induces A-module homomorphisms

$$H_i(\varphi)\colon H_i(\mathcal{P}) \longrightarrow H_i(\mathcal{Q}) \qquad \text{for all } i.$$

Definition D.3. Let $\mathcal{P}$ and $\mathcal{Q}$ be two complexes as in the definition above. A complex map $\varphi\colon \mathcal{P} \to \mathcal{Q}$ is ***null homotopic***, written $f \sim 0$, if there exist A-module homomorphisms $s_i\colon P_i \to Q_{i+1}$ such that $\varphi_i = q_{i+1} \circ s_i + s_{i-1} \circ p_i$. In a diagram:

$$\begin{tikzcd}
\cdots \arrow[r] & P_{i+1} \arrow[r, "p_{i+1}"] \arrow[d, "\varphi_{i+1}"'] \arrow[dl] & P_i \arrow[r, "p_i"] \arrow[d, "\varphi_i"'] \arrow[dl, "s_i"'] & P_{i-1} \arrow[r] \arrow[d, "\varphi_{i-1}"'] \arrow[dl, "s_{i-1}"'] & \cdots \arrow[dl] \\
\cdots \arrow[r] & Q_{i+1} \arrow[r, "q_{i+1}"'] & Q_i \arrow[r, "q_i"'] & Q_{i-1} \arrow[r] & \cdots .
\end{tikzcd}$$

Two complex maps $\varphi, \psi\colon \mathcal{P} \to \mathcal{Q}$ are ***homotopic***, written $\varphi \sim \psi$, if $f - g \sim 0$.

Proposition D.4. *If $\varphi, \psi\colon \mathcal{P} \to \mathcal{Q}$ are homotopic, then $H_i(\varphi) = H_i(\psi)$ for all i.*

Theorem D.5 (Comparison Theorem)**.** *Let $M \in \operatorname{Mod}(A)$ and let*

$$\mathcal{P}: \qquad \cdots \to P_2 \to P_1 \to P_0 \xrightarrow{\varepsilon} M \to 0$$

be a chain complex, where all the P_i are projective. Let $f\colon M \to N$ be any homomorphism of A-modules. Then, for any exact sequence of A-modules

$$\mathcal{C}: \qquad \cdots \to C_2 \to C_1 \to C_0 \xrightarrow{\eta} N \to 0,$$

there exists a homomorphism of complexes $\varphi\colon \mathcal{P} \to \mathcal{C}$ that "lifts" f, that is, such that $f \circ \varepsilon = \eta \circ \varphi_0$. Moreover, this complex homomorphism is unique up to homotopy, in the sense that if $\psi\colon \mathcal{P} \to \mathcal{C}$ is another complex morphism that lifts f, then $\varphi \sim \psi$.

Proof. By induction. □

We only apply this theorem in Section 10.1 to the case where $M = N$ and the complexes $\mathcal{P}$ and $\mathcal{C}$ are two free resolutions of M.