Lecture Notes:
Commutative Algebra
&
Introduction to Algebraic Geometry

Prof. Dr. Vladimir Lazić,
Dr. Massimilano Alessandro

(Based on the notes taken by Friedrich Günther and Niklas Müller in Summer Term 2019)

Contents

Chapter 1

Rings and Ideals

In this chapter, we introduce and study some basic notions and results concerning rings and ideals. Note that some of them were already presented in the courses "Lineare Algebra I" and "Algebra", but are included here for completeness and clarity.

Throughout these notes, all rings are assumed to be *commutative with identity*, unless explicitly stated otherwise. In particular, any nontrivial ring $R \neq \{0\}$ contains at least two different elements: 0 and 1.

Definition 1.1. Let R and S be rings. A *ring homomorphism* $\varphi\colon R \to S$ is a map fulfilling the following properties:

(a) $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in R$,

(b) $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in R$,

(c) $\varphi(1_R) = 1_S$.

Note that property (c) does not hold automatically and hence must be required.

Example 1.2. Let R and S be nontrivial rings. The following maps between rings fulfill (a) and (b), but not (c).

(1) The zero map $R \to S,\ x \mapsto 0$.

(2) The map $R \to R \times R,\ x \mapsto (x, 0)$.

(3) The map $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z},\ \overline{n} \mapsto \overline{3} \cdot \overline{n}$.

Definition 1.3. Let R be a ring. A subset $S \subseteq R$ is a *subring* of R if it is a ring with respect to the operations induced by those in R and moreover $1_R \in S$.

Remark 1.4. Let R be a ring and let $S \subseteq R$ be a subset.

(a) The subset S is a subring if and only if it is closed under subtraction and under multiplication and $1_R \in S$.

(b) If S is a subring, then the inclusion map $S \to R$, $x \mapsto x$, is a ring homomorphism.

Remark 1.5. In the definition of a subring $S \subseteq R$, the condition $1_R \in S$ is not automatically satisfied and must be imposed. Indeed, a subset of a ring may itself form a ring under the induced operations without containing the identity element of the larger ring. For example, let R be a nontrivial ring and consider

$$S := \{(x, 0) \mid x \in R\} \subseteq R \times R.$$

The subset S is a ring under the operations inherited from $R \times R$: indeed, S is nonempty, closed under subtraction and multiplication, and $(1, 0)$ is the multiplicative identity of S. However, the identity element of $R \times R$ is $(1, 1)$ and since R is nontrivial we have $(1, 0) \neq (1, 1)$. Since $(1, 1) \notin S$, the ring S is not a subring of $R \times R$.

Definition 1.6. Let R be a ring and let $a, b \in R$. We say that b *divides* a, or that b *is a divisor of* a, and write $b \mid a$, if there exists an element $c \in R$ such that $a = bc$.

Definition 1.7. Let R be a ring and let $r \in R$.

(a) The element r is called a *unit* if it is invertible with respect to multiplication, i.e., there exists $s \in R$ such that $rs = 1$. We denote by R^* the set of all units in R. Notice that $(R^*, \cdot)$ is an abelian group.

(b) The element r is called a *zero divisor* if there exists $s \in R \setminus \{0\}$ such that $rs = 0$. A nontrivial ring whose only zero divisor is 0 is called an *integral domain*.

(c) The element r is called *nilpotent* if there exists $n \in \mathbb{N}_{>0}$ such that $r^n = 0$.

(d) Assume now that $r \neq 0$ and $r \notin R^*$.

(i) The element r is called *prime* if for all $a, b \in R$

$$r \mid ab \quad \Longrightarrow \quad r \mid a \quad \text{or} \quad r \mid b.$$

(ii) The element r is called *irreducible* if for all $a, b \in R$

$$r = ab \quad \Longrightarrow \quad a \in R^* \quad \text{or} \quad b \in R^*.$$

Remark 1.8.

(a) In a nontrivial ring any nilpotent element is a zero divisor. However, the converse is not true in general. For instance, in the ring $\mathbb{Z}/6\mathbb{Z}$ the element $\overline{2}$ is a zero divisor, but it is not nilpotent.

(b) In general, the notions of prime and irreducible elements are independent: a prime element need not be irreducible, and an irreducible element need not be prime. For instance, in the ring $\mathbb{Z} \times \mathbb{Z}$ the element $(1,0)$ is prime, but not irreducible since $(1,0) = (1,0) \cdot (1,0)$. Also, in the ring $\mathbb{Z}[i\sqrt{5}] := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ the element 2 is irreducible, but not prime. Thus, without additional assumptions on the ring, there is no implication between the two concepts. However, in special classes of rings the situation improves:

(i) In an integral domain, every prime element is irreducible.

(ii) In a unique factorization domain (UFD), the two notions coincide.

1.1 Ideals: Examples and Operations

Definition 1.9. Let $(R, +, \cdot)$ be a ring. A subset $I \subseteq R$ is called an *ideal* if:

(a) $(I, +)$ is a subgroup of $(R, +)$, and

(b) for all $r \in R$, for all $a \in I$, it holds $ra \in I$.

We give now some examples of ideals and define operations on them.

Example 1.10. Let R be a ring.

(a) The subsets $\{0\}$ and R are ideal and are called *trivial ideals*.

(b) Given two ideals $I, J \subseteq R$, we define

$$\begin{aligned} I + J &:= \Big\{ i + j \mid i \in I,\ j \in J \Big\}, \\ IJ &:= \left\{ \sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N},\ i_k \in I,\ j_k \in J \right\}, \\ I \cap J &:= \Big\{ a \mid a \in I \text{ and } a \in J \Big\}. \end{aligned}$$

All three of them are ideals and it holds $IJ \subseteq I \cap J$. Notice that

$$I \cup J := \Big\{ a \mid a \in I \text{ or } a \in J \Big\}$$

is an ideal if and only if $I \subseteq J$ or $J \subseteq I$.

(c) Let $\{I_\alpha\}_{\alpha \in \mathcal{A}}$ be a family of ideals in R. We define

$$\begin{aligned} \sum_{\alpha \in \mathcal{A}} I_\alpha &:= \left\{ \sum_{\alpha \in \mathcal{A}} i_\alpha \;\middle|\; i_\alpha \in I_\alpha \text{ for all } \alpha \in \mathcal{A} \text{ and } i_\alpha \neq 0 \text{ only for finitely many } \alpha \right\}, \\ \bigcap_{\alpha \in \mathcal{A}} I_\alpha &:= \Big\{ a \;\Big|\; a \in I_\alpha \text{ for all } \alpha \in \mathcal{A} \Big\}. \end{aligned}$$

Both of them are ideals. Now, assume that $\{I_\alpha\}_{\alpha\in\mathcal{A}}$ is a chain of ideals, i.e., for any $\alpha, \beta \in \mathcal{A}$, either $I_\alpha \subseteq I_\beta$ or $I_\beta \subseteq I_\alpha$. Then,

$$\bigcup_{\alpha\in\mathcal{A}} I_\alpha := \Big\{ a \;\Big|\; a \in I_\alpha \text{ for some } \alpha \in \mathcal{A} \Big\}$$

is also an ideal.

(d) Let $a \in R$. We define

$$(a) := \{\lambda a \mid \lambda \in R\}.$$

This is an ideal called *the ideal generated by* a; we denote it by aR as well.

(e) Let $I \subseteq R$ be an ideal. We say that I is *principal* if there exists $a \in R$ such that $I = (a)$.

(f) Let $a_1, \ldots, a_n \in R$. We define

$$(a_1, \ldots, a_n) := a_1R + \ldots + a_nR = \left\{ \sum_{i=1}^{n} \lambda_i a_i \;\Big|\; \lambda_i \in R \right\}.$$

This is called *the ideal generated by* $a_1, \ldots, a_n$.

(g) Let $\{a_i\}_{i\in\mathcal{A}}$ be a subset of R. We define

$$(a_i)_{i\in\mathcal{A}} := \sum_{i\in\mathcal{A}} a_i R_i.$$

This is called *the ideal generated by the subset* $\{a_i\}_{i\in\mathcal{A}}$.

(h) Let $I \subseteq R$ be an ideal. We say that the subset $\{a_i \mid i \in \mathcal{A}\} \subseteq I$ is a *system of generators for* I if $I = (a_i)_{i\in\mathcal{A}}$. The ideal I is said to be *finitely generated* if there exists a finite system of generators for I.

Remark 1.11.

(a) Let R be a ring and let $I \subseteq R$ be an ideal. If $1_R \in I$, then $I = R$. In particular, a proper ideal $I \subsetneq R$ is not a subring of R.

(b) A proper ideal $I \subsetneq R$ of a ring R might be itself a ring. In this case, $1_I \neq 1_R$ is an idempotent element of R. For instance, the ring $S \subseteq R \times R$ given in Remark 1.5 is an ideal in $R \times R$. A natural question then arises: does there exist an example of a subset of a ring that is itself a ring but neither a subring nor an ideal of the ambient ring? The answer is positive. Indeed, the same ring S can be regarded as a subset of the polynomial ring $(R \times R)[x]$, but it is neither a subring nor an ideal of $(R \times R)[x]$.

1.2 Prime Ideals and Maximal Ideals

Definition 1.12. Let R be a ring and let $I \subsetneq R$ be a proper ideal.

(a) The ideal I is called *prime* if for any $a, b \in I$

$$ab \in I \implies a \in I \text{ or } b \in I.$$

(b) The ideal I is called *maximal* if for any ideal J

$$I \subseteq J \subseteq R \implies J = I \text{ or } J = R.$$

Proposition 1.13. *Let R be a ring and let $I \subsetneq R$ be a proper ideal.*

(i) The ideal I is prime if and only if R/I is an integral domain.

(ii) The ideal I is maximal if and only if R/I is a field.

Corollary 1.14. *In a ring any maximal ideal is prime.*

The converse does not hold true in general.

Example 1.15. Let R be a ring and let $I \subsetneq R$ be a proper ideal.

(a) If R is an integral domain that is not a field, then $I = (0)$ is prime, but not maximal.

(b) In $R = \mathbb{Z}[x, y]$, the ideal $I = (x)$ is prime, but not maximal since

$$(x) \subsetneq (x, y) \subsetneq \mathbb{Z}[x, y].$$

Proposition 1.16. *Let R be a ring and let $I \subseteq R$ be an ideal. There is a one-to-one inclusion-preserving correspondence between the ideals of R containing I and the ideals of R/I. Under this correspondence, prime (resp. maximal) ideals correspond to prime (resp. maximal) ideals.*

Hint: Let $\pi \colon R \to R/I$ be the canonical projection. If J is an ideal in R/I, then $\pi^{-1}(J)$ is an ideal in R containing I.

Proof. Exercise. □

Proposition 1.17. *(i) Every nontrivial ring $R \neq 0$ has a maximal ideal.*

(ii) Let R be a ring and let $I \subsetneq R$ be a proper ideal. Then there exists in R a maximal ideal containing I.

Proof. (i) Let $\mathcal{I} := \{I' \subsetneq R \mid I' \text{ is an ideal of } R\}$. Since $(0) \in \mathcal{I}$, the set $\mathcal{I}$ ordered by inclusion is a nonempty partially ordered set (poset for short). Let $\{I_\alpha\}_{\alpha\in\mathcal{A}}$ be a chain in $\mathcal{I}$, i.e., a totally ordered family of proper ideals in R. Since $\bigcup_{\alpha\in\mathcal{A}} I_\alpha$ is a proper ideal, every totally ordered subset of $\mathcal{I}$ has an upper bound in $\mathcal{I}$. Hence, by Zorn's Lemma, there exists a maximal element for the poset $(\mathcal{I}, \subseteq)$, i.e., a maximal ideal in R.

(ii) Apply (i) to the quotient ring R/I and then the one-to-one inclusion-preserving correspondence given by Proposition 1.16. Alternatively, argue as in (i) setting

$$\mathcal{I} := \{I \subseteq I' \subsetneq R \mid I' \text{ is an ideal of } R\}.$$

□

Corollary 1.18. *Every non-unit of a ring R is contained in a maximal ideal.*

Proof. Let $r \in R \setminus R^*$. Then the principal ideal (r) is a proper ideal of R. Now we apply Proposition 1.17 (ii) and we are done. □

Proposition 1.19. *Let R be a ring.*

(i) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subsetneq R$ be prime ideals and let $I \subseteq R$ be an ideal such that $I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Then $I \subseteq \mathfrak{p}_i$ for some $i \in \{1, \ldots, n\}$.

(ii) Let $I_1, \ldots, I_n \subseteq R$ be ideals and let $\mathfrak{p} \subsetneq R$ be a prime ideal such that $\mathfrak{p} \supseteq \bigcap_{j=1}^n I_j$. Then $\mathfrak{p} \supseteq I_j$ for some $j \in \{1, \ldots, n\}$. Moreover, if $\mathfrak{p} = \bigcap_{j=1}^n I_j$, then $\mathfrak{p} = I_j$ for some $j \in \{1, \ldots, n\}$.

Proof. (i) The statement will be shown by induction on n in the form: If $I \not\subseteq \mathfrak{p}_i$ for $1 \leq i \leq n$, then $I \not\subseteq \bigcup_{i=1}^n \mathfrak{p}$.

For $n = 1$ the statement is trivial. Let now $n \geq 2$ and assume the statement is true for $n-1$. Then for each $1 \leq i \leq n$ by the inductive hypothesis there exists $x_i \in I$ such that $x_i \notin \mathfrak{p}_j$ for all $j \neq i$. If for some $1 \leq i \leq n$ it holds $x_i \notin \mathfrak{p}_i$, then $x_i \notin \mathfrak{p}_j$ for all $1 \leq j \leq n$, thus we are done. Otherwise, it holds $x_i \in \mathfrak{p}_i$ for all $1 \leq i \leq n$. Consider the element

$$y := \sum_{i=1}^{n} x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n.$$

Note that $y \in I$ and $y \notin \mathfrak{p}_i$ for all $1 \leq i \leq n$. Indeed, assume by contradiction that $y \in \mathfrak{p}_i$ for some i. Then $x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n \in \mathfrak{p}_i$ since each of the other summands is a multiple of $x_i \in \mathfrak{p}_i$ and hence in $\mathfrak{p}_i$. But then, since $\mathfrak{p}_i$ is prime, we would have $x_j \in \mathfrak{p}_i$ for some $j \neq i$, a contradiction. Hence $y \notin \bigcup_{i=1}^n \mathfrak{p}_i$ and we are done.

(ii) Assume that $\mathfrak{p} \not\supseteq I_j$ for all $1 \leq j \leq n$. Then there exists $x_j \in I_j$ but $x_j \notin \mathfrak{p}$ for each $1 \leq j \leq n$. Thus

$$\prod_{j=1}^{n} x_j \in \prod_{j=1}^{n} I_j \subseteq \bigcap_{j=1}^{n} I_j.$$

But, since $\mathfrak{p}$ is prime, $\prod_{j=1}^{n} x_j \notin \mathfrak{p}$ and thus $\mathfrak{p} \not\supseteq \bigcap_{j=1}^{n} I_j$.

Now, if $\mathfrak{p} = \bigcap_{j=1}^{n} I_j$, then in particular we have $\mathfrak{p} \supseteq \bigcap_{j=1}^{n} I_j$ and therefore there is some $j_0 \in \{1, \ldots, n\}$ such that $I_{j_0} \subseteq \mathfrak{p}$. On the other hand, $\mathfrak{p} \subseteq I_j$ for $1 \leq j \leq n$, hence $\mathfrak{p} = I_{j_0}$.

□

1.3 Nilradical, Jacobson Radical and Local Rings

Proposition/Definition 1.20. *Let R be a ring and let $I \subseteq R$ be an ideal. The set*

$$\sqrt{I} := \{a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N}_{>0}\}$$

is an ideal called the radical of I.

Proof. Let $r \in R$ and let $a \in \sqrt{I}$. Then $a^n \in I$ for some $n \in \mathbb{N}_{>0}$ and so $(ra)^n = r^n a^n \in I$ since I is an ideal. Now let $x, y \in \sqrt{I}$. Then there exist $n, m \in \mathbb{N}_{>0}$ such that $x^n, y^m \in I$. By the binomial formula we get

$$(x+y)^{m+n-1} = \sum_{k=0}^{m+n-1} \binom{m+n-1}{k} \underbrace{x^k y^{m+n-1-k}}_{\in I} \quad ,$$

hence, $(x+y)^{m+n-1} \in I$, which implies $x + y \in \sqrt{I}$. Thus, we have shown that $\sqrt{I}$ is indeed an ideal.

□

Proposition 1.21. *Let R be a ring. Let I and J be two ideals in R. Then:*

(i) $\sqrt{I} \supseteq I$,

(ii) $\sqrt{\sqrt{I}} = \sqrt{I}$,

(iii) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(iv) $\sqrt{I} = R \iff I = R$.

Definition 1.22. Let R be a ring. The *nilradical of R* is defined as

$$N_R := \sqrt{(0)} = \{a \in R \mid a^n = 0 \text{ for some } n \in \mathbb{N}_{>0}\}.$$

In other words, the set of nilpotent elements in R is indeed an ideal called the nilradical of R.

Proposition 1.23. *Let R be a ring. Then in the quotient ring R/N_R the only nilpotent element is* 0.

Proof. Let $[x] \in R/N_R$ be nilpotent. This means there is $k \in \mathbb{N}$ such that $[x]^k = [x^k] = 0$ in R/N_R, hence $x^k \in N_R$. Because $x^k \in N_R$, there is $l \in \mathbb{N}$ such that $(x^k)^l = x^{kl} = 0$ in R, and thus $x \in N_R$. Because $x \in N_R$, $[x] = 0$ in R/N_R. □

The following theorem describes the nilradical of a ring and, more in general, the radical of any ideal.

Theorem 1.24. *Let R be a ring and let $I \subseteq R$ be an ideal. Then:*

(i) The nilradical of R is the intersection of all prime ideals of R, i.e.,

$$N_R = \bigcap_{\substack{P \subsetneq R \\ prime}} P.$$

(ii) The radical of I is the intersection of all prime ideals containing I, i.e.,

$$\sqrt{I} = \bigcap_{\substack{I \subseteq P \subsetneq R \\ prime}} P.$$

Proof. (i) "$\subseteq$": Let $P' \subsetneq R$ be a prime ideal in R. If $x \in N_R$, there is $k \in \mathbb{N}$ such that $x^k = 0 \in P'$. Since P' is prime, it holds $x \in P'$, and thus $N \subseteq \bigcap_{\substack{P \subsetneq R \\ \text{prime}}} P$.

"$\supseteq$": Let now $x \in R \setminus N_R$ and let $\mathcal{S}_x$ be the set of proper ideals $I \subsetneq R$ with the property that if $n \in \mathbb{N}_{>0}$, then $x^n \notin I$. Since $(0) \in \mathcal{S}_x$, the set $\mathcal{S}_x$ is a nonempty poset (with respect to inclusion). As in the proof of Proposition 1.17 (i), by Zorn's Lemma $\mathcal{S}_x$ has a maximal element, say P'.

We show now that P' is a prime ideal in R. To see this, let $a, b \in R \setminus P'$. Then the ideals $(a) + P'$ and $(b) + P'$ are strictly larger than P' (with respect to inclusion) and thus are not in $\mathcal{S}_x$. Since $(a) + P'$, $(b) + P' \notin \mathcal{S}_x$, there is $m \in \mathbb{N}_{>0}$ such that $x^m \in (a) + P'$ and there is $k \in \mathbb{N}_{>0}$ such that $x^k \in (b) + P'$. Thus $x^m x^k = x^{m+k} \in [(a) + P'][(b) + P'] \subseteq (ab) + P'$. Since $x^{m+k} \in (ab) + P'$, the ideal $(ab) + P' \notin \mathcal{S}_x$, and thus $(ab) + P' \supsetneq P'$, which implies $ab \notin P'$. Finally, we have found a prime ideal P' such that $P' \in \mathcal{S}_x$. By definition of $\mathcal{S}_x$, the ideal P' does not contain any power of x. In particular, $x \notin P'$ and hence $x \notin \bigcap_{\substack{P \subsetneq R \\ \text{prime}}} P$.

(ii) Let $\pi \colon R \to R/I$ be the canonical projection. Note that $\pi^{-1}(N_{R/I}) = \sqrt{I}$. Hence, we first apply (i) to the ring R/I and then use the correspondence between prime ideals in R containing I and prime ideals in R/I given by Proposition 1.16.

□

Definition 1.25. Let R be a ring. The *Jacobson radical* J_R *of* R is definded as the intersection of all maximal ideals, i.e.,

$$J_R := \bigcap_{\substack{\mathfrak{m} \subsetneq R \\ \text{maximal}}} \mathfrak{m}.$$

Proposition 1.26. *Let R be a ring. The Jacobson radical J_R admits the following description*

$$J_R = \{x \in R \mid 1 - xy \in R^* \text{ for all } y \in R\}.$$

Proof. "$\subseteq$": Let $x \in J_R$ and assume that $1 - xy$ is not a unit for some $y \in R$. Then by Proposition 1.17 (ii) the element $1 - xy$ is contained in some maximal ideal $\mathfrak{m}$ of R and by definition of Jacobson radical, $x \in \mathfrak{m}$ as well. But then $1 \in \mathfrak{m}$, which is a contradiction.

"$\supseteq$": If $x \notin J_R$, then $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ in R. Hence, $(x)+\mathfrak{m} \supsetneq \mathfrak{m}$ and thus $(x)+\mathfrak{m} = (1)$, i.e., there are elements $y \in R$ and $z \in \mathfrak{m}$ such that $xy+z = 1$. In other words, the element $1 - xy = z \in \mathfrak{m}$ and therefore $1 - xy$ is not a unit. □

Definition 1.27. A ring R is called *local* if it contains only one maximal ideal $\mathfrak{m}$. Then the quotient $R/\mathfrak{m}$ is a field, called the *residue field* of R. In literature, a local ring is often denoted by $(R, \mathfrak{m})$ or $(R, \mathfrak{m}, k)$, where $k := R/\mathfrak{m}$.

Proposition 1.28. *(i) Let R be a ring and let $\mathfrak{m} \subsetneq R$ be an ideal such that every element in $R \setminus \mathfrak{m}$ is a unit. Then R is a local ring and $\mathfrak{m}$ is its unique maximal ideal.*

(ii) Let R be a ring and let $\mathfrak{m} \subsetneq R$ be a maximal ideal such that every element in the set $1 + \mathfrak{m} := \{1 + x \mid x \in \mathfrak{m}\}$ is a unit. Then R is local and $\mathfrak{m}$ is its unique maximal ideal.

Proof. Exercise. □

1.4 Chinese Remainer Theorem

Definition 1.29. Let R be a ring and let $I, J \subseteq R$ be ideals. Then I and J are called *coprime* (or *comaximal*) if $I + J = R$.

Remark 1.30. Let R be a ring and I, J be ideals in R.

(i) If the ideals I, J are coprime, it holds $IJ = I \cap J$.

(ii) Two ideals $I, J \subseteq R$ are coprime if and only if there exist $i \in I$, $j \in J$ such that $i + j = 1$.

Proposition 1.31 (Chinese Remainder Theorem)**.** *Let R be a ring and $I_1, \ldots, I_n \subseteq R$ be ideals. We define a ring homomorphism by*

$$\varphi\colon R \longrightarrow \prod_{j=1}^{n}(R/I_j), \qquad x \longmapsto (x + I_1, \ldots, x + I_n).$$

(i) If I_k and I_l are coprime for $k \neq l$, then $\prod_{j=1}^{n} I_j = \bigcap_{j=1}^{n} I_j$.

(ii) φ is surjective if and only if I_k and I_l are coprime for $k \neq l$.

(iii) φ is injective if and only if $\bigcap_{j=1}^{n} I_j = (0)$.

1.5 Hilbert's Basis Theorem

Definition 1.32. A ring R is called *Noetherian* if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq \ldots$$

is stationary, i.e., there exists $N \in \mathbb{N}_{>0}$ such that $I_k = I_N$ for $k \geq N$.

Example 1.33. Any principal ideal domain (PID) is a Noetherian ring, as shown in the course "Algebra".

The following well-known theorem allows us to construct new Noetherian rings from a given one.

Theorem 1.34 (Hilbert's Basis Theorem)**.** *Let R be a Noetherien ring. Then $R[x_1, \ldots, x_n]$ is also Noetherian.*

Proof. First of all, it suffices to show the theorem when $n = 1$ since

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n].$$

By contradiction, assume $R[x]$ is not Noetherian. Let $I_1 \subsetneq I_2 \subsetneq \ldots$ be a strictly ascending chain of ideals. Set $I := \bigcup_{n\in\mathbb{N}} I_n$. We construct a sequence $\{f_1, f_2, \ldots\}$ of polynomials in $R[x]$ as follows:

(a) We choose $f_1 \in I - \{0\}$ of minimal degree.

(b) Assume we found $f_1, f_2, \ldots, f_{n-1}$. We pick f_n in $I \setminus (f_1, \ldots, f_{n-1})$ of minimal degree.

Note that this is a well-defined construction: indeed, $\mathbb{N}$ is well-ordered and step (b) is repeated infinitely many times since the given chain of ideals is strictly ascending.

Claim 1. $\deg(f_n) \geq \deg(f_{n-1})$ for $n \geq 2$.

Proof of Claim 1. First of all, $\deg(f_2) \geq \deg(f_1)$ by (a). Assume by contradiction $\deg(f_n) < \deg(f_{n-1})$ for some $n \geq 3$. Since by construction $f_n \in I \setminus (f_1, \ldots, f_{n-1}) \subseteq I \setminus (f_1, \ldots, f_{n-2})$, we found a polynomial in $I \setminus (f_1, \ldots, f_{n-2})$ whose degree is lower than $\deg(f_{n-1})$, against the choice of f_{n-1} as a polynomial in $I \setminus (f_1, \ldots, f_{n-2})$ of minimal degree. □

For $i \in \mathbb{N}$ define $a_i \in R$ to be the leading coefficient of f_i and define the ideal $J_i := (a_1, \ldots, a_i)$. We have then an ascending chain of ideals of R, namely $J_1 \subseteq J_2 \subseteq J_3 \subseteq \ldots$. As R is noetherian, there is $N \in \mathbb{N}$ such that $J_k = J_N$ for all $k \geq N$. Consider the element $a_{N+1} \in J_{N+1} = J_N = (a_1, \ldots, a_n)$. Then for $1 \leq i \leq N$ there are $u_i \in R$ such that $a_{N+1} = \sum_{i=1}^{N} u_i a_i$. Now set

$$f'_{N+1} := u_1 x^{\deg(f_{N+1})-\deg(f_1)} f_1 + \cdots + u_N x^{\deg(f_{N+1})-\deg(f_N)} f_N.$$

The leading term of f'_{N+1} is $a_{N+1} x^{\deg(f_{N+1})}$ and $f'_{N+1} \in (f_1, \ldots, f_N)$. Consider the polynomial

$$g := f'_{N+1} - f_{N+1}.$$

It holds $g \in I \setminus (f_1, \ldots, f_N)$ since otherwise $f_{N+1} = f'_{N+1} - g \in (f_1, \ldots, f_N)$. Moreover, by construction $\deg(g) < \deg(f_{N+1})$ and this contradicts the choice of f_{N+1} as a polynomial in $I \setminus (f_1, \ldots, f_N)$ of minimal degree. □

Chapter 2

Modules

Definition 2.1. Let A be a ring. An *A-module* is an abelian group $(M, +)$ together with a map $\mu\colon A \times M \to M$, $(a, m) \mapsto a \cdot m := \mu(a, m)$, which satisfies the following properties for all $a, b \in A$ and for all $x, y \in M$:

(a) $a(x + y) = ax + ay$,

(b) $(a + b)x = ax + bx$,

(c) $(ab)x = a(bx)$,

(d) $1_A\, x = x$.

Example 2.2. Let A be a ring. The following are some examples of modules:

(a) An ideal $I \subseteq A$ is an A-module. In particular, A is itself an A-module.

(b) If A is a field, then an A-module is an A-vector space.

(c) Let $(G, +)$ be an abelian group. Then G is a $\mathbb{Z}$-module with respect to the scalar multiplication

$$n \cdot x := \begin{cases} \underbrace{x + \ldots + x}_{n-\text{times}} & \text{if } n \geq 0 \\ \underbrace{(-x) + \ldots + (-x)}_{(-n)-\text{times}} & \text{if } n < 0 \end{cases}$$

(d) Assume $A = k[X]$, where k is a field. Let V be a k-vector space and let $T \in \mathrm{End}(V)$ be a linear map. Then we can regard V as an A-module via the following construction: for $f = \sum_{i=0}^{n} a_i X^i \in k[X]$ set $f(T) := \sum_{i=0}^{n} a_i T^i$ and define $\mu\colon k[X] \times V \to V$ for $f \in k[X]$ and $v \in V$ by

$$f \cdot v := f(T)(v).$$

Definition 2.3. Let A be a ring and M, N be A-modules. A map $f\colon M \to N$ is called an *A-module homomorphism* (or *A-linear*) if the following properties are satisfied:

(i) $f(x+y) = f(x) + f(y)$ for all $x, y \in M$,

(ii) $f(ax) = af(x)$ for all $x \in M$, for all $a \in A$.

Example 2.4. If A is a field, then an A-module homomorphism is a linear map.

Remark 2.5.

(a) Let M, N be A-modules. The set $\mathrm{Hom}_A(M, N)$ of all A-module homomorphisms from M to N is an A-module in the following way. We define the sum of $f, g \in \mathrm{Hom}_A(M, N)$ via

$$(f+g)(x) := f(x) + g(x) \quad \text{for all } x \in M,$$

and the scalar multiplication of $a \in A$ and $f \in \mathrm{Hom}_A(M, N)$ via

$$(af)(x) := af(x) \quad \text{for all } x \in M.$$

These operations make $\mathrm{Hom}_A(M, N)$ into an A-module. When the ring A is clear from the context, we simply write $\mathrm{Hom}(M, N)$.

(b) The composition of A-module homomorphisms is again an A-module homomorphism.

(c) Let M, M', N, N'' be A-modules and let $U\colon M' \to M$ and $V\colon N \to N''$ be A-module homomorphisms. Then we have the following induced A-module homomorphisms:

$$\begin{aligned} \overline{U}\colon\ & \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M', N), \quad \overline{U}(f) := f \circ U, \\ \overline{V}\colon\ & \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M, N''), \quad \overline{V}(f) := V \circ f. \end{aligned}$$

(d) For any A-module M we have a natural isomorphism

$$\mathrm{Hom}_A(A, M) \cong M, \qquad f \longmapsto f(1).$$

2.1 Submodules and Quotient Modules

Definition 2.6. Let A be a ring and M be an A-module. A *submodule* $N \subseteq M$ is a subgroup of M which is closed under scalar multiplication, i.e., $a \cdot x \in N$ for $a \in A$ and $x \in N$.

Definition 2.7. Let M be an A-module and let $N \subseteq M$ be a submodule. The abelian group M/N inherits an A-module structure from M via

$$a \cdot (x + N) := ax + N \quad \text{for } a \in A,\ x \in M.$$

The A-module M/N is called the *quotient of M by N*. The canonical projection $\pi\colon M \to M/N$ is an A-module homomorphism.

Proposition 2.8. *Let M be an A-module and let $N \subseteq M$ be a submodule. There is a one-to-one inclusion-preserving correspondence between the submodules of M which contain N and submodules of the quotient M/N.*

Definition 2.9. Let A be a ring and let M, N be A-modules. Let $f\colon M \to N$ be an A-module homomorphism.

(a) The *kernel of f* is defined as $\ker(f) := \{x \in M \mid f(x) = 0\}$. This is indeed a submodule of M.

(b) The *image of f* is defined as $\mathrm{im}(f) := \{f(x) \mid x \in M\} = f(M)$. This is indeed a submodule of N.

(c) The *cokernel of f* is defined as the quotient $\mathrm{coker}(f) := N/\mathrm{im}(f)$.

Theorem 2.10 (Homomorphism Theorem/First Isomorphism Theorem)**.** *Let A be a ring, let M, N be A-modules and let $f\colon M \to N$ be an A-module homomorphism. Then*

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

2.2 Operations on Submodules

Definition 2.11. Let M be an A-module and let $\{M_i\}_{i \in I}$ be a family of submodules of M. We define the *intersection of the submodules M_i*

$$\bigcap_{i \in I} M_i := \Big\{ m \;\Big|\; m \in M_i \text{ for all } i \in I \Big\}$$

and the *sum of the submodules M_i*

$$\sum_{i \in I} M_i := \left\{ \sum_{i \in I} m_i \;\middle|\; m_i \in M_i \text{ for all } i \in I \text{ and } m_i \neq 0 \text{ for only finitely many } i \right\}.$$

Both are submodules of M. Moreover, we say that the sum $\sum_{i \in I} M_i$ is *direct* and denote it by $\bigoplus_{i \in I} M_i$ if every element $m \in \sum_{i \in I} M_i$ can be written uniquely as $\sum_{i \in I} m_i$ where $m_i \in M_i$ for each $i \in I$.

Remark 2.12. Let M_1 and M_2 be submodules of M. The sum $M_1 + M_2$ is direct if and only if $M_1 \cap M_2 = \{0\}$.

Now, assume $\{M_i\}_{i\in I}$ is a chain of submodules of M, i.e., for any $i, j \in I$, either $M_i \subseteq M_j$ or $M_j \subseteq M_i$. Then

$$\bigcup_{i\in I} M_i := \Big\{ m \;\Big|\; m \in M_i \text{ for some } i \in I \Big\}$$

is also a submodule of M.

Since we can't multiply two elements of a module, there is no product of submodules. However, we define the product of an ideal $I \subseteq A$ with the A-module M as

$$IM := \Big\{ \sum_{i=1}^{n} a_i m_i \;\Big|\; a_i \in I,\ m_i \in M,\ n \in \mathbb{N} \Big\},$$

which is a submodule of M.

Theorem 2.13 (Second Isomorphism Theorem)**.** *Let A be a ring, let M be an A-module and let M_1 and M_2 be submodules of M. Then*

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2).$$

Proof. Consider

$$M_2 \longrightarrow M_1 + M_2 \longrightarrow (M_1 + M_2)/M_1, \qquad x \longmapsto 0 + x \longmapsto x + M_1.$$

The composition $\varphi\colon M_2 \to (M_1 + M_2)/M_1$ is surjective since for $m_i \in M_i$ it holds $(m_1 + m_2) + M_1 = m_2 + M_1$. Moreover, we have $\ker(\varphi) = M_1 \cap M_2$. Now the first isomorphism theorem gives the thesis. □

Theorem 2.14 (Third Isomorphism Theorem)**.** *Let A be a ring. Let $L \supseteq M \supseteq N$ be A-modules. Then*

$$(L/N)/(M/N) \cong L/M.$$

Proof. Consider

$$\psi\colon L/N \longrightarrow L/M, \qquad x + N \longmapsto x + M.$$

This is a well-defined A-module homomorphism since $N \subseteq M$. It is clearly surjective and moreover $\ker(\psi) = M/N$. Therefore, the first isomorphism theorem shows the assertion. □

2.3 Direct Sums and Direct Products

Definition 2.15. Let A be a ring and let $\{M_i\}_{i\in I}$ be a family of A-modules. We define:

(i) The *direct product of the* M_i

$$\prod_{i\in I} M_i := \Big\{ f\colon I \to \bigsqcup_{i\in I} M_i \;\Big|\; f(i) \in M_i \text{ for } i \in I \Big\}.$$

This is an A-module whose elements are usually written as sequences $(m_i)_{i\in I}$ such that $m_i \in M_i$ for $i \in I$. The operations in $\prod_{i\in I} M_i$ are componentwise.

(ii) The *direct sum of the* M_i

$$\bigoplus_{i\in I} M_i := \Big\{ f \in \prod_{i\in I} M_i \;\Big|\; f(i) \neq 0 \text{ for only finitely many } i \Big\}.$$

This is a submodule of the direct product $\prod_{i\in I} M_i$.

Remark 2.16. In general, direct sum and direct product of a family $\{M_i\}_{i\in I}$ of A-modules are not the same. They coincide if the index set I is finite.

Remark 2.17 (Internal and External Direct Sum)**.** Let M be an A-module. For a family $\{M_i\}_{i\in I}$ of submodules of M we have at this stage two notions of their direct sum: namely, the direct sum as submodules in the sense of Definition 2.11 and the direct sum as a family of modules in the sense of Definition 2.15. For the time being, we refer to them, respectively, as *internal direct sum* and *external direct sum*. Indeed, the two concepts coincide up to isomorphism and this is the reason why one refers to both of them simply as direct sum. For the benefit of the reader, we explain in detail the case of two submodules M_1 and M_2. Suppose that the sum $M_1 + M_2$ is direct in the sense of Definition 2.11 and denote it by $M_1 \oplus_i M_2$. On the other hand, we consider the external direct sum of M_1 and M_2, which we denote here by $M_1 \oplus_e M_2$. Consider

$$f\colon M_1 \oplus_i M_2 \to M_1 \oplus_e M_2, \quad m_1 + m_2 \mapsto (m_1, m_2).$$

This map is well-defined since the sum $M_1 + M_2$ is direct in the sense of Definition 2.11. It is easy to see that f is indeed an isomorphism of A-modules.

Let now M_1 and M_2 be A-modules. Consider the external direct sum $M_1 \oplus_e M_2$. We define:

$$\widetilde{M}_1 := \{(m_1, 0) \mid m_1 \in M_1\} \qquad \text{and} \qquad \widetilde{M}_2 := \{(0, m_2) \mid m_2 \in M_2\}.$$

Both are submodules of $M_1 \oplus_e M_2$ and clearly $\widetilde{M}_i \cong M_i$. It is easy to see that the sum $\widetilde{M}_1 + \widetilde{M}_2$ is direct in the sense of Definition 2.11. Moreover, we have

$$\widetilde{M}_1 \oplus_i \widetilde{M}_2 = M_1 \oplus_e M_2.$$

Remark 2.18 (Direct Sum of Rings and Direct Sum of Ideals)**.**

Let A be a nontrivial ring.

(i) Assume that A is a direct sum of rings $A = \bigoplus_{j=1}^{n} A_j = A_1 \times \ldots \times A_n$. Then the ring

$$I_j := \{(0, \ldots, 0, a_j, 0, \ldots, 0) \mid a_j \in A_j\} \cong A_j$$

is an ideal of A, but not a subring since $1_A = (1, \ldots, 1) \notin I_j$. Hence, the ring A, considered as an A-module, is the direct sum of the ideals I_j, i.e., $A = \bigoplus_{j=1}^{n} I_j$.

(ii) Assume now that A, considered as an A-module, is a direct sum of ideals $A = \bigoplus_{j=1}^{n} I_j$. Set $B_j := \bigoplus_{k \neq j} I_k$ and note that $A/B_j \cong I_j$, which shows that I_j is indeed a ring, and hence there is a ring isomorphism

$$A \cong \bigoplus_{j=1}^{n} (A/B_j).$$

Since $A = \bigoplus_{j=1}^{n} I_j$, we may write $1_A = (y_1, \ldots, y_n)$ with $y_j \in I_j$. Then we have that

$$1_{A/B_j} = 1_A + B_j = (y_1, \ldots, y_n) + B_j = (0, \ldots, 0, y_j, 0, \ldots, 0) + B_j$$

and by means of the isomorphism $A/B_j \cong I_j$ we get $1_{I_j} = y_j$. Note that $1_{I_j} = y_j$ is idempotent and $I_j = (y_j)$ as an ideal in A.

2.4 Finitely Generated Modules

We now introduce some terminology and key concepts needed for what follows.

Definition 2.19. Let A be a ring and M be an A-module.

(a) Let $x \in M$. The set $Ax := \{ax \mid a \in A\} \subseteq M$ is a submodule of M which is called *the submodule generated by* x.

(b) The A-module M is called *principal* if there exists $x \in M$ such that $M = Ax$.

(c) Let $\{x_i\}_{i \in I}$ be a subset of M. The sum $\sum_{i \in I} Ax_i$ is called *the submodule generated by the subset* $\{x_i\}_{i \in I}$.

(d) If $M = \sum_{i \in I} Ax_i$, then the set $\{x_i\}_{i \in I}$ is called a *set of generators of* M.

(e) The A-module M is called *finitely generated* if there exists a finite set of generators of M, i.e., $M = Ax_1 + \ldots + Ax_n$ for some $x_1, \ldots, x_n \in M$.

(f) The A-module M is called *free* if $M \cong \bigoplus_{i \in I} M_i$, where $M_i \cong A$ for each $i \in I$.

(g) For $n \in \mathbb{N}$, we denote by A^n the direct sum of A with itself n times:

$$A^n := \bigoplus_{i=1}^{n} A = \underbrace{A \oplus \ldots \oplus A}_{n-\text{times}}.$$

For $i \in \{1, \ldots, n\}$, we define $e_i := (0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0)$. The set $\{e_i\}_{i=1}^n$ is called the *canonical basis* (or *canonical set of generators*) of A^n. By convention, we set $A^0 := \{0\}$.

(h) Let X be a set. We define

$$A^X := \Big\{ f \colon X \to A \mid f(x) \neq 0 \text{ for only finitely many } x \Big\}.$$

For $f, g \in A^X$ and for $a \in A$ we define for each $x \in X$

$$(f+g)(x) := f(x) + g(x) \quad \text{and} \quad (a \cdot f)(x) := af(x).$$

The operations above make A^X into an A-module. Indeed, there is an A-linear isomorphism $A^X \cong \bigoplus_{x \in X} M_x$, where $M_x = A$ for all $x \in X$. Thus, A^X is a free module called *the free module over* X. For each $x \in X$ define $e_x \in A^X$ by

$$e_x(y) = \delta_{xy} = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases}$$

The set $\{e_x\}_{x \in X}$ is called the *canonical basis* (or *canonical set of generators*) of A^X.

Remark 2.20. (a) Note that the free module A^X can be described as the A-module S of finite formal linear combinations

$$\sum_{i=1}^{n} a_i x_i,$$

where $n \in \mathbb{N}_{>0}$, $a_i \in A$ and $x_i \in X$. Indeed, there is an A-linear isomorphism

$$A^X \to S, \quad f \mapsto \sum_{x \in X} f(x) \cdot x,$$

where the sum is finite since $f(x) \neq 0$ for only finitely many $x \in X$. We will adopt the description of A^X as S, since it is more convenient for computations and constructions. Note that in this description of A^X the canonical basis is given by the set X itself: each $x \in X$ can be regarded as the formal linear combination $1 \cdot x$.

(b) Note that the trivial module $M = 0$ is finitely generated: the unique set of generators is the empty-set.

We will mostly focus on finitely generated modules. The following result provides a useful characterization of these modules.

Proposition 2.21. *Let A be a ring and let M be an A-module. Then M is a finitely generated A-module if and only if it is isomorphic to a quotient of a finitely generated free A-module. More precisely, $M \cong A^n/B$ if and only if M has n generators.*

Proof. "$\Rightarrow$": Let $x_1, \ldots, x_n$ be generators of M. Define

$$\varphi\colon A^n \longrightarrow M, \qquad (a_1, \ldots, a_n) \longmapsto \sum_{i=1}^{n} a_i x_i.$$

The map φ is a surjective A-module homomorphism, and thus $A^n/\ker(\varphi) \cong M$ by the homomorphism theorem.

"$\Leftarrow$": If $M \cong A^n/B$, we have a surjective A-module homomorphism $\varphi\colon A^n \to M$. Then the images $\varphi(e_i)$ of the canonical generators e_i generate M. □

Proposition 2.22 (Nakayama's Lemma)**.** *Let A be a ring and let M be a finitely generated A module. Let I be an ideal of A contained in the Jacobson radical J_A. Then $IM = M$ implies $M = \{0\}$.*

Proof. We argue by contradiction. Suppose $M \neq \{0\}$ and let $u_1, \ldots, u_n$ be a minimal set of generators of M. Then $u_n \in M = IM$, thus we may write $u_n = a_1u_1 + \cdots + a_nu_n$ for some $a_i \in I$. But then

$$(1 - a_n)u_n = a_1u_1 + \cdots + a_{n-1}u_{n-1} \tag{2.1}$$

and since $a_n \in I \subseteq J_A$, it follows from Proposition 1.26 that $1 - a_n$ is a unit in A. Hence, by multiplying (2.1) with $(1 - a_n)^{-1}$ we have that $u_n \in Au_1 + \ldots + Au_{n-1}$, a contradiction since the set of u_i is a minimal set of generators of M. □

Corollary 2.23. *Let A be a ring and let M be a finitely generated A-module. Let $N \subseteq M$ be a submodule and let I be an ideal contained in the Jacobson radical J_A. Then $M = IM + N$ implies $N = M$.*

Proof. Observe that

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

Since $M = IM + N$, we have

$$I(M/N) = M/N.$$

Moreover, because M is is finitely generated, the quotient module M/N is finitely generated as well. Therefore, we apply Nakayama's Lemma to M/N and get $M/N = 0$, equivalently, $N = M$. □

Definition 2.24. Let A be a ring and let M be an A-module. The *annihilator of* M is defined as

$$\mathrm{Ann}(M) := \{a \in A \mid am = 0 \text{ for all } m \in M\}$$

This is an ideal in A.

Definition 2.25. An A-module M is called *faithful* if $\mathrm{Ann}(M) = 0$.

Remark 2.26. (a) Let M be an A-module and let $I \subseteq \mathrm{Ann}(M)$ be an ideal. Then we may regard M as an (A/I)-module as follows: for $a \in A$ and for $x \in M$, we define

$$(a + I) \cdot x := ax.$$

This scalar multiplication is well-defined since $IM = 0$.

(b) Let M be a finitely generated A-module and let $\{x_1, \ldots, x_n\}$ be a minimal set of generators of M. Let $I \subseteq J_A$ be an ideal. Since $I \subseteq \mathrm{Ann}(M/IM)$, the quotient M/IM has a natural structure of (A/I)-module by (a). Denote by $[x_1], \ldots, [x_n]$ the residue classes of $x_1, \ldots, x_n$ in M/IM; these classes generate M/IM as an A-module as well as an (A/I)-module. Since the x_i's form a minimal set of generators, by using the same argument as in the proof of Nakayama's lemma we have that $[x_j] \neq 0$ for $1 \leq j \leq n$ and $[x_i] \neq [x_j]$ for any $i \neq j$.

Let $(A, \mathfrak{m}, k)$ be a local ring and let M be a finitely generated A-module. Since $\mathfrak{m} \subseteq \mathrm{Ann}(M/\mathfrak{m}M)$, by Remark 2.26(a) the quotient module $M/\mathfrak{m}M$ can be regarded as an $(A/\mathfrak{m})$-module, i.e., a k-vector space. Since M is a finitely generated A-module, then $M/\mathfrak{m}M$ is a finitely generated A-module, hence a finite dimensional k-vector space. Let $\{x_1, \ldots, x_n\}$ be a minimal set of generators of M and denote by $[x_1], \ldots, [x_n]$ the residue classes of $x_1, \ldots, x_n$ in $M/\mathfrak{m}M$. By Remark 2.26(b) the classes $[x_1], \ldots, [x_n]$ are pairwise distinct. Indeed, we can say more.

Proposition 2.27. *Let $(A, \mathfrak{m}, k)$ be a local ring and let M be a finitely generated A-module. Let $\{x_1, \ldots, x_n\}$ be a minimal set of generators of M. Then the classes $[x_1], \ldots, [x_n]$ form a basis of $M/\mathfrak{m}M$ as a k-vector space. In particular, any minimal set of generators of M contains exactly $\dim_k(M/\mathfrak{m}M)$ elements.*

Proof. It is enough to show that $[x_1], \ldots, [x_n]$ are linearly independent over k.
Let

$$\overline{a_1}[x_1] + \ldots + \overline{a_n}[x_n] = [0], \quad \overline{a_i} \in A/\mathfrak{m} = k.$$

Hence, for $1 \leq i \leq n$ there exists $b_i \in \mathfrak{m}$ such that

$$a_1x_1 + \ldots + a_nx_n = b_1x_1 + \ldots + b_nx_n \in \mathfrak{m}M.$$

Assume by contradiction that $\overline{a_i} \neq \overline{0}$, i.e., $a_i \notin \mathfrak{m}$, for some i. Then $a_i - b_i \notin \mathfrak{m}$ since $b_i \in \mathfrak{m}$, and hence $a_i - b_i$ is invertible since $\mathfrak{m}$ is the unique maximal ideal of the local ring A. It follows that

$$x_i = \sum_{j \neq i} (a_i - b_i)^{-1}(b_j - a_j)x_j,$$

against the minimality of $\{x_1, \dots, x_n\}$. □

Hence, if $\{x_1, \dots, x_n\}$ is a minimal set of generators of M, then $\{[x_1], \dots, [x_n]\}$ is a basis of the k-vector space $M/\mathfrak{m}M$. The following result shows that the converse holds true as well.

Proposition 2.28 (Nakayama's Lemma for Local Rings)**.** *Let $(A, \mathfrak{m}, k)$ be a local ring and let M be a finitely generated A-module. Let $x_1, \dots, x_n$ be elements of M whose residue classes $[x_1], \dots, [x_n] \in M/\mathfrak{m}M$ form a basis of this k-vector space. Then $x_1, \dots, x_n$ generate M.*

Proof. If $M/\mathfrak{m}M = 0$, then the unique subset of M fulfilling the assumptions is the empty-set. The thesis is then true since $M = 0$ by Nakayama's lemma. Now assume $M/\mathfrak{m}M \neq 0$. Then there are elements $x_1, \dots, x_n \in M$ fulfilling the assumptions. Let $N := \sum_{i=1}^{n} Ax_i$. Observe that the map A-linear map

$$\varphi \colon N \to M/\mathfrak{m}M, \qquad x \mapsto [x]$$

is surjective since $\{[x_i] \mid 1 \leq i \leq n\}$ is a basis of $M/\mathfrak{m}M$.

Since M is finitely generated and $J_A = \mathfrak{m}$, if we show that $N + \mathfrak{m}M = M$, then $N = M$ by Corollary 2.23 and we are done. Hence, let us show that $N + \mathfrak{m}M = M$.

"$\subseteq$" is clear. For "$\supseteq$", let $x \in M$ and consider $[x] \in M/\mathfrak{m}M$. Since φ is surjective, there is $n \in N$ such that $[n] = [x]$, and thus $x - n \in \mathfrak{m}M$. Therefore, there exists $y \in \mathfrak{m}M$ such that $x = n + y \in N + \mathfrak{m}M$. □

Remark 2.29. Let $(A, \mathfrak{m}, k)$ be a local ring. Then the following statements are equivalent:

(a) Let M be a finitely generated A-module. If $M = \mathfrak{m}M$, then $M = 0$.

(b) Let M be a finitely generated A-module. Let $x_1, \dots, x_n$ be elements of M whose residue classes $[x_1], \dots, [x_n] \in M/\mathfrak{m}M$ form a basis of this k-vector space. Then $x_1, \dots, x_n$ generate M.

Hence, for a local ring Nakayma's Lemma (Proposition 2.22) and Proposition 2.28 are indeed equivalent and this motivates the name "Nakayama's lemma for local rings" given to Proposition 2.28.

2.5 Exact Sequences

Definition 2.30. Let A be a ring. A sequence of A-modules and A-module homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \dots \tag{2.2}$$

is called

(i) *exact at* M_i if $\ker(f_{i+1}) = \operatorname{im}(f_i)$,

(ii) *exact* if it is exact at every M_i.

In particular, a sequence $0 \to M' \xrightarrow{f} M$ is exact if and only if f is injective, a sequence $M \xrightarrow{g} M'' \to 0$ is exact if and only if g is surjective and

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is exact if and only if f is injective, g is surjective and $\ker(g) = \operatorname{im}(f)$. A sequence of this form is called a *short exact sequence*.

Remark 2.31. Any long exact sequence of the form 2.2 can be split into short exact sequences. Indeed, for each i set $N_i := \operatorname{im}(f_i) = \ker(f_{i+1})$. Then we have a short exact sequence

$$0 \longrightarrow N_i \xrightarrow{j} M_i \xrightarrow{f_{i+1}} N_{i+1} \longrightarrow 0,$$

where $j\colon N_i \to M_i$ is the inclusion map.

Proposition 2.32. *(i) Let*

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \tag{2.3}$$

be a sequence of A-modules and A-module homomorphisms. Then (2.3) *is exact if and only if for all A-modules N the sequence*

$$\begin{array}{ccccc} 0 \longrightarrow \operatorname{Hom}_A(M'', N) & \xrightarrow{\overline{v}} & \operatorname{Hom}_A(M, N) & \xrightarrow{\overline{u}} & \operatorname{Hom}_A(M', N) \\ f \longmapsto f \circ v & & & & \\ & & g \longmapsto g \circ u & & \end{array}$$

is exact.

(ii) Let

$$0 \longrightarrow N' \xrightarrow{u} N \xrightarrow{v} N'' \tag{2.4}$$

be a sequence of A-modules and A-module homomorphisms. Then (2.4) *is exact if and only if for all A-modules M the sequence*

$$\begin{array}{ccccc} 0 \longrightarrow \operatorname{Hom}_A(M, N') & \xrightarrow{\overline{u}} & \operatorname{Hom}_A(M, N) & \xrightarrow{\overline{v}} & \operatorname{Hom}_A(M, N'') \\ f \longmapsto u \circ f & & & & \\ & & g \longmapsto v \circ g & & \end{array}$$

is exact.

Proposition 2.33 (Snake Lemma)**.** *Let*

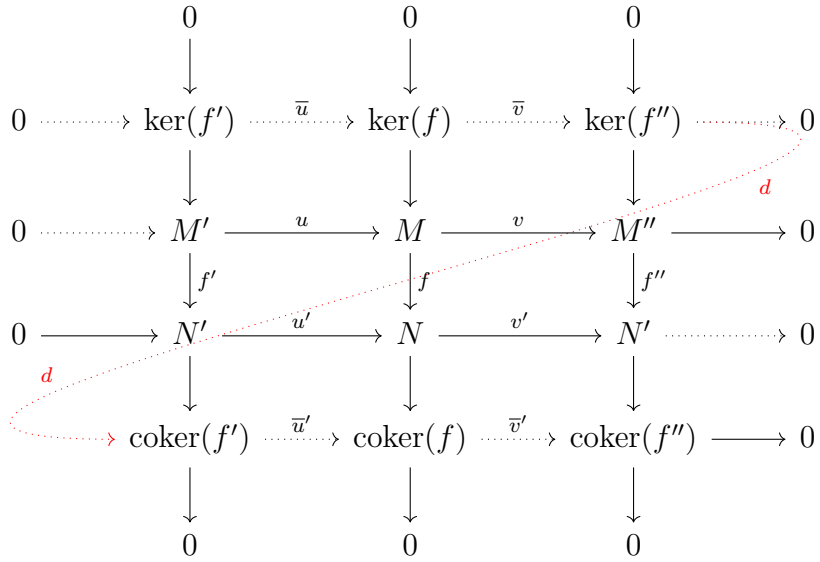
$$\begin{array}{ccccccc} & & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' \longrightarrow 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' \end{array}$$

be a commutative diagram of A-modules and A-module homomorphisms with exact rows. Then there is an exact sequence

$$\begin{array}{ccccccc} \ker(f') & \xrightarrow{\overline{u}} & \ker(f) & \xrightarrow{\overline{v}} & \ker(f'') & & \\ & & & \overset{d}{\searrow} & & & \\ \operatorname{coker}(f') & \xrightarrow{\overline{u}'} & \operatorname{coker}(f) & \xrightarrow{\overline{v}'} & \operatorname{coker}(f'') & & \end{array} \tag{2.5}$$

where $\overline{u}$, $\overline{v}$ are restrictions of u, v and $\overline{u}'$, $\overline{v}'$ are induced by u', v'. The map d is called the connecting homomorphism *(or* boundary homomorphism*). Moreover, if u is injective, then so is the first map in* (2.5)*, and if v' is surjective, then so is the last map in* (2.5)*.*

Proof. We have a diagram as follows:



Define $\overline{u} := u_{|\ker(f')}\colon \ker(f') \to \ker(f)$. We have to check just that $f(u(x)) = 0$ for $x \in \ker(f')$. Since the diagram above is commutative, we have $f(u(x)) = u'(f'(x)) = u'(0) = 0$. Similarly, one can check that $\overline{v} := v_{|\ker(f)}\colon \ker(f) \to \ker(f'')$ is well-defined. Note that $\overline{u}'$ (resp. $\overline{v}'$) is well-defined if $u'(\operatorname{im}(f')) \subseteq \operatorname{im}(f)$ (resp. $v'(\operatorname{im}(f)) \subseteq \operatorname{im}(f'')$). Let $y = f'(x) \in \operatorname{im}(f')$. Then $u'(y) = u'(f'(x)) = f(u(x))$, hence $u'(y) \in \operatorname{im}(f)$. Similarly for $v'(\operatorname{im}(f)) \subseteq \operatorname{im}(f'')$.

Define now $d\colon \ker(f'') \to \operatorname{coker}(f')$ as follows. Let $x \in \ker(f'') \subseteq M''$. Since v is surjective, there exists $t \in M$ such that $v(t) = x$. Hence, $0 = f''(x) = f''(v(t)) = v'(f(t))$, and thus $f(t) \in \ker(v') = \operatorname{im}(u')$, i.e., there exists $y \in N'$ such that

$u'(y) = f(t)$ and we can define $d(x) := [y] = y + \mathrm{im}(f')$. For the time being, it seems that our definition of d depends on two choices: the choice of $t \in M$ such that $v(t) = x$ and the choice of $y \in N'$ such that $u'(y) = f(t)$. Hence, let $t' \in M$ such that $v(t') = x = v(t)$ and let $y' \in N'$ such that $u'(y') = f(t')$. We have to show that $y + \mathrm{im}(f') = y' + \mathrm{im}(f')$, i.e., $y - y' \in \mathrm{im}(f')$. Observe that by definition of t and t' we have $t - t' \in \ker(v) = \mathrm{im}(u)$, i.e., there exists $z \in M'$ such that $u(z) = t - t'$. On the other hand, by definiton of y and y' we have

$$u'(y - y') = f(t - t') = f(u(z)) = u'(f'(z)),$$

hence

$$y - y' - f'(z) \in \ker(u') = 0 \implies y - y' = f'(z).$$

Finally, $y - y' \in \mathrm{im}(f')$ and this shows that the map d is well-defined. It is now easy to check that d is an A-module homomorphism and this is left to the reader. As for the exactness of (2.5), we observe for example that

$$\mathrm{im}(\overline{u}) = \mathrm{im}(u)_{|\ker(f)} = \ker(v)_{|\ker(f)} = \ker(\overline{v}),$$

where the first equality holds because $f \circ u = u' \circ f'$ and u' is injective, the second equality is true because $\mathrm{im}(u) = \ker(v)$ and the third equality is immediate since $\overline{v}$ is the restriction of v to $\ker(f)$. By diagram chasing the reader can fully check the exactness of (2.5). □

Definition 2.34. Let $\mathcal{C}$ be a class of A-modules. A function $\lambda\colon \mathcal{C} \to \mathbb{Z}$ is called *additive* if for every short exact sequence $0 \to M' \to M \to M'' \to 0$ it holds that $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.

Remark 2.35. Let $\mathcal{C}$ be a class of A-modules such that $M = 0 \in \mathcal{C}$. Let $\lambda\colon \mathcal{C} \to \mathbb{Z}$ be an additive function. Since $0 \to M \to M \to M \to 0$ is a short exact sequence, we have by additivity $\lambda(M) = \lambda(M) + \lambda(M)$, hence $\lambda(M) = 0$.

Example 2.36. Let $A = k$ be a field and $\mathcal{C}$ be the class of finite-dimensional k-vector spaces. Then $\lambda\colon \mathcal{C} \to \mathbb{Z}$, $V \to \dim_k V$, is additive.

Proposition 2.37. *Let*

$$0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow \cdots \longrightarrow M_n \longrightarrow 0$$

be an exact sequence of A-modules where all the modules M_i and the kernels of all homomorphisms belong to $\mathcal{C}$. Then for any additive function $\lambda\colon \mathcal{C} \to \mathbb{Z}$ on $\mathcal{C}$ we have

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

Proof. Like in Remark 2.31, split the exact sequence into short exact sequences $0 \to N_i \to M_i \to N_{i+1} \to 0$, where $N_0 = N_{n+1} = 0$. Then for each $0 \le i \le n$ we have $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$, namely:

$$\begin{aligned} \lambda(M_0) &= \lambda(N_0) + \lambda(N_1) \\ \lambda(M_1) &= \lambda(N_1) + \lambda(N_2) \\ &\cdots \\ \lambda(M_{n-1}) &= \lambda(N_{n-1}) + \lambda(N_n) \\ \lambda(M_n) &= \lambda(N_n) + \lambda(N_{n+1}) \end{aligned}$$

We sum these $n+1$ equality with alternating signs, and since $\lambda(N_0) = \lambda(N_{n+1}) = 0$, on the right-hand side all terms cancel pairwise, yielding

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

□

2.6 Tensor Products of Modules

Definition 2.38. Let A be a ring and let M, N, P be A-modules. A map $f\colon M \times N \to P$ is called *A-bilinear* if for each $x \in M$, the map $N \to P$, $y \mapsto f(x,y)$, is A-linear, and for each $y \in N$ the map $M \to P$, $x \mapsto f(x,y)$, is A-linear.

Given A-modules M, N, we construct an A-module T, called the *tensor product of M and N*, characterized by the property that, for any A-module P, there is a natural one-to-one correspondence between A-bilinear maps $M \times N \to P$ and A-linear maps $T \to P$. The following proposition makes this precise.

Proposition 2.39. *Let A be a ring and let M, N be A-modules. Then there exists a pair (T, g), where T is an A-module and $g\colon M \times N \to T$ is an A-bilinear map with the following property: For any A-module P and any A-bilinear map $f\colon M \times N \to P$, there exists a unique A-linear map $f'\colon T \to P$ such that $f = f' \circ g$, i.e., the diagram*

$$\begin{array}{ccc} & & T \\ & \overset{g}{\nearrow} & \big\downarrow {\scriptstyle f'} \\ M \times N & \xrightarrow[f]{} & P \end{array} \tag{2.6}$$

commutes. Moreover, if (T, g) and (T', g') are two pairs with the above property, then there is a unique isomorphism $h\colon T \to T'$ such that $h \circ g = g'$.

Proof. (i) *Uniqueness*: Assume we have two pairs (T, g) and (T', g') with this property. Applying the property of (T, g) with $P = T'$ and $g'\colon M \times N \to T'$,

and similarly applying the property of (T', g') with $P = T$ and $g\colon M\times N \to T$, we obtain the following commutative diagrams

$$\begin{array}{ccc} & & T \\ & \overset{g}{\nearrow} & \downarrow{\scriptstyle h} \\ M\times N & \xrightarrow{g'} & T' \end{array} \qquad \begin{array}{ccc} & & T' \\ & \overset{g'}{\nearrow} & \downarrow{\scriptstyle h'} \\ M\times N & \xrightarrow{g} & T \end{array}$$

By combining the two diagrams above, we have the following commutative diagram

$$\begin{array}{ccccc} & & & & T \\ & \overset{g}{\nearrow} & & \overset{h}{\downarrow} & \\ M\times N & \xrightarrow{g'} & T' & & \mathrm{id}_T \\ & \underset{g}{\searrow} & & \underset{h'}{\downarrow} & \\ & & & & T \end{array}$$

and applying the property of (T, g) with $P = T$ and $g\colon M \times N \to T$, we obtain $h' \circ h = \mathrm{id}_T$. Similarly we show that $h \circ h' = \mathrm{id}_{T'}$.

(ii) *Existence*: Let C be the free A-module $A^{M\times N}$, whose elements are finite formal linear combinations of elements of $M \times N$ with coefficients in A, i.e., they are expressions of the form $\sum_i a_i(x_i, y_i)$.

Let D be the submodule of C generated by the elements of C of the form

- $(x + x', y) - (x, y) - (x', y)$,
- $(x, y + y') - (x, y) - (x, y')$,
- $(ax, y) - a(x, y)$,
- $(x, ay) - a(x, y)$,

where $x, x' \in M$, $y, y' \in N$, $a \in A$. Let $T = C/D$. For each canonical generator (x, y) of C denote by $x \otimes y$ its image in T. Then T is generated by elements of the form $x \otimes y$, and from the definitions we have for $x \in M$, $y \in N$ and $a \in A$:

$$\begin{gathered}(x + x') \otimes y = x \otimes y + x' \otimes y, \qquad x \otimes (y + y') = x \otimes y + x \otimes y', \\ (ax) \otimes y = a(x \otimes y) = x \otimes (ay).\end{gathered}$$

Hence, the map $g\colon M \times N \to T$, $(x, y) \mapsto x \otimes y$ is A-bilinear. Let P be an A-module and let $f\colon M \times N \to P$ be an A-bilinear map. Then

$$\overline{f}\colon C \to P, \qquad \sum_{i=1}^{k} a_i(x_i, y_i) \longmapsto \sum_{i=1}^{k} a_i f(x_i, y_i)$$

is an A-linear map that vanishes on all generators of D, hence $D \subseteq \ker(\overline{f})$. Thus, $\overline{f}$ induces a well-defined A-linear map $f' \colon T \to P$ such that $f'(x \otimes y) = f(x, y)$. Since the elements of the form $x \otimes y$ generate T, the condition $x \otimes y \mapsto f(x, y)$ uniquely determines f'. Thus, f' is the unique A-linear map such that $f' \circ g = f$. In other words, the pair (T, g) satisfies the required property.

□

Definition 2.40. Let A be a ring and let M, N be A-modules. A pair (T, g) fulfilling the property of Proposition 2.39 is called *the tensor product of M and N as A-modules* and is denoted by $(M \otimes_A N, \otimes)$. When the ring A is clear from the context, we just write $M \otimes N$ instead of $M \otimes_A N$.

Remark 2.41. Let M, N be A-modules.

(a) It is clear from the construction that $M \otimes_A N$ is generated as an A-module by the elements of the form $x \otimes y$, where $x \in M$ and $y \in M$. These elements are called *pure tensors*. If $(x_i)_{i \in I}$ respectively $(y_j)_{j \in J}$ are families of generators of M respectively N, then the set $\{x_i \otimes y_j \mid i \in I,\ j \in J\}$ generates $M \otimes_A N$. In particular, if M and N are finitely generated A-modules, then so is $M \otimes N$.

(b) Every element in $M \otimes_A N$ can be written as a finite sum of pure tensors. Indeed, let $z \in M \otimes_A N$. Then

$$z = \sum_{i=1}^{n} a_i(x_i \otimes y_i) = \sum_{i=1}^{n} (a_i x_i) \otimes y_i = \sum_{i=1}^{n} x_i \otimes (a_i y_i).$$

(c) The notation $x \otimes y$ is inherently ambiguous unless we specify the tensor product to which it belongs. Indeed, let M' respectively N' be submodules of M respectively N, and let $x \in M'$, $y \in N'$. It can happen that $x \otimes y$ is zero as an element of $M \otimes N$, while $x \otimes y$ is nonzero as an element of $M' \otimes N'$. For example, take $A = \mathbb{Z}$, $M = \mathbb{Z}/4\mathbb{Z}$, $M' = 2\mathbb{Z}/4\mathbb{Z}$, $N = N' = \mathbb{Z}/2\mathbb{Z}$, $x = \overline{2}$ and $y = \overline{1}$. Then $x \otimes y = 0$ as an element of $M \otimes N = (\mathbb{Z}/4\mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z}$ since

$$x \otimes y = \overline{2} \otimes \overline{1} = 2(\overline{1} \otimes \overline{1}) = \overline{1} \otimes \overline{2} = \overline{1} \otimes \overline{0} = 0.$$

On the other hand, $M' \otimes N' = (2\mathbb{Z}/4\mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z}$ is generated by $x \otimes y = \overline{2} \otimes \overline{1}$. Moreover, $M' \otimes N'$ is a nontrivial $\mathbb{Z}$-module since

$$(2\mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}, \quad (\overline{a}, \overline{b}) \mapsto \overline{a/2} \cdot \overline{b},$$

is a nonzero $\mathbb{Z}$-bilinear map. Therefore, it must be $x \otimes y \neq 0$.

Proposition 2.42. *Let M and N be A-modules. Let $x_i \in M$ and $y_i \in N$ be elements such that $\sum_i x_i \otimes y_i = 0$ as an element of $M \otimes N$. Then there exist finitely generated submodules $M_0 \subseteq M$ and $N_0 \subseteq N$ such that $\sum_i x_i \otimes y_i = 0$ as an element of $M_0 \otimes N_0$.*

Proof. If $\sum_i x_i \otimes y_i = 0$ in $M \otimes N$, then $\sum_i (x_i, y_i) \in D$. Therefore, we can write

$$\sum_i (x_i, y_i) = \sum_j a_j z_j,$$

where $a_j \in A$ and each $z_j \in D$ is one of the (maybe infinitely many!) generators of D. Let M_0 be the submodule of M generated by the x_i's and all the elements of M that appear as first coordinates in each of the z_j. Similarly, let N_0 be the submodule of N generated by the y_i's and all the elements of N that appear as second coordinates in each of the z_j. Then, by construction of $M_0 \otimes N_0$, it is clear that $\sum_i x_i \otimes y_i = 0$ as an element of $M_0 \otimes N_0$. □

One can also define the tensor product of finitely many A-modules.

Definition 2.43. Let A be a ring. Let $M_1, \ldots, M_n, P$ be A-modules. A map $f\colon M_1 \times \ldots \times M_n \to P$ is called *n-linear over A* if for each $i \in \{1, \ldots, n\}$ and for all fixed $\overline{x}_j \in M_j$ with $j \neq i$, the map $M_i \to P,\ x_i \mapsto f(\overline{x}_1, \ldots, x_i, \ldots, \overline{x}_n)$, is A-linear.

Proposition 2.44. *Let $M_1, \ldots, M_n$ be A-modules. Then there exists a pair (T, g), consisting of an A-module T and an n-linear map $g\colon \prod_{i=1}^n M_i \to T$, with the following property: For any A-module P and any n-linear map $f\colon \prod_{i=1}^n M_i \to P$, there exists a unique linear map $f'\colon T \to P$ such that $f = f' \circ g$. Moreover, if (T, g) and (T', g') are two pairs with this property, then there is a unique isomorphism $h\colon T \to T'$ such that $h \circ g = g'$.*

Definition 2.45. Let A be a ring. Let $M_1, \ldots, M_n$ be A-modules. A pair (T, g) fulfilling the property of Proposition 2.44 is called *the tensor product of $M_1, \ldots, M_n$ as A-modules* and denoted by $(M_1 \otimes_A \ldots \otimes_A M_n, \otimes)$. When the ring A is clear from the context, we just write $M_1 \otimes \ldots \otimes M_n$ instead of $M_1 \otimes_A \ldots \otimes_A M_n$.

Proposition 2.46 (Canonical Isomorphisms)**.** *Let M, N, P be A-modules. Then there exist unique isomorphisms*

(i) $M \otimes N \to N \otimes M$,

(ii) $(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$,

(iii) $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$,

(iv) $A \otimes M \to M$,

such that, respectively,

(i) $x \otimes y \longmapsto y \otimes x$,

(ii) $(x \otimes y) \otimes z \longmapsto x \otimes (y \otimes z) \longmapsto x \otimes y \otimes z$,

(iii) $(x, y) \otimes z \longmapsto (x \otimes z, y \otimes z)$,

(iv) $a \otimes x \longmapsto ax$.

Proof. We partially show (ii), the rest of the assertions are left to the reader as an exercise. We construct A-linear maps $f\colon (M \otimes N) \otimes P \to M \otimes N \otimes P$ and $g\colon M \otimes N \otimes P \to (M \otimes N) \otimes P$ such that

$$f((x \otimes y) \otimes z) = x \otimes y \otimes z, \qquad g(x \otimes y \otimes z) = (x \otimes y) \otimes z.$$

To construct f, we fix $z \in P$. The map

$$M \times N \longrightarrow M \otimes N \otimes P, \qquad (x, y) \longmapsto x \otimes y \otimes z$$

is A-bilinear, so it induces an A-linear map $f_z\colon M \otimes N \to M \otimes N \otimes Z$ such that $f_z(x \otimes y) = x \otimes y \otimes z$. Next, we consider the map

$$F\colon (M \otimes N) \times P \longrightarrow M \otimes N \otimes P, \qquad (t, z) \longmapsto f_z(t).$$

This map is A-linear in t since f_z is so; we show that F is also A-linear in z. Namely, we have to show that for $a, b \in A$ and $z, z' \in P$ it holds

$$f_{az+bz'}(t) = af_z(t) + bf_{z'}(t) \quad \text{for all } t \in M \otimes N.$$

It is enough to show the previous equality for $t = x \otimes y$ since if two A-linear maps agree on a set of generators, they are equal. Now, we have

$$f_{az+bz'}(x \otimes y) = x \otimes y \otimes (az + bz') = a(x \otimes y \otimes z) + b(x \otimes y \otimes z') = af_z(x \otimes y) + bf_{z'}(x \otimes y),$$

and this shows that F is A-linear in z, hence A-bilinear. Thus, F induces an A-linear map

$$f\colon (M \otimes N) \otimes P \longrightarrow M \otimes N \otimes P, \qquad (x \otimes y) \otimes z \longmapsto x \otimes y \otimes z.$$

To construct g, consider the map

$$M \times N \times P \longrightarrow (M \otimes N) \otimes P, \qquad (x, y, z) \longmapsto (x \otimes y) \otimes z.$$

This map is A-linear in each variable, so it induces an A-linear map

$$g\colon M \otimes N \otimes N \longrightarrow (M \otimes N) \otimes P, \qquad x \otimes y \otimes z \longmapsto (x \otimes y) \otimes z.$$

The A-linear maps $f \circ g$ and $\mathrm{id}_{M \otimes N \otimes P}$ agree on a set of generators, hence $f \circ g = \mathrm{id}_{M \otimes N \otimes P}$. Similarly, $g \circ f = \mathrm{id}_{(M \otimes N) \otimes P}$, and thus f and g are isomorphisms. The uniqueness of f (respectively g) is clear since the condition $(x \otimes y) \otimes z \mapsto x \otimes y \otimes z$ (respectively $x \otimes y \otimes z \mapsto (x \otimes y) \otimes z$) uniquely determines f (respectively g). $\square$

Definition 2.47. Let $f\colon M \to M'$ and $g\colon N \to N'$ be two A-module homomorphisms. We define

$$h\colon M \times N \to M' \otimes N', \qquad (x, y) \longmapsto f(x) \otimes g(y).$$

One checks easily that h is A-bilinear, thus it factors through an A-module homomorphism

$$h'\colon M \otimes N \longrightarrow M' \otimes N'.$$

We call this map *the tensor product of f and g*, and denote it by $f \otimes g$. Note that

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y).$$

2.7 Algebras, Restriction and Extension of Scalars

Definition 2.48. Let A, B be rings and let $f\colon A \to B$ be a ring homomorphism. Then B has a natural A-module structure as follows:

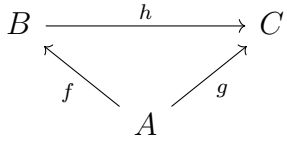
$$a \cdot b := f(a)b \quad \text{for all } a \in A, b \in B.$$

Hence, B has both a ring structure and an A-module structure which are compatible, i.e.,

$$a \cdot (bc) = (a \cdot b)c = b(a \cdot c).$$

The ring B together with the ring homomorphism f is called an *A-algebra*.

Definition 2.49. Let B and C be A-algebras with ring homomorphisms $f\colon A \to B$ and $g\colon A \to C$, respectively. A ring homomorphism $h\colon B \to C$ is called an *A-algebra homomorphism* if h is also A-linear. Equivalently, a ring homomorphism $h\colon B \to C$ is called an A-algebra homomorphism if $h \circ f = g$, i.e., if we have a commutative diagram



Definition 2.50. (a) A ring homomorphism $f\colon A \to B$ is called *finite* and B is called a *finite A-algebra* if B is finitely generated as an A-module.

(b) A ring homomorphism $f\colon A \to B$ is called *of finite type* and B is called a *finitely generated A-algebra* if there exist $b_1, \ldots, b_n \in B$ such that every element in B is a polynomial expression in $b_1, \ldots, b_n$ with coefficients in A. In other words, $B = A[b_1, \ldots, b_n]$, where

$$A[b_1, \ldots, b_n] := \Big\{ g(b_1, \ldots, b_n) \mid g \in A[X_1, \ldots, X_n] \Big\} \subseteq B$$

is in general a subring of B. Equivalently, B is called a finitely generated A-algebra if there exists a surjective ring homomorphism $A[X_1, \ldots, X_n] \twoheadrightarrow B$.

Example 2.51. Let K be a field. The polynomial ring $K[X_1, \ldots, X_n]$ is a finitely generated K-algebra, but it is not finite over K. Indeed, it admits the following direct sum decomposition as a K-vector space

$$K[X_1, \ldots, X_n] = \bigoplus_{d \geq 0} K[X_1, \ldots, X_n]_d,$$

where $K[X_1, \ldots, X_n]_d$ denotes the K-vector space of homogeneous polynomials of degree d.

Definition 2.52 (Restriction of Scalars)**.** Let B be an A-algebra with ring homomorphism $f\colon A \to B$. Let N be a B-module. Then there is an induced A-module structure on N: for all $a \in A$ and for all $x \in N$ we define

$$a \cdot x := f(a) \cdot x.$$

The A-module structure on N is called *the restriction of scalars of N to A.*

Let B be an A-algebra with ring homomorphism $f\colon A \to B$. If N is a finitely generated B-module, it is natural to ask if it is also finitely generated as an A-module. This holds true if B is a finite A-algebra.

Proposition 2.53. *Let B be an A-algebra with ring homomorphism $f\colon A \to B$ and let N be a finitely generated B-module. Assume that B is a finite A-algebra. Then N is finitely generated as an A-module.*

Proof. Let $\{x_1, \ldots, x_n\} \subseteq N$ be a generating set of the B-module N and let $\{y_1, \ldots, y_m\}$ be a generating set for the A-module B. Then the set

$$\{y_i x_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$$

is a generating set of the A-module N. □

Definition 2.54 (Extension of Scalars)**.** Let B be an A-algebra with ring homomorphism $f\colon A \to B$. Let M be an A-module. The tensor product $M_B := M \otimes_A B$ has a natural structure as a B-module: For all $b \in B$, $\beta \in B$ and $m \in M$ we set

$$b \cdot (m \otimes \beta) := m \otimes (b\beta).$$

The B-module M_B is called *the extension of scalars of M to B.*

Definition 2.55. Let A, B be rings. An (A, B)*-module* N is an abelian group which is both an A-module and a B-module and the two structures are compatible, i.e., for all $a \in A$, $b \in B$ and $x \in N$ it holds

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

A map $f\colon N \to N'$ between (A, B)-modules is an (A, B)*-module homomorphism* if it is A-linear as well as B-linear.

Remark 2.56. Let A, B be rings. Let M be an A-module, let N be an (A, B)-module and let P be a B-module. Then $M \otimes_A N$ and $N \otimes_B P$ have a natural structure as (A, B)-modules.

Remark 2.57. Let B be an A-algebra.

(a) Let N be a B-module. Then N together with its restriction of scalars to A is clearly an (A, B)-module. In particular, B is itself an (A, B)-module.

(b) Let M be an A-module. Then the extension of scalars $M_B = M \otimes_A B$ is an (A, B)-module by Remark 2.56 since B is an (A, B)-module.

The following proposition gives an important and useful canonical isomorphism.

Proposition 2.58. *Let A, B be rings. Let M be an A-module, let N be an (A, B)-module and let P be a B-module. Then there exists a unique (A, B)-module isomorphism*

$$(M \otimes_A N) \otimes_B P \xrightarrow{\sim} M \otimes_A (N \otimes_B P)$$

such that $(x \otimes y) \otimes z \longmapsto x \otimes (y \otimes z)$.

Proof. Exercise. □

Corollary 2.59. *Let B be an A-algebra. Let M be an A-module and let N, P be B-modules. Then there exists a unique B-linear isomorphism*

$$(M \otimes_A N) \otimes_B P \xrightarrow{\sim} M \otimes_A (N \otimes_B P)$$

such that $(x \otimes y) \otimes z \longmapsto x \otimes (y \otimes z)$.

2.8 Tensor Product of Algebras

Let B and C be two A-algebras with ring homomorphisms $f\colon A \to B$ and $g\colon A \to C$, respectively. Consider the tensor product

$$D := B \otimes_A C.$$

We would like to endow D with an A-algebra structure. For this purpose, we need to define a product $\cdot : D \times D \to D$ which is A-bilinear. The natural definition would be

$$\cdot : D \times D \to D, \quad (b \otimes c, b' \otimes c') \longmapsto bb' \otimes cc'.$$

Indeed, this is the correct definition, provided that it is well-defined! Hence, we need an argument to show it. Consider the map

$$B \times C \times B \times C \to D, \quad (b, b', c, c') \longmapsto bb' \otimes cc'.$$

This is a 4-linear map over A, hence, by the universal property of the tensor product (Proposition 2.44), it induces a unique A-linear map

$$B \otimes_A C \otimes_A B \otimes_A C \to D,$$

Now, by the canonical isomorphism (ii) from Proposition 2.46, we have an A-linear map

$$D \otimes D \to D, \quad (b \otimes c) \otimes (b' \otimes c') \longmapsto bb' \otimes cc'.$$

By the universal property of the tensor product (Proposition 2.39), such an A-linear map induces a unique A-bilinear map

$$\cdot : D \times D \to D, \quad (b \otimes c, b' \otimes c') \longmapsto bb' \otimes cc'.$$

Hence, we have a well-defined product on D:

$$\Big(\sum_i b_i \otimes c_i\Big) \cdot \Big(\sum_j b_j \otimes c_j\Big) := \sum_{i,j} b_i b'_j \otimes c_i c'_j.$$

It is easy to see that $(D, +, \cdot)$ is a ring: the associativity (resp. the commutativity) of $\cdot$ is a consequence of the associativity (resp. the commutativity) of the products in B and C, the distributivity laws hold by A-bilinearity, and $1_D = 1_B \otimes 1_C$. Moreover, for all $a \in A$, $b \in B$ and $c \in C$ it holds

$$\begin{aligned} a \cdot (b \otimes c) &= (a \cdot b) \otimes c = f(a) \otimes c \\ a \cdot (b \otimes c) &= b \otimes (a \cdot c) = b \otimes g(a)c \end{aligned}$$

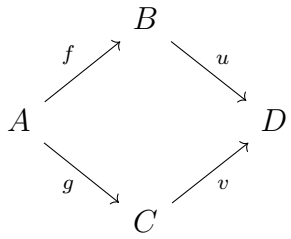
In particular, if $b = 1_B$ and $c = 1_C$, we have

$$f(a) \otimes 1_C = 1_B \otimes g(a).$$

Therefore, D is an A-algebra with ring homomorphism

$$A \to D, \quad a \mapsto f(a) \otimes 1_C = 1_B \otimes g(a),$$

and we have the following commutative diagram (of ring homomorphisms)



where $u : B \to D$, $b \mapsto b \otimes 1_C$ and $v : C \to D$, $c \mapsto 1_B \otimes c$.

2.9 Exactness of Tensor Products

Let $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ be an exact sequence of A-modules and let N be an A-module. Is the sequence $M_1 \otimes N \xrightarrow{f\otimes \mathrm{id}_N} M_2 \otimes N \xrightarrow{g\otimes \mathrm{id}_N} M_3 \otimes N$ exact? The answer is in general no, as shown by the following example.

Example 2.60. Let $A = \mathbb{Z}$ and let $N = \mathbb{Z}/2\mathbb{Z}$. Consider the exact sequence

$$\begin{aligned} 0 \longrightarrow \mathbb{Z} &\xrightarrow{f} \mathbb{Z} \\ x &\longmapsto 2x. \end{aligned}$$

Then by tensoring with N, we have the sequence

$$0 \longrightarrow \mathbb{Z} \otimes N \xrightarrow{f\otimes \mathrm{id}_N} \mathbb{Z} \otimes N.$$

Note that $(f \otimes \mathrm{id}_N)(x \otimes y) = f(x) \otimes y = (2x) \otimes y = x \otimes (2y) = x \otimes 0 = 0$, thus $f \otimes \mathrm{id}_N$ is far from being injective and the sequence is not exact.

However, we can show that "tensoring is right exact". To do so, we need the following lemma.

Lemma 2.61. *Let M, N, P be A-modules. Then we have a canonical isomorphism*

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)).$$

Proof. Let $f\colon M \otimes_A N \to P$ be an A-linear map. By the universal property of the tensor product (Proposition 2.39), there exists a unique A-bilinear map $f'\colon M \times N \to P$ such that $f(m \otimes n) = f'(x, y)$. Now, we construct an A-linear map

$$\overline{f'}\colon M \longrightarrow \mathrm{Hom}_A(N, P), \qquad m \longmapsto (n \mapsto f'(m, n)).$$

On the other hand, if $g\colon M \to \mathrm{Hom}_A(N, P)$ is an A-linear map, we define the A-bilinear map $\widetilde{g}\colon M \times N \longrightarrow P$, $(m, n) \longmapsto [g(m)](n)$, which induces by the universal property of the tensor product a unique A-linear map

$$\widehat{g}\colon M \otimes N \longrightarrow P, \quad m \otimes n \longmapsto [g(m)](n),$$

These two constructions are inverse to each other, yielding a one-to-one correspondence

$$\mathrm{Hom}_A(M \otimes_A N, P) \to \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)), \quad f \longmapsto \overline{f'},$$

which is indeed A-linear. □

Proposition 2.62 ("Tensoring is Right Exact")**.** *Let*

$$M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be an exact sequence of A-modules. Furthermore, let N be an A-module. Then the sequence

$$M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0$$

is exact.

Proof. Let P be an A-module. Then the sequence

$$0 \to \mathrm{Hom}(M_3, \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M_2, \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M_1, \mathrm{Hom}(N, P))$$

is exact by Proposition 2.32(i). Thus, by the previous lemma, we have an exact sequence

$$0 \longrightarrow \mathrm{Hom}(M_3 \otimes N, P) \longrightarrow \mathrm{Hom}(M_2 \otimes N, P) \longrightarrow \mathrm{Hom}(M_1 \otimes N, P).$$

Hence, since P is an arbitrary A-module, by Proposition 2.32(ii) the sequence

$$M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0$$

is exact. □

Definition 2.63. An A-module N is called *flat* if tensoring with N is also left exact, i.e., for any short exact sequences $0 \to M_1 \to M_2 \to M_3 \to 0$ of A-modules, the sequence

$$0 \longrightarrow M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0$$

is exact.

Proposition 2.64. *Let N be an A-module. Then the following are equivalent:*

(i) N is flat.

(ii) For any exact sequence $M_1 \to M_2 \to M_3$ of A-modules, the sequence $M_1 \otimes N \to M_2 \otimes N \to M_3 \otimes N$ is exact.

(iii) If $f\colon M \to M'$ is an injective A-linear map, then $f \otimes \mathrm{id}_N\colon M \otimes N \to M' \otimes N$ is injective.

(iv) If $f\colon M \to M'$ is an injective A-linear map where M and M' are finitely generated, then $f \otimes \mathrm{id}_N\colon M \otimes N \to M' \otimes N$ is injective.

Proof. (ii) ⇒ (i). Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence of A-modules. Split it into the three exact sequences

$$0 \to M_1 \to M_2, \quad M_1 \to M_2 \to M_3, \quad M_2 \to M_3 \to 0,$$

and then apply (ii) three times.

(i) ⇒ (ii). Let $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ be an exact sequence. Then the sequences

$$\begin{aligned} &0 \to \ker(f) \to M_1 \to \mathrm{im}(f) \to 0, \\ &0 \to \mathrm{im}(f) \to M_2 \to \mathrm{im}(g) \to 0 \\ &0 \to \mathrm{im}(g) \to M_2 \to \mathrm{coker}(g) \to 0 \end{aligned}$$

Now apply (i) three times.

(i) $\Rightarrow$ (iii). Let $f\colon M \to M'$ be an injective A-linear map. Consider the short exact sequence $0 \to M \xrightarrow{f} M' \to M'/\operatorname{im}(f) \to 0$. Since N is flat, the sequence

$$0 \to M \otimes N \xrightarrow{f\otimes \mathrm{id}_N} M' \otimes N \to (M/M') \otimes N \to 0$$

is exact. In particular, $f \otimes \mathrm{id}_N$ is injective.

(iii) $\Rightarrow$ (i). Let $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ be a short exact sequence. By Proposition 2.62 the sequence

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

is exact. By (iii) the map $f \otimes \mathrm{id}_N$ is injective, hence the sequence

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

is exact.

(iii) $\Rightarrow$ (iv). This is obvious.

(iv) $\Rightarrow$ (iii). Let $f\colon M \to M'$ be an injective A-linear map. We have to show that $f \otimes \mathrm{id}_N\colon M \otimes N \to M' \otimes N$ is also injective. Let $u = \sum_i x_i \otimes y_i \in \ker(f \otimes \mathrm{id}_N)$, where $x_i \in M$ and $y_i \in N$. This means

$$(f \otimes \mathrm{id}_N)(u) = \sum_i f(x_i) \otimes y_i = 0 \in M' \otimes N.$$

Let M_0 be the submodule of M generated by the elements x_i's. Note that $f(M_0)$ is generated by the elements $f(x_i)$'s. By the same argument given in the proof of Proposition 2.42, there exists a finitely generated A-module $M_0' \subseteq M'$ such that

$$\sum_i f(x_i) \otimes y_i = 0 \in M_0' \otimes N.$$

Since M_0' contains by constructions the elements $f(x_i)$'s, we have

$$f(M_0) \subseteq M_0'.$$

Let u_0 denote $\sum_i x_i \otimes y_i$ as an element of $M_0 \otimes N$. In other words, if $j\colon M_0 \to M$ is the inclusion map, we have

$$(j \otimes \mathrm{id}_N)(u_0) = u. \tag{2.7}$$

Since M_0 and M_0' are finitely generated and the map $f_{|M_0}\colon M_0 \to M_0'$ is injective, by (iv) the map

$$f|_{M_0} \otimes \mathrm{id}_N\colon M_0 \otimes N \to M_0' \otimes N$$

is injective. Hence, $(f|_{M_0} \otimes \mathrm{id}_N)(u_0) = \sum_i f(x_i) \otimes y_i = 0$ implies $u_0 = 0$, which in turn implies $u = 0$ by (2.7). Finally, we have just shown that $\ker(f \otimes \mathrm{id}_N) = 0$, i.e., $f \otimes \mathrm{id}_N$ is injective. $\square$

Flatness is preserved under extension of scalars.

Proposition 2.65. *Let $f\colon A \to B$ be a ring homomorphism and let M be a flat A-module. Then the extension of scalars $M_B = M \otimes_A B$ is a flat B-module.*

Proof. Exercise. □

Chapter 3

Localizations

Definition 3.1. Let A be a ring. A *multiplicative set* $S \subseteq R$ is a subset satisfying the following properties:

(i) $1_A \in S$

(ii) $xy \in S$ if $x, y \in S$.

Let A be a ring and let $S \subseteq A$ be a multiplicative set. We define an equivalence relation on $A \times S$ as follows:

$$(a, s) \sim (a', s') \quad \overset{\text{def}}{\iff} \quad \exists u \in S : \ u(as' - a's) = 0.$$

The relation $\sim$ is clearly reflexive and symmetric. We show the transitivity. Assume that $(a, s) \sim (a', s')$ and $(a', s') \sim (a'', s'')$. We have to show that $(a, s) \sim (a'', s'')$. By assumption, there exist $u, v \in S$ such that

$$u(as' - a's) = 0, \qquad v(a's'' - a''s') = 0.$$

In other words,

$$uas' = ua's, \qquad va's'' = va''s'.$$

Multiplying these equalities with vs'' and us respectively, we obtain

$$uvs'as'' = uvs'a''s \quad \iff \quad \underbrace{uvs'}_{\in S}(as'' - a''s) = 0,$$

whence $(a, s) \sim (a'', s'')$.

The set of equivalence classes $(A \times S)/\sim$ is denoted by $S^{-1}A$. For $a \in A$ and $s \in S$, we denote the equivalence class $[(a, s)]_\sim$ by a/s. Moreover, we define on $S^{-1}A$ the following operations:

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'},$$
$$\frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}.$$

It is easy to check that the operations above are well-defined and that $(S^{-1}A, +, \cdot)$ is a ring with $1_{S^{-1}A} = 1/1$.

Definition 3.2. The ring $S^{-1}A$ is called *the ring of fractions of A with respect to S* (or *the localization of A along S*).

Example 3.3. Let A be a ring and let $S \subseteq A$ be a multiplicative set.

(a) If $0 \in S$, then $S^{-1}A = \{0\}$.

(b) If A is an integral domain and $S = A \setminus \{0\}$, then $S^{-1}A = Q(A)$ is the field of fractions of A.

(c) Let $\mathfrak{p}$ be a prime ideal in A and let $S = A \setminus \mathfrak{p}$. Then $S^{-1}A$ is called *the localization of A at $\mathfrak{p}$* and denoted by $A_{\mathfrak{p}}$.

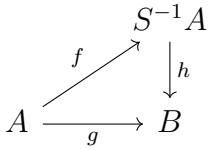
(d) Let $f \in A$ and let $S = \{f^n\}_{n\in\mathbb{N}} = \{1, f, f^2, \dots\}$. Then $S^{-1}A$ is called *the localization of A at f* and denoted by A_f.

Let A be a ring and let $S \subseteq A$ be a multiplicative set. There is a canonical ring homomorphism

$$f\colon A \to S^{-1}A, \quad a \mapsto \frac{a}{1}.$$

This homomorphism is in general not injective. The pair $(S^{-1}A, f)$ has a universal property.

Proposition 3.4 (Universal Property of $S^{-1}A$)**.** *Let A be a ring, let $S \subseteq A$ be a multiplicative set and let $f\colon A \to S^{-1}A,\ a \mapsto a/1$. Let $g\colon A \to B$ be a ring homomorphism such that $g(s)$ is a unit in B for all $s \in S$. Then there exists a unique ring homomorphism $h\colon S^{-1}A \to B$ such that $h \circ f = g$, i.e., the following diagram commutes*



Proof. Uniqueness. Assume that $h\colon S^{-1}A \to B$ is a ring homomorphism fulfilling the hypothesis. Then

$$h(a/s) = h(a/1 \cdot 1/s) = h(a/1)h((s/1)^{-1}) = g(a)g(s)^{-1}.$$

Hence, h is uniquely determined.

Existence. If we define the map h as above, we can easily see that it is well-defined. Assume $a/s = a'/s'$, i.e., $u(as' - a's) = 0$ for some $u \in S$. Then $g(u)[g(a')g(s) - g(a)g(s')] = 0$, and since $g(u)$ is invertible we have

$$g(a')g(s) - g(a)g(s') = 0 \quad \iff \quad g(a')g(s')^{-1} = g(a)g(s)^{-1}.$$

□

The ring homomorphism $f\colon A \to S^{-1}A$ has the following properties:

(i) $f(s)$ is a unit in $S^{-1}A$ for all $s \in S$,

(ii) $f(a)$ implies $as = 0$ for some $s \in S$,

(iii) Every element in $S^{-1}A$ is of the form $f(a)f(s)^{-1}$ for some $a \in A$, $s \in S$.

Indeed, the three properties above characterize $S^{-1}A$.

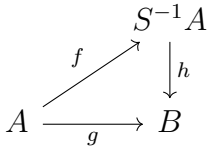
Proposition 3.5. *Let A be a ring, let $S \subseteq A$ be a multiplicative set and let $f\colon A \to S^{-1}A,\ a \mapsto a/1$. Let $g\colon A \to B$ be a ring homomorphism such that*

(i) $g(s)$ is a unit in B for all $s \in S$,

(ii) $g(a)$ implies $as = 0$ for some $s \in S$,

(iii) Every element in B is of the form $g(a)g(s)^{-1}$ for some $a \in A$, $s \in S$.

Then there exists a unique ring isomorphism $h\colon S^{-1}A \to B$ such that $h \circ f = g$, i.e., the following diagram commutes



Proof. Since (i) holds, we already have the existence and uniqueness of

$$h\colon S^{-1}A \to B, \quad a/s \mapsto g(a)g(s)^{-1}$$

by Proposition 3.4. Property (iii) implies that h is surjective, so it remains to show that h is injective. Let $a/s \in \ker h$. Then $h(a/s) = g(a)g(s)^{-1} = 0$, which implies $g(a) = 0$. Hence, by (ii) we have $at = 0$ for some $t \in S$. But this means $a/1 = 0$, whence $a/s = 0$. Finally, we have just shown that $\ker h = 0$, i.e., h is injective. □

3.1 Localization of a Module

Let A be a ring, let $S \subseteq A$ be a multiplicative set and let M be an A-module. We define on $M \times A$ the following equivalence relation:

$$(m, s) \sim (m', s') \quad \overset{\text{def}}{\iff} \quad \exists u \in S :\ u(s'm - sm') = 0.$$

As before, it is easy to check that this is a well-defined equivalence relation. We denote the equivalence class of a pair (m, s) by m/s. We also denote the set of equivalence classes $(M \times S)/\sim$ by $S^{-1}M$ and define on it the following operations:

$$\frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'},$$
$$\frac{a}{s} \cdot \frac{m}{t} := \frac{am}{st}.$$

It is easy to check that the operations above are well-defined and make $S^{-1}M$ into an $(S^{-1}A)$-module.

Definition 3.6. The $(S^{-1}A)$-module $S^{-1}M$ is called *the module of fractions of M with respect to S* (or *the localization of M along S*).

Example 3.7. Let M be an A-module and let $S \subseteq A$ be a multiplicative set.

(a) If $0 \in S$, then $S^{-1}M = \{0\}$.

(b) Let $\mathfrak{p}$ be a prime ideal in A and let $S = A \setminus \mathfrak{p}$. Then $S^{-1}M$ is called *the localization of M at $\mathfrak{p}$* and denoted by $M_{\mathfrak{p}}$.

(c) Let $f \in A$ and let $S = \{f^n\}_{n\in\mathbb{N}} = \{1, f, f^2, \dots\}$. Then $S^{-1}M$ is called *the localization of M at f* and denoted by M_f.

Definition 3.8. Let $u\colon M \to N$ be an A-module homomorphism and let $S \subseteq A$ be a multiplicative set. Then we have the induced $(S^{-1}A)$-linear map

$$S^{-1}u\colon S^{-1}M \longrightarrow S^{-1}N, \qquad m/s \longmapsto u(m)/s.$$

Remark 3.9. Let $u\colon M \to N$ and $v\colon N \to P$ be A-module homomorphisms and let $S \subseteq A$ be a multiplicative set. Then

$$S^{-1}(v \circ u) = S^{-1}v \circ S^{-1}u.$$

Proposition 3.10. *Let A be a ring and let $S \subseteq A$ be a multiplicative set. Furthermore, let $M_1 \xrightarrow{u} M_2 \xrightarrow{v} M_3$ be an exact sequence of A-modules. Then the sequence*

$$S^{-1}M_1 \xrightarrow{S^{-1}u} S^{-1}M_2 \xrightarrow{S^{-1}v} S^{-1}M_3$$

is also exact.

Proof. We have to show that $\operatorname{im} S^{-1}u = \ker S^{-1}v$.

$\subseteq$. By assumption we know that $\operatorname{im} u = \ker v$, whence $v \circ u = 0$. Thus, by Remark 3.9 we have that $S^{-1}v \circ S^{-1}u = S^{-1}(v \circ u) = S^{-1}(0) = 0$, which implies $\operatorname{im} S^{-1}u \subseteq \ker S^{-1}v$.

$\supseteq$. Let $m_2/s \in \ker S^{-1}v$. By definition, $v(m_2)/s = 0$, i.e., there exists $t \in S$ such that $tv(m_2) = v(tm_2) = 0$. Since $\ker v = \operatorname{im} u$, there exists $m_1 \in M_1$ such that $u(m_1) = tm_2$. Then $m_2/s = tm_2/st = u(m_1)/st = (S^{-1}u)(m_1/st)$. In other words, $m_2/s \in \operatorname{im} S^{-1}u$. □

As a result, formation of fraction preserves short exact sequences.

Corollary 3.11. *Let A be a ring and let $S \subseteq A$ be a multiplicative set. Let $0 \to M_1 \xrightarrow{u} M_2 \xrightarrow{v} M_3 \to 0$ be a short exact sequence of A-modules. Then the sequence*

$$0 \longrightarrow S^{-1}M_1 \xrightarrow{S^{-1}u} S^{-1}M_2 \xrightarrow{S^{-1}v} S^{-1}M_3 \longrightarrow 0$$

is also exact.

Proof. Split the sequence $0 \to M_1 \xrightarrow{u} M_2 \xrightarrow{v} M_3 \to 0$ into

$$0 \to M_1 \xrightarrow{u} M_2, \quad M_1 \xrightarrow{u} M_2 \xrightarrow{v} M_3, \quad M_2 \xrightarrow{v} M_3 \to 0$$

and apply Proposition 3.10 three times. □

3.1.1 Submodules and Canonical Isomorphisms

Let M be an A-module, let $N \subseteq M$ be a submodule and let $S \subseteq A$ be a multiplicative set. Proposition 3.10 implies in particular that $S^{-1}N$ can be regarded as a submodule of $S^{-1}M$. Hence, it makes sense to study the behavior of formation of fractions with respect to operations on submodules. Indeed, we show that formation of fractions commutes with sums, finite intersections and quotients.

Proposition 3.12. *Let A be a ring and let $S \subseteq A$ be a multiplicative set . Let M be an A-module, let $N, T \subseteq M$ be submodules and let $\{N_i\}_{i\in I}$ be a family of submodules. Then it holds*

(i) $S^{-1}(N \cap T) = S^{-1}N \cap S^{-1}T$.

(ii) $S^{-1}(\sum_{i\in I} N_i) = \sum_{i\in I} S^{-1}N_i$.

(iii) $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

Proof. (i) The inclusion $\subseteq$ is obvious. Let us show the inclusion $\supseteq$. Let $x \in S^{-1}N \cap S^{-1}T$. Then $x = n/s_1 = t/s_2$ with $n \in N$, $t \in T$ and $s_1, s_2 \in S$. By definition, there is $q \in S$ such that $q(s_1t - s_2n) = 0$. Then $y := qs_1t = qs_2n \in N \cap T$ and $x = n/s_1 = y/(s_1s_2q) \in S^{-1}(N \cap T)$.

(ii) $\subseteq$. Let $z = (x_{i_1} + \ldots + x_{i_k})/s \in S^{-1}(\sum_{i\in I} N_i)$. Then $z = x_{i_1}/s + \ldots + x_{i_k}/s \in \sum_{i\in I} S^{-1}N_i$.

$\supseteq$. Let $y = x_{i_1}/s_{i_1} + \ldots + x_{i_k}/s_{i_k} \in \sum_{i\in I} S^{-1}N_i$. Then for $1 \le j \le k$ set $\widehat{s}_{i_j} := \prod_{l\neq j} s_{i_l}$ and $s := \prod_{l=1}^{k} s_{i_l}$. Then

$$y = \frac{\widehat{s}_{i_1}x_{i_1} + \ldots + \widehat{s}_{i_k}}{x}_{i_k} \, s \in S^{-1}(\sum_{i\in I} N_i).$$

(iii) Applying Corollary 3.11 to the exact sequence $0 \to N \to M \to M/N \to 0$, we obtain the short exact sequence

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}(M/N) \longrightarrow 0.$$

Hence, $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

□

Remark 3.13. Note that formation of fraction does not commute with infinite intersections of submodules. Indeed, let $A := \mathbb{Z}$, let $S := \mathbb{Z} \setminus \{0\}$ and for $n \in \mathbb{N}_{>0}$ let $M_n := n\mathbb{Z}$. It is easy to see that $S^{-1}A = S^{-1}M_n = \mathbb{Q}$ for all $n \in \mathbb{N}_{>0}$, while $\bigcap_{n\in\mathbb{N}_{>0}} M_n = 0$. Thus, we have

$$S^{-1}\Big(\bigcap_{n\in\mathbb{N}_{>0}} M_n\Big) = S^{-1}0 = 0 \neq \mathbb{Q} = \bigcap_{n\in\mathbb{N}_{>0}} S^{-1}M_n.$$

Proposition 3.14. *Let M be an A-module and let $S \subseteq A$ be a multiplicative set. Then there exists a unique $(S^{-1}A)$-module homomorphism*

$$S^{-1}A \otimes_A M \to S^{-1}M$$

such that $a/s \otimes m \longmapsto am/s$.

Corollary 3.15. *Let A be a ring and let $\{M_i\}_{i\in I}$ be a family of modules. Then*

$$S^{-1}\Big(\bigoplus_{i\in I} M_i\Big) \cong \bigoplus_{i\in I} S^{-1}M_i.$$

Corollary 3.16. *Let A be a ring and let $S \subseteq A$ be a multiplicative set. Then $S^{-1}A$ is a flat A-module.*

Proposition 3.17. *Let A be a ring and let $S \subseteq A$ be a multiplicative set. Let M and N be two A-modules. Then there exists a unique $(S^{-1}A)$-module homomorphism*

$$S^{-1}(M \otimes_A N) \to S^{-1}M \otimes_{S^{-1}A} S^{-1}N$$

such that $m/s \otimes n/t \longmapsto (m \otimes n)/(st)$.

Corollary 3.18. *Let A be a ring, let $P \subseteq A$ be a prime ideal and let M and N be two A-modules. Then*

$$(M \otimes_A N)_P \cong M_P \otimes_{A_P} N_P.$$

3.2 Local Properties of Rings and Modules

Definition 3.19. A property Φ of a ring A (resp. of an A-module M) is called *local* if it holds

A (resp. M) fulfills $\Phi \iff A_P$ (resp. M_P) fulfills Φ for all $P \subseteq A$ prime ideals.

Proposition 3.20. *Let A be a ring and let M be an A-module. Then the following are equivalent:*

(i) $M = \{0\}$,

(ii) $M_P = \{0\}$ *for all prime ideals* $P \subseteq A$,

(iii) $M_{\mathfrak{m}} = \{0\}$ *for all maximal ideals* $\mathfrak{m} \subseteq A$.

Proof. The implications "(i) $\Rightarrow$ (ii)" and "(ii) $\Rightarrow$ (iii)" are obvious.

"(iii) $\Rightarrow$ (i)": Assume by contradiction that $M \neq \{0\}$. Let $x \in M$ be any element and consider the ideal

$$\mathrm{Ann}(x) := \{a \in A \mid ax = 0\}.$$

Now let $x \in M$ be a nonzero element. Hence, $\mathrm{Ann}(x)$ is a proper ideal of A, and thus there exists a maximal ideal $\mathfrak{m} \subseteq A$ such that $\mathrm{Ann}(x) \subseteq \mathfrak{m}$. Since (iii) holds, $M_{\mathfrak{m}} = \{0\}$ and so $x/1 = 0$ in $M_{\mathfrak{m}}$. Thus, there is $t \in A \setminus \mathfrak{m}$ such that $tx = 0$, a contradiction since $\mathrm{Ann}(x) \subseteq \mathfrak{m}$. □

Proposition 3.21. *Let* $\phi\colon M \to N$ *be an* A*-module homomorphism. Then the following are equivalent:*

(i) ϕ *is injective (respectively surjective),*

(ii) $\phi_P\colon M_P \to N_P$ *is injective for all prime ideals* $P \subseteq A$ *(respectively surjective),*

(iii) $\phi_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ *is injective for all maximal ideals* $\mathfrak{m} \subseteq A$ *(respectively surjective).*

Proposition 3.22 (Flatness is a Local Property)**.** *Let* A *be a ring and* M *be an* A*-module. The following are equivalent:*

(i) M *is a flat* A*-module,*

(ii) M_P *is a flat* A_P*-module for all prime ideals* $P \subseteq A$*,*

(iii) $M_{\mathfrak{m}}$ *is a flat* $A_{\mathfrak{m}}$*-module for all maximal ideals* $\mathfrak{m} \subseteq A$*.*

3.3 Ideals in Ring of Fractions

Definition 3.23. Let $f\colon A \to B$ be a ring homomorphism.

(a) Let J be an ideal of B. Then $J^c := f^{-1}(J)$ is an ideal of A called *the contraction of* J *via* f.

(b) Let I be an ideal of A. The set

$$f(I)B := \{\sum_{i=1}^{n} b_i f(a_i) \mid n \in \mathbb{N},\ a_i \in A,\ b_i \in B\}$$

is an ideal in B called *the extension of* I *via* f. This is the smallest ideal in B containing $f(I)$ and is denoted by I^e.

Remark 3.24. Let A be a ring, let $S \subseteq A$ be a multiplicative set and let $f\colon A \to S^{-1}A$ be the canonical map. Let I be an ideal in A.

(a) The extended ideal I^e coincides with the $(S^{-1}A)$-module $S^{-1}I$, i.e.,

$$I^e = S^{-1}I = \{a/s \mid a \in I,\ s \in S\}.$$

The inclusion $\supseteq$ is clear since $a/s = 1/s \cdot a/1 = 1/s \cdot f(a)$.

We show the inclusion $\subseteq$. Let $x \in I^e$. This means that there are $b_i \in A$, $s_i \in S$ and $a_i \in I$ such that

$$x = \frac{b_1}{s_1}\frac{a_1}{1} + \ldots + \frac{b_n}{s_n}\frac{a_n}{1}.$$

For $1 \leq i \leq n$ set $\widehat{s_i} := \prod_{j \neq i} s_j$ and $s := \prod_{j=1}^{n} s_j$. Then we have

$$x = \frac{\overbrace{\widehat{s_1} b_1 a_1}^{\in I} + \ldots + \overbrace{\widehat{s_n} b_n a_n}^{\in I}}{s} \in S^{-1}I.$$

(b) If $S = A \setminus \mathfrak{p}$ for some prime ideal $\mathfrak{p}$, then we denote the extended ideal I^e by $IA_{\mathfrak{p}}$.

(c) If $S = \{f^n\}_{n \in \mathbb{N}}$ for some element $f \in A$, then we denote the extended ideal I^e by IA_f.

Proposition 3.25. *Let A be a ring, let $S \subseteq A$ be a multiplicative set and let $f\colon A \to S^{-1}A$ be the natural map.*

(i) Every ideal in $S^{-1}A$ has the form $S^{-1}I$ for some ideal I in A.

(ii) There is a one-to-one inclusion-preserving correspondence between prime ideals in A which are disjoint from S and prime ideals in $S^{-1}A$.

(iii) Let $I, J \subseteq A$ be ideals. Let $\{I_\alpha\}_{\alpha \in \mathcal{A}}$ be a family of ideals of A. Then it holds

(a) $S^{-1}\Big(\sum_{\alpha \in \mathcal{A}} I_\alpha\Big) = \sum_{\alpha \in \mathcal{A}} S^{-1}I_\alpha$,

(b) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$,

(c) $S^{-1}(IJ) = S^{-1}I \cdot S^{-1}J$,

(d) $S^{-1}(\sqrt{I}) = \sqrt{S^{-1}I}$.

For short, the localization operation S^{-1} commutes with formation of sums, finite intersections, finite products and radicals.

Corollary 3.26. *Let A be a ring and let $S \subseteq A$ be a multiplicative set. Then it holds*

$$S^{-1}N_A = N_{S^{-1}A}.$$

Proof. Apply (iii)(d) of Proposition 3.25 to the ideal $\{0\}$. □

Corollary 3.27. *Let A be a ring and let $P \subseteq A$ be a prime ideal. Then there is a one-to-one inclusion-preserving correspondence between prime ideals of A_P and prime ideals in A contained in P.*

Proof. Apply (ii) of Proposition 3.25 with $S = A \setminus P$. □

Proposition 3.28. *Let A be a ring and let $S \subseteq A$ be a multiplicative set. Let M be a finitely generated A-module. Then*

$$S^{-1}(\operatorname{Ann} M) = \operatorname{Ann}(S^{-1}M).$$

Remark 3.29. Let A be a ring and let $P \subseteq Q$ be prime ideals of A. By Proposition 1.16 and Corollary 3.27 there is a one-to-one inclusion-preserving correspondence between the set

$$\{P' \subseteq A \text{ prime ideal} \mid P \subseteq P' \subseteq Q\}$$

and the set of prime ideals of

$$(A/P)_{Q/P} \cong A_Q/PA_Q,$$

where the ring isomorphism is given by

$$\frac{a + Q/P}{s + Q/P} \longmapsto \frac{a}{s} + PA_Q.$$

Chapter 4

Integral Dependence

Definition 4.1. Let A and B be rings such that A is a subring of B. Recall that this means $A \subseteq B$ and $1_B \in A$. In such a situation, $A \subseteq B$ is called a *ring extension*.

(a) A ring extension $A \subseteq B$ is called *finite* if B is a finitely generated A-module.

(b) A ring extension $A \subseteq B$ is called *of finite type* if B is a finitely generated A-algebra.

(c) Let $A \subseteq B$ be a ring extension. An element $b \in B$ is called *integral over* A if there exists a monic polynomial

$$f := x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$$

such that $f(b) = 0$.

Remark 4.2. Let $A \subseteq B$ be a ring extension and let $a \in A$. Then a is integral over A since $x - a \in A[x]$ vanishes at a.

Remark 4.3. Let $A \subseteq B$ be a ring extension and let $b_1, \ldots, b_n \in B$. Then we have the following tower of ring extensions

$$A \subseteq A[b_1, \ldots, b_n] \subseteq B,$$

where $A[b_1, \ldots, b_n]$ is the ring of polynomial expressions in $b_1, \ldots, b_n$ with coefficients in A, introduced in Definition 2.50(b).

Proposition 4.4. *Let $A \subseteq B$ be a ring extension and let $b \in B$. Then the following are equivalent:*

(i) b is integral over A,

(ii) $A \subseteq A[b]$ is a finite ring extension,

(iii) There exists a subring $C \subseteq B$ containing $A[b]$ and such that $A \subseteq C$ is a finite ring extension.

(iv) There exists a faithful $A[b]$-module M which is finitely generated as an A-module.

Corollary 4.5. *Let $A \subseteq B$ be a ring extension and let $b_1, \ldots, b_n$ be elements of B which are integral over A. Then the extension $A \subseteq A[b_1, \ldots, b_n]$ is finite.*

Corollary 4.6. *Let $A \subseteq B$ be a ring extension and let C be the set of all elements of B which are integral over A. Then C is a subring of B which contains A.*

Definition 4.7. Let $A \subseteq B$ be a ring extension. The ring C from Corollary 4.6 is called the *integral closure of A in B*.

(a) If $A = C$, then A is called *integrally closed in B*.

(b) If $B = C$, then B is called *integral over A* and the ring extension $A \subseteq B$ is called *integral*.

(c) If A is an integral domain and $B = Q(A)$, then C is called the *integral closure of A*. If $A = C$, then A is called an *integrally closed integral domain*.

Corollary 4.8. *Let $A \subseteq B$ be a ring extension. Then*

$$A \subseteq B \text{ is finite} \quad \Longleftrightarrow \quad A \subseteq B \text{ is integral and of finite type.}$$

Proposition 4.9 (Transitivity of Integrality)**.** *Let $A \subseteq B \subseteq C$ be a tower of ring extensions such that C is integral over B and B is integral over A. Then C is integral over A.*

Corollary 4.10. *Let $A \subseteq B \subseteq C$ be a tower of ring extensions. Then*

$$A \subseteq C \text{ integral} \quad \Longleftrightarrow \quad A \subseteq B \text{ and } B \subseteq C \text{ integral.}$$

Corollary 4.11. *Let $A \subseteq B$ be a ring extension and let C be the integral closure of A in B. Then C is integrally closed in B.*

4.1 Going-Up Theorem

Lemma 4.12. *Let $A \subseteq B$ be an integral ring extension.*

(i) Let Q be an ideal in B and $P := A \cap Q$. Then B/Q is integral over A/P.

(ii) If $S \subseteq A$ is a multiplicative set, then $S^{-1}B$ is integral over $S^{-1}A$.

Lemma 4.13. *Let $A \subseteq B$ be an integral ring extension, where A and B are integral domains. Then A is a field if and only if B is a field.*

Proposition 4.14. *Let $A \subseteq B$ be an integral ring extension. Let $Q \subseteq B$ be a prime ideal and set $P := Q \cap A$. Then P is maximal in A if and only if Q is maximal in B.*

Proposition 4.15 (Incomparability)**.** *Let $A \subseteq B$ be an integral ring extension. Let Q and Q' be prime ideals in B such that $Q \subseteq Q'$ and $Q \cap A = Q' \cap A$. Then $Q = Q'$.*

Theorem 4.16 (Lying-Over Theorem)**.** *Let $A \subseteq B$ be an integral ring extension. Let $P \subseteq A$ be a prime ideal. Then there exists a prime ideal $Q \subseteq B$ such that $Q \cap A = P$.*

Proof. Let $S := A \setminus P$ and denote $S^{-1}B$ by B_P. By Lemma 4.12(ii) B_P is integral over A_P, hence we have the following commutative diagram

$$\begin{array}{ccc} A & \hookrightarrow & B \\ {\scriptstyle \lambda_A}\downarrow & & \downarrow{\scriptstyle \lambda_B} \\ A_P & \hookrightarrow & B_P \end{array}$$

where λ_A and λ_B are the natural maps. Let $\mathfrak{n}$ be a maximal ideal in B_P and let $\mathfrak{m} := A_P \cap \mathfrak{n}$. By Proposition 4.14 $\mathfrak{m}$ is maximal in A_P and since A_P is local, it holds $\mathfrak{m} = PA_P$, hence $\lambda_A^{-1}(\mathfrak{m}) = P$. Set $Q := \lambda_B^{-1}(\mathfrak{n})$. Then Q is prime in B (because $\mathfrak{n}$ is prime) and since the diagram above commutes we have

$$Q \cap A = \lambda_B^{-1}(\mathfrak{n}) \cap A = \lambda_A^{-1}(\mathfrak{n} \cap A_P) = \lambda_A^{-1}(\mathfrak{m}) = P.$$

□

Theorem 4.17 (Going-Up Theorem)**.** *Let $A \subseteq B$ be an integral ring extension. Let $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n$ be a chain of prime ideals in A and let $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m$ (where $m < n$) be a chain of prime ideals in B such that $Q_i \cap A = P_i$ for $1 \leq i \leq m$. Then we can extend this sequence to a sequence $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m \subseteq Q_{m+1} \subseteq \cdots \subseteq Q_n$ of prime ideals in B such that $Q_i \cap A = P_i$ for $1 \leq i \leq n$.*

Proof. By induction it suffices to show the statement for $n = 2$, $m = 1$. We have the following commutative diagram

$$\begin{array}{ccc} A & \xhookrightarrow{\ i\ } & B \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle \pi_B} \\ A/P_1 & \xhookrightarrow[\ j\ ]{} & B/Q_1 \end{array}$$

where i is the inclusion giving the ring extension $A \subseteq B$, $j\colon A/P_1 \hookrightarrow B/Q_1$, $[a]_{P_1} \mapsto [a]_{Q_1}$, and π_A and π_B are the canonical projections. By Lemma 4.12 B/Q_1 is integral over A/P_1. By Proposition 1.16 $\widetilde{P}_2 = \pi_A(P_2)$ is a prime ideal in A/P_1.

Hence, by the lying-over theorem (Theorem 4.16) there is a prime ideal $\widetilde{Q}_2$ in B/Q_1 such that $\widetilde{Q}_2 \cap (A/P_1) = \widetilde{P}_2$. Set $Q_2 := \pi_B^{-1}(\widetilde{Q}_2)$. Thus, by Proposition 1.16 Q_2 is a prime ideal in B such that $Q_1 \subseteq Q_2$ and since the diagram above commutes we have

$$Q_2 \cap A = \pi_B^{-1}(\widetilde{Q}_2) \cap A = \pi_A^{-1}(\widetilde{Q}_2 \cap (A/P_1)) = \pi_A^{-1}(\widetilde{P}_2) = P_2.$$

□

4.2 Integral Closure

Proposition 4.18. *Let $A \subseteq B$ be a ring extension and let C be the integral closure of A in B. Let $S \subseteq A$ be a multiplicative set. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. By (ii) of Lemma 4.12 we know that $S^{-1}C$ is contained in the integral closure of $S^{-1}A$ in $S^{-1}B$. For the other inclusion, take $x/s \in S^{-1}B$ which is integral over $S^{-1}A$. Then we have

$$(x/s)^n + (a_{n-1}/s_{n-1})(x/s)^{n-1} + \cdots + (a_0/s_0) = 0,$$

where $a_i \in A$ and $s_i \in S$. Set $s' := s_{n-1} \cdots s_0$. By multiplying the equality above with $(s \cdot s')^n$, we obtain in $S^{-1}B$

$$(x \cdot s')^n + \sum_{i=1}^{n} a_{n-i}\ s^i s_{n-1}^i \cdots s_{n-i}^{i-1} \cdots s_0^i\ (x \cdot s')^{n-i} = 0$$

By definition of equivalence classes in $S^{-1}B$ there is $t \in S$ such that

$$t\Big((x \cdot s')^n + \sum_{i=1}^{n} a_{n-i}\ s^i s_{n-1}^i \cdots s_{n-i}^{i-1} \cdots s_0^i\ (x \cdot s')^{n-i}\Big) = 0$$

in B, thus multiplying with t^{n-1} we get in B

$$(x \cdot t \cdot s')^n + \sum_{i=1}^{n} b_{n-i}\ s^i s_{n-1}^i \cdots s_{n-i}^{i-1} \cdots s_0^i\ (x \cdot t \cdot s')^{n-i} = 0,$$

where $b_{n-i} = a_{n-i}t^i \in A$. Hence, $x \cdot t \cdot s'$ is integral over A and thus $x \cdot t \cdot s' \in C$. Finally,

$$\frac{x}{s} = \frac{x \cdot t \cdot s'}{s \cdot t \cdot s'} \in S^{-1}C.$$

□

For an integral domain being integrally closed is a local property.

Theorem 4.19 (Integral Closure is a Local Property)**.** *Let A be an integral domain. Then the following are equivalent:*

(i) A is integrally closed,

(ii) A_P is integrally closed for all $P \subseteq A$ prime ideals,

(iii) $A_{\mathfrak{m}}$ is integrally closed for all $\mathfrak{m} \subseteq A$ maximal ideals.

Proof. Let C be the integral closure of A in $Q(A)$ and let $f\colon A \to C$ be the inclusion map. Observe that f is an A-module homomorphism. We have

$$A \text{ integrally closed} \quad \iff \quad f \text{ is surjetive.}$$

Let P be a prime ideal in A and let $S := A \setminus P$. By Proposition 4.18 the integral closure of $S^{-1}A = A_P$ in $S^{-1}Q(A) \cong Q(A) \cong Q(A_P)$ is $S^{-1}C$. Hence,

$$A_P \text{ integrally closed} \quad \iff \quad f_P\colon A_P \to S^{-1}C \text{ is surjective.}$$

Now by Proposition 3.21 we have

$$\begin{aligned} f \text{ surjective} \quad &\iff \quad f_P \text{ surjective for all } P \subseteq A \text{ prime ideals} \\ &\iff \quad f_{\mathfrak{m}} \text{ surjective for all } \mathfrak{m} \subseteq A \text{ maximal ideals.} \end{aligned}$$

□

Example 4.20. Let k be a field. Then $k[x_1, \ldots, x_n]$ is an integrally closed integral domain.

Now we extend the notion of integrality by introducing integrality relative to an ideal.

Definition 4.21. Let $A \subseteq B$ a ring extension and let $I \subseteq A$ be an ideal. An element $b \in B$ is called *integral over I* if there exists a monic polynomial

$$f := x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$$

with $a_i \in I$ for all $i \in \{0, \ldots, n-1\}$ such that $f(b) = 0$. The *integral closure of I in B* is the set of all elements in B which are integral over I.

Remark 4.22. Let $A \subseteq B$ be a ring extension and let I be an ideal in A. Let C be the integral closure of A in B and let D be the integral closure of I in B. Any $a \in I$ is integral over I since $x - a \in A[x]$ vanishes at a and $a \in I$. Hence, $I \subseteq D$. Note that at this stage $D \subseteq C$ is just a subset of the ring C. Indeed, D is an ideal of C, as shown by the next lemma.

Lemma 4.23. *Let $A \subseteq B$ be a ring extension, let C be the integral closure of A in B and let $I \subseteq A$ be an ideal of A and let I^e denote the extension of I in C. Then the integral closure of I in B is $\sqrt{I^e}$. In particular, sums and products of elements of B which are integral over I are again integral over I.*

Proof. $\subseteq$. Let $b \in B$ be an element which is integral over I. In particular, b is integral over A, and thus $b \in C$. This means that there exist $n \in \mathbb{N}$ and $a_i \in I$ such that $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$. Since

$$b^n = -a_{n-1}b^{n-1} + \ldots - a_0 \in I \cdot C = I^e,$$

it holds $b \in \sqrt{I^e}$.

$\supseteq$. Let $b \in \sqrt{I^e}$. Then $b^n = \sum_{i=1}^{k} a_i c_i \in I^e = I \cdot C$ with $a_i \in I$ and $c_i \in C$. Now consider $M := A[c_1, \ldots, c_k]$. Since the elements c_i's are integral over A, the ring extension $A \subseteq M$ is finite by Corollary 4.5. Hence, $M = Am_1 + \ldots + Am_r$ for some $m_i \in M$. Set $x := b^n$ and observe that $x \cdot m_1, \ldots, x \cdot m_r \in IM$. Thus, similarly as in the proof of Proposition 4.4 (see (iv)⇒(i)), we obtain

$$f := x^r + \alpha_{r-1}x^{r-1} + \ldots + \alpha_0$$

with $\alpha_i \in I$ for $0 \leq i \leq r-1$ such that $f \cdot m = 0$ for all $m \in M$. Hence, in particular $f = f \cdot 1 = 0$ and we have

$$(b^n)^r + \alpha_{r-1}(b^n)^{r-1} + \ldots + \alpha_0 = 0,$$

which implies that b is integral over I. □

Remark 4.24. Let $A \subseteq B$ be a ring extension where A and B are integral domains. Then we have the following commutative diagram

$$\begin{array}{ccc} A & \xhookrightarrow{i} & B \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ Q(A) & \xhookrightarrow{j} & Q(B) \end{array}$$

where $i\colon A \to B$ is the inclusion giving the ring extension, $\alpha\colon A \to Q(A)$, $a \mapsto a/1$, $\beta\colon B \to Q(B)$, $b \mapsto b/1$ and $j\colon Q(A) \to Q(B)$, $a/s \mapsto a/s$.

Proposition 4.25. *Let $A \subseteq B$ be a ring extension where A and B are integral domains and A is integrally closed. Let I be an ideal of A and let $b \in B$ be integral over I. Then b is algebraic over $Q(A)$ and if its minimal polynomial (over $Q(A)$) is $t^n + a_{n-1}t^{n-1} + \ldots + a_0$, then $a_i \in \sqrt{I}$.*

Proof. The element b (regarded as an element of the field $Q(B)$, see Remark 4.24) is obviously algebraic over $Q(A)$. Let $\mu = t^n + \sum_{i=0}^{n-1} a_i t^i$ be the minimal polynomial of b over $Q(A)$ and let $L \supseteq Q(A)$ be a splitting field of μ over $Q(A)$. Then $\mu = (t - b_1) \cdots (t - b_n) \in L[t]$ and there is $1 \leq i \leq n$ such that $b = b_i$. Without loss of generality, we may assume $b = b_1$. If λ is the monic polynomial with coefficients in I such that $\lambda(b) = 0$, then $\mu \mid \lambda$, hence $\lambda(b_i) = 0$ for $1 \leq i \leq n$. Thus, $b_1, \ldots, b_n$ are elements of L which are integral over I. The coefficients a_i of μ are (up to a sign) elementary symmetric polynomials in $b_1, \ldots, b_n$. Hence, by Lemma 4.23 applied to the ring extension $A \subseteq L$ the a_i's are integral over I. Finally, since $a_i \in Q(A)$ for all i and A is integrally closed, by Lemma 4.23 applied to the ring extension $A \subseteq Q(A)$ we have $a_i \in \sqrt{I}$. □

Corollary 4.26. *Let $A \subseteq B$ be a ring extension where A and B are integral domains and A is integrally closed. Let $b \in B$ be integral over A. Then b is algebraic over $Q(A)$ and if its minimal polynomial (over $Q(A)$) is $t^n + a_{n-1}t^{n-1} + \ldots + a_0$, then $a_i \in A$.*

Proof. Take $I = A$ in Proposition 4.25. □

4.3 Going-Down Theorem

Proposition 4.27. *Let $f\colon A \to B$ be a ring homomorphism and $P \subseteq A$ be a prime ideal. Then there is a prime ideal $Q \subseteq B$ such that $P = f^{-1}(Q)$ if and only if $P = f^{-1}(f(P)B)$.*

Proof. The implication $\Rightarrow$ is easy. Let us show $\Leftarrow$. Let $S := f(A \setminus P) \subseteq B$. Then S is a multiplicative set in B and $S \cap f(P)B = \varnothing$ since by assumption $P = f^{-1}(f(P)B)$. Hence, $S^{-1}[f(P)B]$ is a proper ideal of $S^{-1}B$. Let $\mathfrak{m}$ be a maximal ideal of $S^{-1}B$ such that $\mathfrak{m} \supseteq S^{-1}[f(P)B]$ and set $Q := \pi^{-1}(\mathfrak{m})$, where $\pi\colon B \to S^{-1}B$ is the natural map. Hence, Q is a prime ideal of B such that $Q \supseteq f(P)B$ and $Q \cap S = \varnothing$. Since $Q \supseteq f(P)B$, we have $f^{-1}(Q) \supseteq P$. On the other hand, since $Q \cap S = \varnothing$ and $S = f(A \setminus P)$, it holds

$$\varnothing = f^{-1}(Q) \cap f^{-1}(f(A \setminus P)) \supseteq f^{-1}(Q) \cap (A \setminus P),$$

hence $f^{-1}(Q) \cap (A \setminus P) = \varnothing$, i.e., $f(Q) \subseteq P$. Finally, we have $f^{-1}(Q) = P$. □

Theorem 4.28 (Going-Down Theorem)**.** *Let $A \subseteq B$ be an integral ring extension, where A and B are integral domains and A is integrally closed. Let $P_1 \supseteq P_2 \supseteq \cdots \supseteq P_n$ be a chain of prime ideals in A and let $Q_1 \supseteq Q_2 \supseteq \cdots \supseteq Q_m$ (where $m < n$) be a chain of prime ideals in B such that $Q_i \cap A = P_i$ for $1 \leq i \leq m$. Then we can extend this sequence to a sequence $Q_1 \supseteq Q_2 \supseteq \cdots \supseteq Q_m \supseteq Q_{m+1} \supseteq \cdots \supseteq Q_n$ of prime ideals in B such that $Q_i \cap A = P_i$ for $1 \leq i \leq n$.*

Proof. As in the proof of the going-up theorem, we may assume $n = 2$, $m = 1$. We have the following commutative diagram

$$\begin{array}{ccc} A & \xhookrightarrow{\ i\ } & B \\ {\scriptstyle\lambda_A}\big\downarrow & \searrow^{f} & \big\downarrow{\scriptstyle\lambda_B} \\ A_{P_1} & \xhookrightarrow[\ j\ ]{} & B_{Q_1} \end{array} \tag{4.1}$$

where i is the inclusion giving the ring extension, the natural maps λ_A and λ_B are injective because A and B are integral domains and $j\colon A_{P_1} \to B_{Q_1}$, $a/s \mapsto a/s$, is a well-defined map since $A \setminus P_1 \subseteq B \setminus Q_1$ and it is injective since B is an integral domain. We set $f := j \circ \lambda_A = \lambda_B \circ i$.

We claim that there is a prime ideal $\widetilde{Q}_2 \subseteq B_{Q_1}$ such that $P_2 = f^{-1}(\widetilde{Q}_2)$. If we show this, the assertion of the theorem follows, since $Q_2 := \lambda_B^{-1}(\widetilde{Q}_2)$ fulfills $P_2 = Q_2 \cap A$ (because the diagram is commutative!) and $Q_2 \subseteq Q_1$ by Corollary 3.27.

By Proposition 4.27, it suffices to show that $P_2 = f^{-1}(f(P_2)B_{Q_1})$. Since f is injective, we have to show that $P_2 = A \cap P_2 B_{Q_1}$. Clearly, $P_2 \subseteq A \cap P_2 B_{Q_1}$. Let us show the inclusion $\supseteq$. Take $x \in A \cap P_2 B_{Q_1}$. Since $x \in P_2 B_{Q_1}$, then $x = y/s$ with $y \in P_2 B$ and $s \in B \setminus Q_1$. The element y is integral over P_2 by Lemma 4.23 applied to the integral extension $A \subseteq B$. Hence, by Proposition 4.25 the minimal polynomial of y over $Q(A)$ is of the form

$$t^n + \alpha_{n-1}t^{n-1} + \ldots + \alpha_0 \in Q(A)[t]$$

with $\alpha_i \in P_2$. Since in $Q(B)$ we have $s = yx^{-1}$ with $x^{-1} \in Q(A)$ (because $x \in A$), the minimal polynomial of s over $Q(A)$ is

$$t^n + \beta_{n-1}t^{n-1} + \ldots + \beta_1 t + \beta_0 \in Q(A)[t]$$

where $\beta_i = \alpha_i x^{-(n-i)}$ for $0 \leq i \leq n-1$. Since $s \in B$ is integral over A, then by Corollary 4.26 we have $\beta_{n-i} \in A$. Moreover, it holds

$$\beta_i x^{n-i} = \alpha_i \in P_2 \quad \text{for all } 0 \leq i \leq n-1.$$

If we assume by contradiction that $x \notin P_2$, then $\beta_i \in P_2$ for $0 \leq i \leq n-1$ since P_2 is prime. But then $s^n = -\beta_{n-1}s^{n-1} - \beta_{n-2}s^{n-2} - \ldots - \beta_0 \in P_2 B \subseteq P_1 B \subseteq Q_1$, thus $s \in Q_1$ since Q_1 is prime. This contradicts $s \in B \setminus Q_1$, and hence it must hold $x \in P_2$. Finally, we showed $P_2 = A \cap P_2 B_{Q_1}$. □

Remark 4.29 (Fake Proof of the Going-Down Theorem)**.** A natural (but wrong!) attempt of proving the going-down theorem might have been the following.

Consider diagram (4.1). Take the extension $P_2 A_{P_1}$ of P_2 via λ_A. Since $P_2 A_{P_1}$ is prime, by the lying-over theorem (Theorem 4.16) there exists a prime $\widetilde{Q}_2$ in B_{Q_1} such that $\widetilde{Q}_2 \cap A_{P_1} = P_2 A_{P_1}$. Set $Q_2 := \lambda_B^{-1}(\widetilde{Q}_2)$. By Corollary 3.27 Q_2 is a prime ideal such that $Q_2 \subseteq Q_1$. Moreover, since diagram (4.1) commutes we have

$$Q_2 \cap A = \lambda_B^{-1}(\widetilde{Q}_2) \cap A = \lambda_A^{-1}(\widetilde{Q}_2 \cap A_{P_1}) = \lambda_A^{-1}(P_2 A_{P_1}) = P_2.$$

Everything seems to be correct, but there is a subtle mistake. The problem is that we are not allowed to apply the lying-over theorem since we do not know if the ring extension $A_{P_1} \subseteq B_{Q_1}$ is integral! In fact, we localize A and B with respect two different multiplicative sets, namely $A \setminus P_1$ and $B \setminus Q_1$, respectively. Hence, we cannot apply Lemma 4.12(ii) to the ring extension $A_{P_1} \subseteq B_{Q_1}$.

Chapter 5

Noetherian Modules and Rings

We start with two easy, but important lemmata.

Lemma 5.1. *Let $(\Sigma, \leqslant)$ be a partially ordered set. The following are equivalent:*

(i) Σ *satisfies the* ascending chain condition (ACC)*, that is, if we have an ascending chain $x_1 \leqslant x_2 \leqslant \ldots$, then there exists $n \in \mathbb{N}$ such that $x_m = x_n$ for all $m \geq n$,*

(ii) Σ *satisfies the* maximal condition*, that is, every nonempty set in Σ has a maximal element.*

Lemma 5.2. *Let $(\Sigma, \leqslant)$ be a partially ordered set. The following are equivalent:*

(i) Σ *satisfies the* descending chain condition (DCC)*, that is, if we have a descending chain $x_1 \geqslant x_2 \geqslant \ldots$, then there exists $n \in \mathbb{N}$ such that $x_m = x_n$ for all $m \geq n$,*

(ii) Σ *satisfies the* minimal condition*, that is, every nonempty set in Σ has a minimal element.*

Example 5.3. (a) Let $\Sigma := \{1/n \mid n \in \mathbb{N}_{>0}\}$ and let $\leqslant$ be the usual $\leq$ between real numbers. Then $(\Sigma, \leqslant)$ satifies the ACC (or equivalently, the maximal condition).

(b) Let $\Sigma := \{1-1/n \mid n \in \mathbb{N}_{>0}\}$ and let $\leqslant$ be the usual $\leq$ between real numbers. Then $(\Sigma, \leqslant)$ satifies the DCC (or equivalently, the minimal condition).

Definition 5.4. Let A be a ring and let M be an A-module. Let Σ be the set of submodules of M ordered by inclusion.

(a) M is called *Noetherian* (after Emmy Noether) if Σ satisfies the ACC (or equivalenty, the maximal condition).

(b) M is called *Artinian* (after Emil Artin) if Σ satisfies the DCC (or equivalenty, the minimal condition).

Proposition 5.5. *Let M be an A-module. Then M is Noetherian if and only if every submodule of M is finitely generated.*

Proof. "$\Rightarrow$". Assume by contradiction there exists a submodule $N \subseteq M$ that is not finitely generated. Pick $n_1 \in N$, then $n_2 \in N \setminus An_1$ and so on. The sequence $An_1 \subsetneq An_1 + An_2 \subsetneq \dots$ is an ascending chain of submodules which does not stabilize, a contradiction since M is Noetherian.

"$\Leftarrow$". Let $N_1 \subseteq N_2 \subseteq \dots$ be an ascending chain of submodules of M. Since the submodule $\bigcup_{i=1}^{\infty} N_i$ is finitely generated, there are generators $n_1, \dots, n_k$. Thus, for $1 \leq i \leq k$ there is $j_i \in \mathbb{N}$ such that $n_i \in N_{j_i}$ and for $j := \max\{j_i \mid 1 \leq i \leq k\}$ it holds $n_1, \dots, n_k \in N_j$. Hence, $\bigcup_{i=1}^{\infty} = N_j$ and $N_m = N_j$ for all $m \geq j$. □

Proposition 5.6. *Let M_1, M_2, M_3 be A-modules and let*

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$$

be a short exact sequence. Then

(i) M_2 is Noetherian if and only if M_1 and M_3 are Noetherian.

(ii) M_2 is Artinian if and only if M_1 and M_3 are Artinian.

Proof. Both statements are proven in precisely the same way. We will just prove (i).

"$\Rightarrow$". Assume $N_1 \subseteq N_2 \subseteq \dots$ is an ascending chain of submodules in M_3. Then $\beta^{-1}(N_1) \subseteq \beta^{-1}(N_2) \subseteq \dots$ is an ascending chain of submodules in M_2, which is stationary since M_2 is Noetherian. Since β is surjective, for a subset $X \subseteq M_3$ it holds $\beta(\beta^{-1}(X)) = X$. Thus, the sequence $N_1 \subseteq N_2 \subseteq \dots$ must be stationary.

If $P_1 \subseteq P_2 \subseteq \dots$ is an ascending chain of submodules in M_1, then $\alpha(P_1) \subseteq \alpha(P_2) \subseteq \dots$ is a sequence of submodules in M_2 which stabilizes since M_2 is Noetherian. Since α is injective, for a subset $Y \subseteq M_1$ it holds $\alpha^{-1}(\alpha(Y)) = Y$. Thus, $P_1 \subseteq P_2 \subseteq \dots$ must stabilize.

"$\Leftarrow$". By Proposition 5.5 it is enough to show that any submodule of M_2 is finitely generated. Let $N_2 \subseteq M_2$ be a submodule. Define $N_1 := \alpha^{-1}(N_2)$ and $N_3 := \beta(N_2)$. Hence, the sequence

$$0 \longrightarrow N_1 \xrightarrow{\alpha_{|N_1}} N_2 \xrightarrow{\beta_{|N_2}} N_3 \longrightarrow 0$$

is exact by construction. The modules N_1 and N_3 are finitely generated by Proposition 5.5 since they are submodules of Noetherian modules. Hence, by Exercise 4(a) from Exercise Sheet 3 the module N_2 is finitely generated and so M_2 is Noetherian.

Alternatively, let $N_1 \subseteq N_2 \subseteq \dots$ be an ascending chain of submodules in M_2. Then $\alpha^{-1}(N_1) \subseteq \alpha^{-1}(N_2) \subseteq \dots$ is an ascending chain of submodules in M_1, which is stationary since M_1 is Noetherian. Hence, there exists $k_1 \in \mathbb{N}$ such

that $\alpha^{-1}(N_m) = \alpha^{-1}(N_{k_1})$ for all $m \geq k_1$. Moreover, $\beta(N_1) \subseteq \beta(N_2) \subseteq \dots$ is an ascending chain of submodules in M_3, which is stationary since M_3 is Noetherian. Hence, there exists $k_2 \in \mathbb{N}$ such that $\beta(N_m) = \beta(N_{k_2})$ for all $m \geq k_2$. Set $k := \max\{k_1, k_2\}$. Then for all $m \geq k$ it holds

$$\alpha^{-1}(N_m) = \alpha^{-1}(N_k) \quad \text{and} \quad \beta(N_m) = \beta(N_k).$$

Now we show that $N_m = N_k$ for all $m \geq k$. Since $N_k \subseteq N_m$ already holds, we need to show only $N_m \subseteq N_k$. Let $x \in N_m$. Then $\beta(x) \in \beta(N_m) = \beta(N_k)$, thus there exists $y \in N_k$ such that $\beta(x) = \beta(y)$. This implies that $x - y \in \ker \beta = \operatorname{im} \alpha$, hence there exists $z \in M_1$ such that $x - y = \alpha(z)$. Since $x, y \in N_m$, then $z \in \alpha^{-1}(N_m) = \alpha^{-1}(N_k)$, and thus $\alpha(z) \in N_k$. Finally, we have $x = y + \alpha(z) \in N_k$. □

Corollary 5.7. *Let A be a ring, let I be a finite index set and let $\{M_i\}_{i \in I}$ be family of Noetherian (respectively Artinian) A-modules. Then $\bigoplus_{i \in I} M_i$ is Noetherian (respectively Artinian) as well.*

Proof. By induction, it suffices to show the statement for $n = 2$. We have the short exact sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$. Now use Proposition 5.6. □

Definition 5.8. A ring A is called *Noetherian* (respectively *Artinian*) if it is Noetherian (respectively Artinian) as a module over itself.

Proposition 5.9. *Let A be a Noetherian (respectively Artinian) ring and M be a finitely generated A-module. Then M is Noetherian (respectively Artinian) as well.*

Proof. By Corollary 5.7, $A^n = \bigoplus_{i=1}^n A$ is Noetherian (respectively Artinian) for every $n \in \mathbb{N}$. By Proposition 2.21 every finitely generated A-module is a quotient of A^n for some $n \in \mathbb{N}$. Finally, use Proposition 5.6. □

Proposition 5.10. *Let A be a Noetherian (respectively Artinian) ring and let M and N be finitely generated A-modules. Then $\operatorname{Hom}_A(M, N)$ is a Noetherian (respectively Artinian) A-module.*

Proof. Both statements are proven in precisely the same way. We will just prove the Noetherian case. Since M is finitely generated, there is a surjective homomorphism $\varphi\colon A^n \twoheadrightarrow M$, i.e. $M \cong A^n / \ker \varphi$. Thus, we have an injective A-linear map (see Proposition 2.32(i)):

$$\overline{\varphi}\colon \operatorname{Hom}_A(M, N) \hookrightarrow \operatorname{Hom}_A(A^n, N), \quad \theta \longmapsto \theta \circ \varphi.$$

By Proposition 5.6, it suffices to show that $\operatorname{Hom}_A(A^n, N)$ is Noetherian. Observe that, if $e_1, \dots, e_n$ are the canonical generators of A^n, we have an A-module isomorphism

$$\operatorname{Hom}_A(A^n, N) \xrightarrow{\sim} N^n, \quad f \longmapsto (f(e_1), \dots, f(e_n)).$$

Now, since A is Noetherian and N is finitely generated, N is Noetherian by Proposition 5.9. Finally, by Corollary 5.7 N^n is Noetherian, and we are done. □

Corollary 5.11. *Let A be a Noetherian (respectively Artinian) ring and let M be a finitely generated A-module. Then the dual module $M^* := \mathrm{Hom}_A(M, A)$ is a Noetherian (respectively Artinian) A-module.*

Proof. Apply Proposition 5.10 with $N = A$. □

Let A be a Noetherian ring. By Hilbert's basis theorem (Theorem 1.34) the polynomial ring $A[X_1, \ldots, X_n]$ is also Noetherian. This is a way to construct new Noetherian rings from a given one. We now discuss some further constructions that produce new Noetherian (respectively Artinian) rings from existing ones.

Proposition 5.12. *Let A be a Noetherian (respectively Artinian) ring and let $I \subseteq A$ be an ideal. Then A/I is a Noetherian ring (respectively Artinian).*

Proof. Consider the short exact sequence of A-modules $0 \to I \to A \to A/I \to 0$. By Proposition 5.6 A/I is a Noetherian (respectively Artinian) A-module. Since the submodules of A/I as an A-module coincide with the ideals of A/I, we have that A/I is a Noetherian (respectively Artinian) ring. □

Corollary 5.13. *Let $\phi\colon A \to B$ be a surjective ring homomorphism. If A is a Noetherian (respectively Artinian) ring, then B is a Noetherian (respectively Artinian) ring as well.*

Proof. Observe that the ring B is isomorphic to $A/\ker\phi$. Apply now Proposition 5.12. □

Proposition 5.14. *Let A be a Noetherian (respectively Artinian) ring and let $S \subseteq A$ be a multiplicative set. Then $S^{-1}A$ is a Noetherian (respectively Artinian) ring.*

Proof. Both statements are proven in precisely the same way. We will just prove the Noetherian case. Let $f\colon A \to S^{-1}A$, $a \mapsto a/1$, and let $I_1 \subseteq I_2 \subseteq \ldots$ be an ascending chain of ideals in $S^{-1}A$. Then $f^{-1}(I_1) \subseteq f^{-1}(I_2) \subseteq \ldots$ is an ascending sequence of ideals in A which stabilizes beacause A is Noetherian. Since $S^{-1}(f^{-1}(I_j)) = I_j$ for all $j \in \mathbb{N}$, we have that $I_1 \subseteq I_2 \subseteq \ldots$ stabilizes as well. □

Corollary 5.15. *Let A be a Noetherian (respectively Artinian) ring.*

(i) Let $P \subseteq A$ be a prime ideal. Then A_P is a Noetherian (respectively Artinian) ring.

(ii) Let $f \in A$. Then A_f is a Noetherian (respectively Artinian) ring.