Algebra I*

Alexandru Constantinescu

20th November 2024

Freie Universität Berlin
Winter Semester 2024 - 2025

Contents

Bibliography

The bibliography is presented in the order that sources are mentioned in the lecture.

[Webseite] http://userpage.fu-berlin.de/aconstant/A1.html

[AM69] Michael Francis Atiyah, Ian Grang Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, **1969**

[Art91] Michael Artin, *Algebra*, Pearson, **1991**.

[Mun00] James Munkres, *Topology*, 2ed., (Mainly Chapter 2) Prenctice Hall, US, **2000**.

[Stacks] The Stacks Project Authors, *Stacks Project*, https://stacks.math.columbia.edu, **2019**.

[Eis95] David Eisenbud, *Commutative Algebra: with a View toward Algebraic Geometry*, Springer Science & Business Media, **1995**.

[Hul03] Klaus Hulek, *Elementary Algebraic Geometry*, American Mathematical Society, Student Mathematical Library, Vol. 20, **2003**.

[AK17] Allen Altman, Steven Kleiman, *A Term of Commutative Algebra*, Worldwide Center of Mathematics, https://www.mi.fu-berlin.de/en/math/groups/arithmetic_geometry/teaching/exercises/Altman_-Kleiman---A-term-of-commutative-algebra-_2017_.pdf.

Chapter 1

Rings

In linear algebra we work with vector spaces over fields. In commutative algebra fields are replaced by commutative rings with identity, and vector spaces by modules. The internal structure of a ring is more complicated than that of a field, and will plays a more important role than that of the field in linear algebra. Instead of looking at individual elements of the ring, we will often look at ideals, which were introduced as a generalization of the concept of number[1].

1.1   The basics

Definition 1.1. A **ring** is a triple $(R, +, \cdot)$ where R is a set, $+$ and $\cdot$ are two internal operations, called **addition** respectively **multiplication**, such that

(R1) $(R, +)$ is an Abelian group.

(R2) Multiplication is associative:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \quad \forall\, a, b, c \in R.$$

(R3) Multiplication is (left and right) distributive over addition, that is $\forall\, a, b, c \in R$ we have
$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

A ring is called **commutative** if the following axiom is satisfied.

(R4) $a \cdot b = b \cdot a, \quad \forall\, a, b \in R.$

A ring is said to have an **identity element** if

(R5) $\exists\, 1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

Usually rings are always assumed to have an identity. When they do not have an identity they called *pseudo-rings* or *rngs* (the i is missing on purpose). One problem which arises when rings have no 1, is: What should the empty product be equal to? Commutativity is "less common", and the terminology in this case is clearer: a ring is *commutative* on *noncommutative/ not commutative*.

Remark 1.2.   1. When it exists, the identity element is unique, called "**one**" and always be denoted by 1.

    2. We denote the neutral Element of the Abelian group $(R, +)$ by **0**, call it "**zero**", or "zero element".

---

[1]"Ideale Zahlen" - Ernst Eduard Kummer

3. For every $a \in R$, we denote the additive inverse of a by $-a$. So $a + (-a) = 0$.

4. For every $a \in R$ we have $a \cdot 0 = 0 \cdot a = 0$.

5. For every $a, b \in R$ we have $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$. Thus also $(-a) \cdot (-b) = a \cdot b$.

6. We do not exclude the case $1 = 0$. It follows from this, that the underlying set of the ring consists of only one element: $R = \{0\}$. We call the unique ring with $1 = 0$ the **zero ring**. We will abuse notation and write $R = 0$.

When convenient, we will ignore the "$\cdot$" sign for multiplication and just write ab for $a \cdot b$. If there is no ambiguity about what the operations of $(R, +, \cdot)$ are, we will simply write and say "R is a ring". Furthermore, for every $a \in R$ we will use the exponential notation as expected:

$$
\begin{aligned}
a^0 &:= 1 \\
a^n &:= \underbrace{a \cdot a \cdots \cdot a}_{n-\text{times}} , \quad \forall n \in \mathbb{N}_{>0}.
\end{aligned}
$$

In particular we have $a^n \cdot a^m = a^{n+m}$ for all $n, m \in \mathbb{N}$.

Examples.   1. $\mathbb{Z}$, the ring of integers.

2. $\mathbb{Z}/n\mathbb{Z}$, the ring of residue classes modulo n.

3. Any field, in particular $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_q$ for p prime and $q = p^n$ for some $n \in \mathbb{N}$, are rings.

4. For any field $\mathbb{K}$ the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$, and the ring of formal power series $\mathbb{K}[[x_1, \ldots, x_n]]$. The field $\mathbb{K}$ may be replaced by any commutative ring.

5. For any complex number $\alpha \in \mathbb{C}$: $\mathbb{Z}[\alpha] = \{f(\alpha) \ : \ f \in \mathbb{Z}[x]\}$ is the extension of $\mathbb{Z}$ by α. This is a subring of $\mathbb{C}$. Here are some important examples:

   - $\mathbb{Z}[i]$ the ring of Gaussian integers.
   - $\mathbb{Z}[\frac{1+\sqrt{19}}{2}]$ is a principal ideal domain that is not Euclidean.
   - $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ the ring of Eisenstein integers.

6. The ring of algebraic integers.

7. For every $(R, +)$ is an Abelian group, we can define the multiplication $\cdot : R \times R \longrightarrow R$ as $ab = 0$, for all $a, b \in R$. Then $(R, +, \cdot)$ is a ring. It is commutative, but, unless R is the trivial group, it has no identity element.

8. Let R be a ring and X an arbitrary set. On the set $\mathrm{Map}(X, R) := \{f : X \longrightarrow R \ : \ f \text{ is a set theoretic map}\}$ define *point-wise* addition and multiplication in the obvious way:

$$
\begin{aligned}
f + g : \quad X &\longrightarrow R \\
a &\longmapsto f(a) + g(a) \\
f \cdot g : \quad X &\longrightarrow R \\
a &\longmapsto f(a) \cdot g(a)
\end{aligned}
$$

   Then $(\mathrm{Map}(X, R), +, \cdot)$ is a ring. It is commutative if R is commutative, and has an identity element if R has one. Note that it will in general not be a field, even if R is a field.

9. If X is is a topological space, then $\mathcal{C}(X, \mathbb{R}) := \{f : X \longrightarrow \mathbb{R} \ : \ f \text{ is continuous}\}$, together with the operations from 8 is a commutative ring with identity.

10. If $X \subseteq \mathbb{C}$ is an open subset, then $\mathcal{O}(X) := \{f : X \longrightarrow \mathbb{C} \ : \ f \text{ is holomorphic}\}$, together with the operations from 8 is a commutative ring with identity.

11. Let G be an Abelian group, and $\mathrm{End}(G) := \{f : G \longrightarrow G \ : \ f \text{ is a group homomorphism}\}$. Then $\mathrm{End}(G)$ together with the addition defined as in 8 and with the composition of maps as a multiplication is a ring. It is in general not commutative. (Recall the ring of endomorphisms of vector spaces).

12. The set of square $n \times n$ matrices with entries in a field (or a commutative ring), together with matrix addition and multiplication is a ring. It is commutative if and only if $n = 1$.

13. Let $R_1, \dots, R_n$ be rings. The Cartesian product $R_1 \times \cdots \times R_n$, together with component-wise addition and multiplication is also a ring, called the **direct product** of the rings $R_1, \dots, R_n$.

14. The set 2^X of all subsets of a given set X, together with the symmetric difference as addition and intersection as multiplication is a ring.

15. For a monoid $(S, +)$ (like a group, but without asking for the existence of inverse elements. E.g. $\mathbb{N}$, $\mathbb{N}^n$) and a field $\mathbb{K}$ we define the monoidring $\mathbb{K}[S]$ in the following way: $(\mathbb{K}[S], +)$ is the $\mathbb{K}$-vector space with basis indexed by S. It is enough to define the multiplication on the elements of the basis as:

$$e_s \cdot e_{s'} := e_{s+s'}, \quad \forall \ s, s' \in S.$$

From now on all rings in this course are commutative, with 1.

Definition 1.3. Let R be a ring. A subset $S \subseteq R$ is a **subring** of R if the following two conditions hold.

(SR1) $(S, +)$ is a subgroup of $(R, +)$: $a - b \in S, \ \forall \ a, b \in S$.

(SR2) S is closed under multiplication: $ab \in S, \ \forall \ a, b \in S$.

(SR3) $1 \in S$.

1.1.1 Ring homomorphisms

As expected, a ring homomorphism is a map that respects the ring structure: addition, multiplication, and the identity element.

Definition 1.4. Let R and S be two rings. A map $f : R \longrightarrow S$ is a **ring homomorphism** if the following three axioms are satisfied.

(RHom1) $f(a + b) = f(a) + f(b), \quad \forall \ a, b \in R$ (i.e. f is a homomorphism of Abelian groups),

(RHom2) $f(ab) = f(a)f(b), \quad \forall \ a, b \in R$,

(RHom3) $f(1) = 1$.

Note that, contrary to the case of group homomorphisms, where $0 \mapsto 0$ follows from the compatibility with the group operation, in the case of rings we may have that (RHom1) and (RHom2) hold, but (RHom3) fails. (Exercise: find such an example.)

Remark 1.5. Let $f : R \longrightarrow S$ be a ring homomorphism.

1. $\mathrm{Im}(f) := \{b \in S \ : \ \exists a \in R \text{ such that } b = f(a)\} \subseteq S$ is a subring of S.

2. $\mathrm{Ker}(f) := \{a \in R \ : \ f(a) = 0\} \subseteq R$ is not a subring of R in general. (Exercise: Why?)

3. If f is bijective, then its inverse $f^{-1} : S \longrightarrow R$ is also a ring homomorphism. In this case, f is called a **ring isomorphism** and the rings R and S are said to be **isomorphic** if there exists an isomorphism between them.

4. If $f : R \longrightarrow S$ and $g : S \longrightarrow T$ are two ring homomorphisms, then their composition $g \circ f : R \longrightarrow T$ is also a ring homomorphism.

Examples.   1. For every ring R, there exists a unique ring homomorphism $f : \mathbb{Z} \longrightarrow R$. This means, that $\mathbb{Z}$ is an *initial object* in the category of rings.

2. There are no ring homomorphisms from the zero ring to a ring with $1 \neq 0$.

3. There is a unique homomorphism from any ring to the zero ring. This means that 0 is an *terminal object* in the category of rings.

4. If $S \subseteq R$ is a subring, the inclusion map $S \hookrightarrow R$ is a homomorphism of rings.

5. The canonical projection $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, sending $a \longmapsto [a]_n$, is a ring homomorphism.

6. Exercise: What are the ring homomorphisms $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}$.

7. Complex conjugation $\mathbb{C} \longrightarrow \mathbb{C}$, sending $z \mapsto \bar{z}$, is a ring homomorphism.

8. Let R be a ring, $a \in R$ an element, and $R[x]$ the polynomial ring in one variable with coefficients in R. The evaluation map $\mathrm{ev}_a : R[x] \longrightarrow R$, sending $p(x) \mapsto p(a)$, is a ring homomorphism. It is the only ring homomorphism from $R[x]$ to R which sends x to a.

1.1.2   Ideals

There are several reasons for introducing the following concept. One which we can see from the objects we introduced so far, is that kernels of ring homomorphisms are not subrings in general. They are important, and should play a role. A second reason will be that we cannot define a canonical ring structure on the quotient of R by a subring S. This quotient R/S is a group (because the additive groups are commutative, thus S is a normal subgroup of R), but the canonical multiplication is not well defined in general. Furthermore, ideals allow one to generalize the fundamental theorem of arithmetic (the one about unique factorization of integers).

Definition 1.6. Let R be a ring. An **ideal** of R is a subset $I \subseteq R$ satisfying the following two axioms.

(id1) I is a subgroup of $(R, +)$.

(id2) $\forall r \in R$ and $\forall a \in I$ we have $r \cdot a \in I$.

In axiom (id2) we may also simply write $R \cdot I \subseteq I$.

Remark 1.7.   1. If (id2) holds for I, we have by Remark 1.2 that $0 \in I$ and $a \in I \Rightarrow -a = (-1) \cdot a \in I$. So, to check that I is an ideal it is enough to check

   (id2) $\forall r \in R$ and $\forall a \in I$ we have $r \cdot a \in I$, and

   (id1') $a, b \in I \Rightarrow a + b \in I$.

2. $\{0\}$ and R are ideals for any ring R. An ideal I is called **proper ideal** if $I \neq R$.

3. $I = R \Leftrightarrow 1 \in I$.

4. For every ring homomorphism $f : R \longrightarrow S$, and any ideal $J \subseteq S$, the preimage

$$f^{-1}(J) := \{ r \in R \ : \ f(r) \in J \}$$

   is an ideal of R. In particular, the kernel of f is an ideal of R.

5. Exercise: If $f : R \longrightarrow S$ is a ring homomorphism, is the preimage $f^{-1}(1)$ of 1 an ideal? What is it?

6. If $I \subseteq R$ is an ideal an $f : R \longrightarrow S$ a homomorphism of rings, then $f(I)$ is in general not an ideal. For example $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is a ring homomorphism, but the image of $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. However, if f is surjective, then $\varphi(I)$ is an ideal.

7. If I and J are ideals of R, then $I \cap J$ and $I + J = \{a + b \; : \; a \in I \text{ and } b \in J\}$ are also ideals.

8. If $(I_i)_{i \in \mathcal{I}}$ is a family of ideals, it is an easy direct check that the intersection of all of them is also an ideal.

9. For every $a \in R$, the set

$$
\begin{aligned}
(a) \;\; &:= \;\; \{r \cdot a \; : \; r \in R\} \\
&:= \;\; R \cdot a,
\end{aligned}
$$

is an ideal of R. It is called the **principal ideal** generated by a, and it is the smallest (under inclusion) ideal of R containing a. An ideal I is called *principal* if <u>there exists</u> an $a \in R$ such that $I = (a)$. We abuse notation even more, and denote the ideal (0) also by 0. (So 0 may mean an element, an ideal, or a ring!)

10. The ideal **generated by** $a_1, \ldots, a_n \in R$ the ideal

$$
(a_1, \ldots, a_n) := (a_1) + \cdots + (a_n).
$$

It is the smallest ideal of R which contains $a_1, \ldots, a_n$.

11. For a random (i.e. not necessarily finite) subset $A \subseteq R$, we define the ideal **generated by** A as the smallest ideal containing A:

$$
(A) := \bigcap_{J \supseteq A} J, \quad \text{where all the } J \text{ are ideals.}
$$

It is an easy check, that $(A) = \left\{ \sum_{a \in A} r_a \cdot a \; : \; r_a \in R \text{ and only finitely many } r_a \text{ are not zero} \right\}$. That is, the ideal generated by A consists of all finite linear combinations of elements of A with coefficients in R.

Note that, and ideal may not seem principal at first sight:

$$
I = (4, 6) \subseteq \mathbb{Z}
$$

is given by two generators, but as $2 = (-1) \cdot 4 + 1 \cdot 6$, we have $(2) = (4, 6)$, so the ideal is principal. Note also, that the set of generators $4, 6$ is *inclusion minimal*, but not of minimal cardinality among all sets of generators of I.

12. Let R be a ring and X a set. Consider the ring $\mathrm{Map}(X, R)$ introduced on page 6 and a subset $Y \subseteq X$. Then

$$
I_Y := \{f : X \longrightarrow R \; : \; f(y) = 0, \; \forall \, y \in Y\}
$$

is an ideal of $\mathrm{Map}(X, R)$.

1.1.3 Quotient rings

Let R be a ring and $I \subseteq R$ an ideal. As I is a subgroup of R, we have the equivalence relation on R given by

$$
r \sim_I s \Leftrightarrow r - s \in I.
$$

The group $(R, +)$ is Abelian, so I is a normal subgroup of $(R, +)$ and thus R/I has a structure of Abelian group as well. For every $r \in R$ we denote the equivalence class of r by $[r]$ or by $r + I$. This is because

$$
[r] = r + I = \{r + a \; : \; a \in I\}.
$$

Remark 1.8. For every ring R and every ideal I the following is a well-defined multiplication, which is associative and distributive over the addition of R/I.

$$\cdot: \begin{array}{rcl} R/I \times R/I & \longrightarrow & R/I \\ ([r],[s]) & \longmapsto & [rs] \end{array}$$

Thus, R/I with the above multiplication is a ring.

Proof. Well-defined: Let $r, r', s, s' \in R$ with $[r] = [r']$ and $[s] = [s']$. This means, there exist $a, b \in I$, such that

$$r' = r + a \qquad \text{and} \qquad s' = s + b.$$

We thus have

$$r's' - rs = (r+a)(s+b) - rs = rs + rb + as + ab - rs = rb + as + ab \in I,$$

because $a, b \in I$ and I is an ideal.

Associativity and distributivity: The map $\pi : R \longrightarrow R/I$ is a surjective group homomorphism satisfying

$$\pi(a \cdot b) = [a \cdot b] = [a] \cdot [b] = \pi(a) \cdot \pi(b).$$

So associativity and distributivity follow. $\qquad\square$

Definition 1.9. Let R be a ring and I and ideal. The ring R/I described in Remark 1.8 is called the **quotient ring** (or **residue-class ring**, or **factor ring**) of R modulo I.

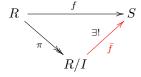The map $\pi : R \longrightarrow R/I$ sending $a \mapsto [a]$ is a ring homomorphism.

Lemma 1.10. *Let R be a ring and I and ideal. There is an inclusion-preserving bijection between the sets*

$$\{\textit{Ideals of } R \textit{ containing } I\} \leftrightarrow \{ \textit{ Ideals of } R/I \},$$

which is given by the association $J \longmapsto \pi(J)$.

Proof. Exercise. $\qquad\square$

Theorem 1.11. *Let R be a ring, $I \subseteq R$ an ideal and $\pi : R \longrightarrow R/I$ the canonical surjection. For every ring S and every ring homomorphism $f : R \longrightarrow S$ with the property that $I \subseteq \mathrm{Ker}(f)$, there exists a unique homomorphism $\bar{f} : R/I \longrightarrow S$, such that $f = \bar{f} \circ \pi$. That is we have the following commutative diagram*

$$
\begin{array}{ccc}
R & \xrightarrow{\ \ f\ \ } & S \\
& {\scriptstyle \pi}\searrow & {\scriptstyle \exists!}\ \nearrow {\scriptstyle \bar{f}} \\
& R/I &
\end{array}
$$

Furthermore,

1. $\bar{f}$ *is injective* $\Leftrightarrow \mathrm{Ker}\, f = I$.

2. $\bar{f}$ *is surjective* $\Leftrightarrow f$ *is surjective.*

Proof. Exercise. $\qquad\square$

Corollary 1.12 (The first isomorphism theorem for rings)**.** *If $f : R \longrightarrow S$ is a ring homomorphism, then there exists a unique ring isomorphism $\bar{f} : R/\mathrm{Ker}(f) \overset{\sim}{\longrightarrow} \mathrm{Im}(f)$ such that the following diagram commutes.*

$$
\begin{array}{ccc}
R & \xrightarrow{\ \ f\ \ } & \mathrm{Im}(f) \\
& {\scriptstyle \pi}\searrow & {\scriptstyle \exists!}\ \nearrow {\scriptstyle \bar{f}} \\
& R/\mathrm{Ker}(f) &
\end{array}
$$

1.1.4 Zero-divisors, nilpotents, units

Definition 1.13. Let R be a ring

1. A **zero divisor** is an element $a \in R$ for which there exists an element $b \in R \setminus \{0\}$ such that $a \cdot b = 0$.
   An **integral domain** is a ring $R \neq 0$, which has no zero divisors other than the element 0.

2. An element $a \in R$ is **nilpotent** if there exists some $n \in \mathbb{N}_{>0}$ such that $a^n = 0$.
   We say that R is a **reduced ring** if $R \neq 0$, and R has no nilpotents other than 0.

3. A **unit** of R is an element $a \in R$ which has a multiplicative inverse: $b \in R$ such that $ab = 1$.
   A **field** is a ring with $1 \neq 0$ in which every non-zero element is a unit.

Just as zero divisors "divide 0", units "divide 1".

Examples.   1. $\mathbb{Z}$ is an integral domain.

2. Every field is an integral domain, but not conversely.

3. $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain, if n is not prime.

4. [6] is nilpotent in $\mathbb{Z}/24\mathbb{Z}$.

5. [3] is a zero divisor in $\mathbb{Z}/24\mathbb{Z}$, but it is not nilpotent.

6. $x - 2$ is a zero divisor in $\mathbb{R}[x]/(x^2 - x - 2)$, but it is not nilpotent.

7. Every nilpotent element is a zero divisor.

Remark 1.14.   1. If $a \in R$ is a unit, its multiplicative inverse is uniquely determined and is denoted by a^{-1}.

2. $R^\times = \{a \in R \ : \ a \text{ is a unit}\}$ is a multiplicative group.

3. $a \in R$ is a unit $\Leftrightarrow (a) = R = (1)$.

Proposition 1.15. *For a ring $R \neq 0$ the following are equivalent.*

(a) *R is a field.*

(b) *The only ideals of R are (0) and (1).*

(c) *Every homomorphism into a non-zero ring S is injective.*

Proof. (a)$\Rightarrow$(b) Let $0 \neq I \subseteq R$ be an ideal. Then there exists $0 \neq a \in I$, so a is a unit. Thus $a^{-1} \cdot a = 1 \in I$, so $I = R$.
(b)$\Rightarrow$(c) If $f : R \longrightarrow S$ is a ring homomorphism, then $\mathrm{Ker}(f) \subseteq R$ is an ideal. Because $f(1) = 1 \neq 0$, we have $\mathrm{Ker}(f) \neq R$, so we must have $\mathrm{Ker} f = 0$, thus f is injective.
(c)$\Rightarrow$(a) Let $a \in R$ be an element which is not a unit. Then $1 \notin (a)$, so $(a) \neq R$, and the quotient ring $R/(a)$ is not the zero ring. The canonical projection $\pi : R \longrightarrow R/(a)$ is injective by (c), so $\mathrm{Ker} \pi = (a) = 0$, and thus $a = 0$. $\qquad\square$

1.1.5 Prime and Maximal Ideals

Definition 1.16. Let R be a ring.

1. An ideal $\mathfrak{p} \subsetneq R$ is a **prime ideal** if $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

2. An ideal $\mathfrak{m} \subsetneq R$ is a **maximal ideal** if there exists no ideal I of R such that $\mathfrak{m} \subsetneq I \subsetneq R$.

Remark 1.17. 1. An ideal $\mathfrak{p} \subset R$ is prime $\Leftrightarrow R/\mathfrak{p}$ is an integral domain.

2. An ideal $\mathfrak{m} \subset R$ is maximal $\Leftrightarrow R/\mathfrak{m}$ is a field.

3. In particular, every maximal ideal is prime, but in general not the other way around.

4. The ideal (0) is prime $\Leftrightarrow R$ is an integral domain.

Remark 1.18. Let $f : R \longrightarrow S$ be a ring homomorphism and $\mathfrak{q} \subseteq S$ an ideal. We have that $R/f^{-1}(\mathfrak{q})$ is isomorphic to a subring of $S/\mathfrak{q}$. This implies:

1. If $\mathfrak{q}$ is prime, then $f^{-1}(\mathfrak{q})$ is also a prime ideal of R.

2. If $\mathfrak{q}$ is maximal, it does not necessarily mean that $f^{-1}(\mathfrak{q})$ is maximal. (Example $\mathbb{Z} \hookrightarrow \mathbb{Q}, \mathfrak{q} = 0$).

Theorem 1.19. *Every nonzero ring contains a maximal ideal.*

This theorem is actually equivalent to the axiom of choice, but we prove here only that it is implied by Zorn's Lemma, which is equivalent to the axiom of choice. Recall that a partial order on a set P is a binary relation $\leq$ which is reflexive, antisymmetric and transitive. A *chain* in $(P, \leq)$ is a totally ordered subset C, that is, for every $x, y \in C$ we have $x \leq y$ or $y \leq x$. A subset $C \subseteq P$ has an upper bound in P, if there is an element $b \in P$ such that $x \leq b$ for all $x \in C$. A maximal element of P is an element $m \in P$ such that $m \leq m'$ implies $m = m'$. This is not to be confused with a maximum/supremum/upper bound.

Lemma 1.20 (Zorn). *Let $(P, \leq)$ be a nonempty partially ordered set. If every chain C of P has an upper bound in P, then P has at least one maximal element.*

Proof. Let $P = \{I \subsetneq R \mid I \text{ is an ideal}\}$ ordered by inclusion. Since $0 \in P$, it is nonempty. We want to show, that every chain in P has an upper bound in P. Let $C = (I_\alpha)_{\alpha \in X}$, where X is some index set, be a chain in P. So for every $I_\alpha, I_\beta \in C$, we either have $I_\alpha \subseteq I_\beta$ or $I_\beta \subseteq I_\alpha$. Define

$$I_C := \bigcup_\alpha I_\alpha.$$

I_C *is an ideal:* Let $a, b \in I_C$. Then, there exist $\alpha, \beta \in X$ such that $a \in I_\alpha$ and $b \in I_\beta$. By the chain condition, we may assume that $I_\alpha \subseteq I_\beta$. Thus $a + b \in I_\beta \subseteq I_C$. The second axiom follows even quicker.
We have $1 \notin I_C$, because $1 \notin I_\alpha$ for all $\alpha \in X$. Hence I_C is an upper bound in P for C, and we conclude by Zorn's Lemma. $\square$

Every nonzero ring contains a prime is weaker than the axiom of choice. But this goes beyond the scope of this course.

Corollary 1.21. *Every proper ideal is contained in a maximal one.*

Proof. Let $I \subset R$ be a proper ideal. Apply Theorem 1.19 and then Lemma 1.10. $\square$

Corollary 1.22. *Every non unit is contained in a maximal ideal.*

1.1.6 Local Rings

Definition 1.23. A **local ring** is a ring R with exactly one maximal ideal $\mathfrak{m}$. The field $R/\mathfrak{m}$ is called the **residue field** of R.

Local rings are usually denote as a pair $(R, \mathfrak{m})$, where $\mathfrak{m}$ is the unique maximal ideal. A **semi-local ring** is a ring with only finitely many maximal ideals.

Proposition 1.24. *Let R be an ideal and $\mathfrak{m} \subsetneq R$ be a proper ideal.*

(a) *If all elements in $R \setminus \mathfrak{m}$ are units, then R is a local ring and $\mathfrak{m}$ its maximal ideal.*

(b) *If $\mathfrak{m}$ is maximal, and every element of $1 + \mathfrak{m} := \{1 + a \ : \ a \in \mathfrak{m}\}$ is a unit, then R is local.*

Proof.   1. If $I \subsetneq R$ is an ideal, then $\forall \, a \in I$, a is not a unit, thus $a \in \mathfrak{m}$. So $I \subseteq \mathfrak{m}$ for every proper ideal of R.

2. Let $a \in R \setminus \mathfrak{m}$, and consider the ideal $\mathfrak{m} + (a) \supsetneq \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, we have $\mathfrak{m} + (a) = R = (1)$. So there exists $r \in R$ and $m \in \mathfrak{m}$ such that $ra + m = 1$. So $ra = 1 - m \in 1 + \mathfrak{m}$, thus ra is a unit, and so must be a. We can now apply (a) to conclude.

$\square$

Remark 1.25.

Examples.   1. If $\mathbb{K}$ is a field, the formal power series ring

$$\mathbb{K}[[x_1, \ldots, x_n]] = \{\sum_{\mathbf{a} \in \mathbb{N}^a} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}} \mid c_{\mathbf{a}} \in \mathbb{K}\}$$

is a local ring with maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n)$. The residue field is $\mathbb{K}$. So is every quotient of $\mathbb{K}[[x_1, \ldots, x_n]]$.

2. A principal ideal domain, is an integral domain in which every ideal is principal. Every prime is maximal, and of the form (p) with p a prime element. We consider the second part as known (it's easy anyway). To see that (p) is maximal when p is prime, assume $(p) \subsetneq (q)$. This means $p = qa$ for some $a \in R$. So $qa = p \in (p)$, thus $q \in (p)$ or $a \in (p)$. The first $(q \in (p))$ contradicts $(p) \subsetneq (q)$, so $a \in (p)$. That is, there exists $b \in R$ such that $a = pb$. So $p = qa = qpb$, thus $p(1 - qb) = 0$. But R is a domain, so one of the factors must be zero. Then, since $p \neq 0$, we get $qb = 1$, so $(q) = (1) = R$, and thus (p) is maximal.

3. In particular, in $\mathbb{Z}$, we have $\mathbb{Z}/(p) =: \mathbb{F}_p$ is the field with p elements. The ring $\mathbb{K}[x]$ is also a PID, for every field. In a PID, every irreducible is prime, so to get a finite field extension of $\mathbb{F}_p$, we choose an irreducible polynomial $f \in \mathbb{F}_p[x]$. Then the ideal (f) is maximal, and $\mathbb{F}_p[x]/(f)$ is a field with $p^{\deg(f)}$ elements. Explicitly, $f = x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, and we get $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$.

4. For every $\mathbf{a} \in \mathbb{K}^n$ the map $\mathrm{ev}_{\mathbf{a}} : \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}$, given by $\mathrm{ev}_{\mathbf{a}}(f) := f(\mathbf{a})$ is a ring homomorphism. Its Kernel is always a maximal ideal: $(x_1 - a_1, \ldots, x_n - a_n)$. In particular, when $\mathbf{a} = (0, \ldots, 0)$, then we get the set of ideals with no constant term.

5. Boolean rings have all prime ideals maximal (exercise).

6. Germs of holomorphic functions and the power series ring.

1.1.7 Nilradical and Jacobson Radical

Definition 1.26. A ring is called **reduced** if it has no nilpotent elements other than zero.

Proposition 1.27. *The set $\mathcal{N}_R$ of all nilpotent elements of a ring R is an ideal, and the quotient $R/\mathcal{N}_R$ is reduced.*

Proof. Let $a \in \mathcal{N}_R$, that is $\exists n \in \mathbb{N}$ such that $a^n = 0$. Clearly, for any $r \in R$ we have $(ra)^n = 0$, so $ra \in \mathcal{N}_R$. Let $b \in \mathcal{N}_R$ with $b^m = 0$ for some $m \in \mathbb{N}$. We want to show that $a + b \in \mathcal{N}_R$. We have that

$$(a+b)^{n+m+1} = \sum_{i=0}^{n+m+1} B_i \cdot a^i \cdot b^{n+m+1-i},$$

where B_i is the corresponding binomial coefficient, i.e. the image of $\binom{n+m+1}{i}$ under the unique homomorphism from $\mathbb{Z}$ to R. So, if $i < n$, then $n + m + 1 - i \geq m$ and $b^{n+m+1-i} = 0$, and if $i \geq n$, then $a^n = 0$. In any case, all the summands are zero, and thus $a + b \in \mathcal{N}_R$.

Let $[a] \in R/\mathcal{N}_R$ be a nilpotent element. Then $[a]^n = [a^n] = 0$, which means that $a^n \in \mathcal{N}_R$. So there exists $m \in \mathbb{N}$ such that $(a^n)^m = a^{n \cdot m} = 0$, thus $a \in \mathcal{N}_R$, so $[a] = 0$. $\qquad \square$

Definition 1.28. The ideal $\mathcal{N}_R = \{a \in R \; : \; a \text{ is nilpotent}\}$ is called the **nilradical** of R.

In Section 1.2 we define the radical of an ideal, and with that in mind we have $\mathcal{N}_R = \sqrt{(0)}$.

Proposition 1.29. *The nilradical $\mathcal{N}_R$ of R is the intersection of all prime ideals of R.*

Proof. Denote by $\mathcal{P}$ the intersection of all prime ideals in R.

$\boxed{\mathcal{N}_R \subseteq \mathcal{P}}$ For every $a \in \mathcal{N}_R$ we have $a^n = 0 \in \mathfrak{p}$ for every prime ideal $\mathfrak{p}$, so $a \in \mathfrak{p}$ for all primes.

$\boxed{\mathcal{P} \subseteq \mathcal{N}_R}$ We show that if $f \notin \mathcal{N}_R$, then $f \notin \mathcal{P}$. So, by assumption, we have $f^n \neq 0$ for all $n \in \mathbb{N}_{>0}$. We consider the set of ideals

$$\Sigma := \{I \subseteq R \; : \; f^n \notin I, \; \forall n \in \mathbb{N}_{>0}\}.$$

We have $\Sigma \neq \emptyset$, because $(0) \in \Sigma$. As in the proof of Theorem 1.19 we apply Zorn's Lemma (Lemma 1.20) to Σ and obtain that it has a maximal element: call it $\mathfrak{p}$. We now show that $\mathfrak{p}$ is a prime ideal, by showing that if $a, b \notin \mathfrak{p}$, then $ab \notin \mathfrak{p}$. So, let $a, b \notin \mathfrak{p}$. This means that $\mathfrak{p} \subsetneq \mathfrak{p} + (a)$ and $\mathfrak{p} \subsetneq \mathfrak{p} + (b)$, so, by the maximality of $\mathfrak{p}$, none of the two is in Σ. This means, there exist $n, m \in \mathbb{N}_{>0}$ such that

$$f^n \in \mathfrak{p} + (a) \quad \text{and} \quad f^m \in \mathfrak{p} + (b).$$

So, there exist $p_1, p_2 \in \mathfrak{p}$ and $r, s \in R$ such that $f^n = p_1 + ra$ and $f^m = p_2 + sb$. This implies

$$f^{n+m} = f^n \cdot f^m = p_1 p_2 + p_1 sb + p_2 ra + rsab \in \mathfrak{p} + (ab),$$

and thus the ideal $\mathfrak{p} + (ab) \notin \Sigma$. This can only happen if $ab \notin \mathfrak{p}$, and we conclude. $\qquad \square$

Definition 1.30. The **Jacobson radical** of a ring is the intersection of all its maximal ideals:

$$\mathcal{J}_R := \bigcap_{\mathfrak{m} \subseteq_{max} R} \mathfrak{m}.$$

Clearly $\mathcal{J}_R$ is an ideal. It is described by the following proposition.

Proposition 1.31. *Let $\mathcal{J}_R$ denote the Jacobson radical of the ring R. We have*

$$\mathcal{J}_R = \{a \in R \mid 1 - ar \text{ is a unit for all } r \in R\}.$$

Proof. $\boxed{\subseteq}$ Let $a \in \mathcal{J}_R$ and $y \in R$. Assume that $1 - ab$ is not a unit. Then, by Corollary 1.22, it is contained in some maximal ideal $\mathfrak{m}$. But $a \in \mathfrak{m}$ as well, which implies $1 \in \mathfrak{m}$. — a contradiction.

$\boxed{\supseteq}$ Assume that a belongs to the right hand side, but that there is some maximal ideal $\mathfrak{m}$ with $a \notin \mathfrak{m}$. This means $\mathfrak{m} \subsetneq \mathfrak{m} + (a)$, and by maximality we get

$$\mathfrak{m} + (a) = (1).$$

So there exists an $b \in \mathfrak{m}$ and $r \in R$ such that $b + ra = 1$. Thus $\mathfrak{m} \ni b = 1 - ra$ which is a unit. — a contradiction. $\qquad\square$

1.2 Operations on ideals

Throughout this section, let R be a ring, I, J ideals of R, and $(I_i)_{i \in \mathcal{I}}$ a family of ideals of R.

We saw in Section 1.1.2 that, $I \cap J$, $\cap_{i \in \mathcal{I}} I_i$ and $I + J = \{a + b \; : \; a \in I \text{ and } b \in J\}$ are ideals of R as well. We are going to extend the sum to arbitrary families, and define further operations on ideals now.

Definition 1.32. (a) The **sum** of the (possibly infinite) family $(I_i)_{i \in \mathcal{I}}$ is the smallest ideal containing all of them:
$$\sum_{i \in \mathcal{I}} I_i := \bigcap_{J \supseteq \bigcup_i I_i} J = \{\textstyle\sum a_i \; : \; \text{all finite sums with } a_i \in I_i\}.$$

(b) The **product** of the *finite* family of (not necessary different) ideals $(I_i)_{i=1,\ldots,n}$ is the ideal *generated* by all the products of n elements, one from each ideal:
$$I_1 \cdot \ldots \cdot I_n := (a_1 \cdots a_n \; : \; a_i \in I_i \text{ for all } i).$$

(c) For every $n \in \mathbb{N}$, the **powers** of I are defined as:
$$I^n := \begin{cases} (1) & \text{if } n = 0 \\ (a_1 \cdots a_n \; : \; a_i \in I \text{ for all } i) & \text{if } n > 0. \end{cases}$$

(d) The **quotient ideal** (or **colon ideal**) of the ideals I and J is the ideal (easy check)
$$I : J := \{a \in R \; : \; a \cdot J \subseteq I\}.$$

(e) The **annihilator** of the ideal I is the ideal
$$\mathrm{Ann}(I) := 0 : I = \{a \in R \; : \; a \cdot I = 0\}.$$

For an element $a \in R$ we just write $\mathrm{Ann}(a)$ instead of $\mathrm{Ann}((a))$.

(f) I and J are **coprime ideals** if $I + J = (1)$.

(g) The **radical of an ideal** I is
$$\sqrt{I} := \{r \in R \; : \; \exists \, n \in \mathbb{N} \text{ such that } r^n \in I\}.$$

This is an ideal, because $\sqrt{I} = \pi^{-1}(\mathcal{N}_{R/I})$, where $\pi : R \longrightarrow R/I$ is the canonical projection, the radical is an ideal.

(h) We say that the ideal I is a **radical ideal** if $I = \sqrt{I}$.

Examples.   1. In $\mathbb{Z}$, we have $I = (a)$ and $J = (b)$ and the operations on the ideals can be interpreted in terms of the generators:

$$\begin{aligned}
(a) + (b) &= (\gcd(a,b)) \\
(a) \cap (b) &= (\mathrm{lcm}(a,b)) \\
(a)(b) &= (ab) \\
(a) : (b) &= (\frac{a}{\gcd(a,b)})
\end{aligned}$$

In particular $(a)(b) = (a) \cap (b)$ if and only if a and b are coprime.
If $a = p_1^{n_1} \ldots p_r^{n_r}$ are the distinct prime factors of a, then

$$\sqrt{(a)} = (p_1 \ldots p_r) = \cap_{i=1}^{r} (p_i).$$

2. In $R = \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a field, the ideal $\mathfrak{m} = (x_1, \ldots, x_n)$ (called the **irrelevant maximal ideal** or the **homogeneous maximal ideal**) consists of all polynomials with trivial free term (i.e. term of degree zero). Its powers $\mathfrak{m}^n$ consist of all polynomials with no terms of degree $< n$.

Remark 1.33. The sum, intersection, and product are commutative and associative operations on the set of ideals. Furthermore, the product is distributive over the addition:

$$I(J_1 + J_2) = IJ_1 + IJ_2.$$

In the ring $\mathbb{Z}$, $\cap$ and $+$ are distributive over each other. This is not the case in general. We only have the *modular law*:

$$I \cap (J_1 + J_2) = I \cap J_1 + I \cap J_2 \text{ if } I \supseteq J_1 \text{ or } I \supseteq J_2.$$

$\supseteq$ always holds: $a \in I \cap J_1 + I \cap J_2 \Rightarrow \exists b_1 \in I \cap J_1, b_2 \in I \cap J_2$ such that $a = b_1 + b_2 \in J_1 + J_2$, by definition, and also in I.

$\subseteq$ may fail in general: $a \in I \cap (J_1 + J_2) \Rightarrow \exists b_1 \in J_1, b_2 \in J_2$ such that $a = b_1 + b_2 \in I$. But it may be that $b_1, b_2 \notin I$; it must be both, for if one is in I, then so is the other. This is why $J_1 \subseteq I$ or $J_2 \subseteq I$ imply the equality.

Remark 1.34. We have

$$(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ,$$

but in general the other inclusion does not hold. In $\mathbb{Z}$ however, we have

$$((a) + (b))((a) \cap (b)) = (\gcd(a,b)) \cdot (\mathrm{lcm}(a,b)) = \big(\gcd(a,b) \cdot \mathrm{lcm}(a,b)\big) = (ab) = (a)(b).$$

This implies, since $IJ \subseteq I \cap J$, that if $I + J = (1)$, then $IJ = I \cap J$.

Remark 1.35. We have the following easy to check relations.

(i) $I \subseteq I : J$

(ii) $(I : J)J \subseteq I$

(iii) $(I : J) : K = I : (JK) = (I : K) : J$

(iv) $(\cap_i I_i) : J = \cap_i (I_i : J)$

(v) $I : (\sum_j J) = \cap_j (I : J_j)$

(vi) $I \subseteq \sqrt{I}$

(vii) $\sqrt{I} = \sqrt{\sqrt{I}}$

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

(ix) $\sqrt{I} = (1) \Leftrightarrow I = (1)$

(x) $\sqrt{I+J} = \sqrt{\sqrt{I}+\sqrt{J}}$

(xi) If $\mathfrak{p}$ is prime, then $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for all $n > 0$.

By the definition of the radical of an ideal, we have the following corollary of Proposition 1.29.

Corollary 1.36. *Let $I \subseteq R$ be an ideal. We have*

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}, \qquad \text{where all } \mathfrak{p} \text{ are prime ideals.}$$

Proof. Apply Proposition 1.29 to R/I, and use Lemma 1.10. $\qquad\square$

1.3 Chinese Remainder Theorem

We will now look at a generalization of the Chinese Remainder Theorem from elementary number theory, which essentially says that

$$\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \gcd(m,n) = 1.$$

For a finite family $(I_i)_{i=1,\ldots,n}$ of ideals of R, we define the map

$$\Phi : R \longrightarrow \prod_{i=1}^n R/I_i$$

$$a \longmapsto (a + I_1, \ldots, a + I_n)$$

Proposition 1.37. *In the above notation we have*

(a) *If I_i and I_j are coprime for all $i \neq j$, then $\prod_{i=1}^n I_i = \bigcap_{i=1}^n I_i$.*

(b) *Φ is surjective if and only if I_i and I_j are coprime for all $i \neq j$.*

(c) *Φ is injective if and only if $\cap_{i=1}^n I_i = 0$.*

Proof. (a) We use induction on n. The case $n = 2$ was dealt with in the previous remark, so assume the statement holds for some $n \geq 2$, and we will prove it for $n + 1$. Denote by $J := \prod_{i=1}^n I_i$. By the inductive hypothesis we have

$$J = \prod_{i=1}^n I_i = \bigcap_{i=1}^n I_i.$$

We first prove that I_{n+1} and J are coprime. From $I_{n+1} + I_i = (1)$ for every $i = 1, \ldots, n$ we get that there exist $a_i \in I_{n+1}$ and $b_i \in I_i$ such that $a_i + b_i = 1$. So

$$\prod_{i=1}^n b_i = \prod_{i=1}^n (1 - a_i) = 1 + \alpha, \quad \text{with } \alpha \in I_{n+1},$$

thus $(\prod_{i=1}^n I_i) + I_{n+1} = (1)$. We now conclude by the $n = 2$ case and the inductive hypothesis that

$$\prod_{i=1}^{n+1} I_i = JI_{n+1} = J \cap I_{n+1} = \bigcap_{i=1}^{n+1} I_i.$$

17

(b) "$\Rightarrow$" By symmetry, it suffices to show that $I_1 + I_2 = (1)$. Since Φ is surjective, there exists $a \in R$ such that $\Phi(a) = (1, 0, \ldots, 0)$, which means $1 - a \in I_1$ and $a \in I_2$. Thus $1 = (1 - a) + a \in I_1 + I_2$.

"$\Leftarrow$" Again by symmetry, it suffices to find an $a \in R$ such that $\Phi(a) = (1, 0, \ldots, 0)$. Since for every $i > 1$ we have $I_1 + I_i = (1)$, there exist for every $i > 1$ elements $a_i \in I_1$ and $b_i \in I_i$ such that $a_i + b_i = 1$. We define

$$a := \prod_{i=2}^{n} b_i = \prod_{i=2}^{n} (1 - a_i)$$

Clearly $a \in I_i$ for all $i > 1$, and $a \equiv 1 \mod I_1$.

(c) We have $a \in \operatorname{Ker} \Phi \Leftrightarrow a \in I_i, \ \forall \ i = 1, \ldots, n$, so $\operatorname{Ker} \Phi = \bigcap_{i=1}^{n} I_i$. $\qquad\square$

Corollary 1.38 (The Chinese Remainder Theorem)**.** *If $I_1, \ldots, I_r$ are pairwise coprime ideals of R, then $\prod_{i=1}^{r} I_i = \bigcap_{i=1}^{r} I_i$ and $\pi : R/\prod I_i \longrightarrow \prod R/I_i$ is an isomorphism.*

1.4   Prime Avoidance

The union of ideals is not an ideal in general: $(2) \cup (3) \subset \mathbb{Z}$ contains 2 and 3, but $2 + 3 = 5 \notin (2) \cup (3)$. However, we may say something about what happens if an ideal is contained in the union of primes. The following result (which has many versions) is known as the prime avoidance lemma. It's significance may become clearer after Section 1.7.

Lemma 1.39 (Prime Avoidance)**.** *Let R be a ring.*

(a) *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals of R and $I \subseteq R$ some ideal with the property that $I \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. Then $I \subseteq \mathfrak{p}_i$ for some i.*

(b) *Let $I_1, \ldots, I_n$ be ideals of R and $\mathfrak{p} \subseteq R$ be a prime ideal with the property that $\mathfrak{p} \supseteq \bigcap_{i=1}^{n} I_i$. Then $\mathfrak{p} \supseteq I_i$ for some i. Furthermore, equality in the first relation implies equality in the second; that is, if $\mathfrak{p} = \bigcap_{i=1}^{n} I_i$. Then $\mathfrak{p} = I_i$ for some i.*

Proof. (a) We will show by induction on n that

$$\text{if } I \not\subseteq \mathfrak{p}_i, \ \forall \ i = 1, \ldots, n \Rightarrow I \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i. \tag{1.1}$$

For $n = 1$ it is clear. To highlight the idea for the general case, we also do the case $n = 2$: Assume $I \not\subseteq \mathfrak{p}_1$ and $I \not\subseteq \mathfrak{p}_2$. This means, there exists $a_1 \notin \mathfrak{p}_2$ and $a_2 \notin \mathfrak{p}_1$. If $a_1 \notin \mathfrak{p}_1$, then $a_1 \notin \mathfrak{p}_1 \cup \mathfrak{p}_2$ and we are done. Similarly for a_2. So we assume that $a_1 \in \mathfrak{p}_1$ and $a_2 \in \mathfrak{p}_2$. We consider now $a := a_1 + a_2$.

$$\text{If } a \in \mathfrak{p}_1, \text{ because } a_1 \in \mathfrak{p}_1 \text{ and } a_2 = a - a_1, \text{ we get } a_2 \in \mathfrak{p}_1, \text{ a contradiction.}$$

Analogously we get $a \notin \mathfrak{p}_2$, so $a \notin \mathfrak{p}_1 \cup \mathfrak{p}_2$.

Assume now that (1.1) holds for n, and we aim at proving it for $n+1$. Just like $n = 2$, for every $i = 1, \ldots, n+1$, by the inductive hypothesis, there exists an $a_i \notin \mathfrak{p}_j$, for all $j \neq i$. As soon as some for some i, we have $a_i \notin \mathfrak{p}_i$, then $a_i \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{n+1}$, and we are done. If $a_i \in \mathfrak{p}_i$ for all i, then we define

$$a := \sum_{j=1}^{n+1} a_1 \cdots \widehat{a}_j \cdots a_{n+1},$$

where the hat symbol means that the factor is skipped in the product. So the jth summand in the definition of a belongs to all the $\mathfrak{p}_i$, except $\mathfrak{p}_j$. If $a \in \mathfrak{p}_1$, then we would have $a_2 \cdots a_{n+1} \in \mathfrak{p}_1$. Because $\mathfrak{p}_1$ is prime, we would get that one of the factors would belong to $\mathfrak{p}_1$, which would be a contradiction. Analogously we get $a \notin \mathfrak{p}_i$ for

all i, and we conclude.

(b) By contradiction, assume $I_i \not\subseteq \mathfrak{p}$ for all i. Therefore, there exists for every i an $a_i \in I_i \setminus \mathfrak{p}$. We thus get on the one hand

$$\textstyle\prod_{i=1}^n a_i \in \prod_{i=1}^n I_i \subseteq \bigcap_{i=1}^n I_i,$$

and on the other hand $\prod_{i=1}^n a_i \notin \mathfrak{p}$, because $\mathfrak{p}$ is prime; a contradiction to our hypothesis.
For the equality part: If $\mathfrak{p} = \cap_{i=1}^n I_i$, then $\mathfrak{p} \subseteq I_i$ for every i, and thus $\mathfrak{p} = I_i$, for that i for which $I_i \subseteq \mathfrak{p}$. $\square$

With the new definitions we can express the set $D \subseteq R$ of zero divisors of R as

$$D = \bigcup_{a \neq 0} \mathrm{Ann}(a).$$

We can furthermore prove the following

Proposition 1.40. *Let D be the set of all zero divisors of R. We have*

$$D = \bigcup_{a \neq 0} \sqrt{\mathrm{Ann}(a)}.$$

Proof. As $I \subseteq \sqrt{I}$ in general, we only have to check "$\supseteq$". If $z \in \bigcup_{a \neq 0} \sqrt{\mathrm{Ann}(a)}$, then $z^n \in \mathrm{Ann}(a)$ for some $a \neq 0$, so z^n is a zero divisor, which clearly implies this for z as well. $\square$

Proposition 1.41. *Let $I, J \subseteq R$ be two ideals such that $\sqrt{I}$ and $\sqrt{J}$ are coprime. Then I and J are coprime.*

Proof. We just apply the results from Remark 1.35 to prove that $I + J = (1)$.

$$\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{(1)} = (1) \quad \Rightarrow \quad I + J = (1).$$

$\square$

1.5   Extension and Contraction

In this final section, let $f : R \longrightarrow S$ be a ring homomorphism.

Definition 1.42. Let $I \subseteq R$ and $J \subseteq S$ be ideals.

1. The **extension** of I (under f) is the ideal of S:

$$I^e := S \cdot f(I) = \{\textstyle\sum s_i f(a_i) \; : \; s_i \in S, a_i \in I\}.$$

2. The **contraction** of J (under f) is the ideal of R:

$$J^c := f^{-1}(J) = \{r \in R \mid f(r) \in J\}.$$

Example 1.43. $\mathbb{Z} \longrightarrow \mathbb{Z}[i]$

Proposition 1.44. *Let $f : R \longrightarrow S$, and $I \subseteq R$ and $J \subseteq S$ ideals. We have*

(a) $I \subseteq I^{ec}$ and $J \supseteq J^{ce}$.

(b) $I^e = I^{ece}$ and $J^c = J^{cec}$.

(c) *Let* $C = \{I \subseteq R \ : \ \exists J \subseteq S \text{ an ideal with } I = J^c\}$ *and* $E = \{J \subseteq R \ : \ \exists I \subseteq R \text{ an ideal with } J = I^e\}$ *be the sets of contracted, respectively extended, ideals. We have*

(i) $C = \{I \subseteq R \ : \ I^{ec} = I\}$

(ii) $E = \{J \subseteq S \ : \ J^{ce} = J\}$

(iii) $\epsilon : C \longrightarrow E$ *given by* $I \mapsto I^e$ *is a bijective map with inverse given by* $J \mapsto J^c$.

Proof. (a) is trivial, and (b) follows from (a).

To prove (c),(i) first notice that if $I = I^{ec}$, then I is the contraction of I^e. If $I \in C$, then $I = J^c$ for some $J \subseteq S$. By (b) we have $J^c = J^{cec}$, which translates to $I = I^{ec}$. (ii) follows analogously, and (iii) is just an application of (b). $\qquad \square$

Remark 1.45. If $I_1, I_2 \subseteq R$ and $J_1, J_2 \subseteq S$ are ideals, then we have

(a) $(I_1 + I_2)^e = I_1^e + I_2^e$ and $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$.

(b) $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$ and $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$.

(c) $(I_1 I_2)^e = I_1^e I_2^e$ and $(J_1 J_2)^c \supseteq J_1^c J_2^c$.

(d) $(I_1 : I_2)^e \subseteq I_1^e : I_2^e$ and $(J_1 : J_2)^c \subseteq J_1^c : J_2^c$.

(e) $(\sqrt{I}\,)^e \subseteq \sqrt{I^e}$ and $(\sqrt{J}\,)^c = \sqrt{J^c}$.

1.6 Algebraic Sets

The original motivation behind the introduction of ideals was the generalization of prime decomposition form arithmetic. For this course, the main motivation to study ideals comes from Algebraic Geometry. This section is a first step in this direction.

Algebraic sets are solution sets to systems of (not necessary linear) polynomial equations. We start by giving a more precise definition for this. Throughout this section $\mathbb{K}$ will denote a field and $n \in \mathbb{N}_{>0}$ a positive integer. The **n -dimensional affine space over** $\mathbb{K}$ is

$$\mathbb{A}_{\mathbb{K}}^n := \{(a_1, \ldots, a_n) \ : \ a_i \in \mathbb{K} \text{ for all } i = 1, \ldots, n\}.$$

We deliberately avoid the notation $\mathbb{K}^n$ in order to emphasize that we do not mean the standard n-dimensional $\mathbb{K}$-vector space.

Via the evaluation map, we can think of polynomials as functions defined on $\mathbb{A}_{\mathbb{K}}^n$ with values in $\mathbb{K}$. These will be called *regular functions*. We can thus study the subsets which are mapped to zero.

Definition 1.46. Let $F \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be a (possibly infinite) set of polynomials. The **vanishing locus** of F is the set
$$V(F) := \{\mathbf{a} \in \mathbb{A}_{\mathbb{K}}^n \ : \ f(\mathbf{a}) = 0 \text{ for all } f \in F\}.$$

A subset $Z \subseteq \mathbb{A}_{\mathbb{K}}^n$ is an **algebraic subset** if there exists a subset $F \subseteq \mathbb{K}[x_1, \ldots, x_n]$ such that
$$Z = V(F).$$

For every subset $S \subseteq \mathbb{A}_{\mathbb{K}}^n$ we define the **vanishing ideal** of S (or the *ideal of regular functions vanishing on S*) as
$$I(S) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \ : \ \forall \mathbf{a} \in S \text{ we get } f(\mathbf{a}) = 0\}.$$

It is an immediate check, that the set $I(S)$ we defined above is actually an ideal.

Example 1.47. 1. If $F = \{c_0 + c_1 x + \cdots + c_n x^n\} \subset \mathbb{C}[x]$, then $V(F)$ consists of the complex roots of the polynomial. The fundamental theorem of algebra states that $\sharp V(F) \geq 1$. We can view these as points on the *complex line* $\mathbb{A}^1_{\mathbb{C}}$. As a consequence of Bézout's little theorem, we also have $\sharp V(F) \leq n$. Ideals will give us a method to keep track of "multiplicities" of the points, but for the moment we are only concerned with them as sets.

2. If $F = \{xy\} \subseteq \mathbb{R}[x, y]$, then $V(F)$ consists of the two coordinate axes. Notice however, that $x = 0$ gives us the y-axis, and $y = 0$ gives us the x-axis. If we substitute F with the set of all multiples of xy, that is with the ideal (xy), we still obtain the same vanishing locus.

3. If $F = \{x^2 + y^2 + z^2 - 1, x - z\} \subseteq \mathbb{R}[x, y]$, the $V(F)$ is the intersection of the unit sphere in $\mathbb{A}^3_{\mathbb{R}}$ with the plane given by $x - z$.

4. The set $\mathbb{C} \setminus \{0\}$ is not an algebraic subset of $\mathbb{A}^1_{\mathbb{C}}$. If we consider a finite field $\mathbb{F}_q$, instead of $\mathbb{C}$, then the set is algebraic.

5. Every point and every line in $\mathbb{A}^n_{\mathbb{K}}$ is algebraic.

Remark 1.48. Let $Y, Z \subseteq \mathbb{A}^n_{\mathbb{K}}$ and $F, G \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be subsets. We have:

(a) The ideal $I(Z) \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is radical.

(b) $I(Y \cup Z) = I(Y) \cap I(Z)$.

(c) If $Z \subseteq Y$, then $I(Z) \supseteq I(Y)$.

(d) If $G \subseteq F$, then $V(G) \supseteq V(F)$.

(e) Let (F) denote the ideal generated by F. Then $V((F)) = V(F)$.

Proof. (a) Let $f \in \sqrt{I(Z)}$. This means there exists $r \in \mathbb{N}$ such that $f^r \in I(Z)$, so $f^r(\mathbf{a}) = 0$ for all $\mathbf{a} \in Z$. From the evaluation map $f^r(\mathbf{a}) = (f(\mathbf{a}))^r = 0 \in \mathbb{K}$ for all $\mathbf{a} \in Z$. Because $\mathbb{K}$ is a field, it has no nilpotents other than 0, so $f(\mathbf{a}) = 0$, for all $\mathbf{a} \in Z$, and thus $f \in I(Z)$.

(b) This is an easy direct check of the definition.

(c) This is an easy direct check of the definition.

(d) This is an easy direct check of the definition.

(e) "$\subseteq$" follows from d) because $F \subseteq (F)$.
"$\supseteq$" Let $\mathbf{a} \in V(F)$. We want to show that $f(\mathbf{a}) = 0$ for all $f \in V((f))$. So let $f \in V((f))$. This means there exists a finite number of elements $f_1, \ldots, f_s \in F$ and $r_1, \ldots, r_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f = r_1 f_1 + \cdots + r_s f_s$. So

$$f(\mathbf{a}) = r_1(\mathbf{a}) \cdot f_1(\mathbf{a}) + \cdots + r_s(\mathbf{a}) \cdot f_s(\mathbf{a}) = r_1(\mathbf{a}) \cdot 0 + \cdots + r_s(\mathbf{a}) \cdot 0 = 0.$$

$\square$

Proposition 1.48 e) implies that when dealing with algebraic sets, it is enough to look at vanishing sets of ideals. The next proposition shows that set operations on algebraic sets are compatible with the operations on ideals.

Proposition 1.49. (a) *The empty set and the affine space are algebraic sets.*

(b) *Let $I, J \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be ideals. Then*

$$V(I) \cup V(J) = V(I \cap J) = V(I \cdot J).$$

21

(c) *Let $\mathcal{I}$ be an index set and $(I_i)_{i\in\mathcal{I}}$ be a family of ideals of $\mathbb{K}[x_1,\dots,x_n]$. Then*

$$\bigcap_{i\in\mathcal{I}} V(I_i) = V\left(\sum_{i\in\mathcal{I}} I_i\right).$$

Proof. (a) We have $\emptyset = V((1))$ and $\mathbb{A}_{\mathbb{K}}^n = V((0))$.

(b) We get $V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(I \cdot J)$ from Proposition 1.48 d) as follows:

$$\left.\begin{array}{l} I \cap J \subseteq I \Rightarrow \quad V(I \cap J) \supseteq V(I) \\ I \cap J \subseteq J \Rightarrow \quad V(I \cap J) \supseteq V(J) \end{array}\right\} \quad \Rightarrow \quad V(I) \cup V(J) \subseteq V(I \cap J)$$

$$I \cdot J \subseteq I \cap J \Rightarrow V(I \cap J) \subseteq V(I \cdot J).$$

To conclude, it is enough to prove $V(I \cdot J) \subseteq V(I) \cup V(J)$. So let $\mathbf{a} \in V(I \cdot J)$ and assume that $\mathbf{a} \notin V(I)$. This implies, there exists and $f \in I$, such that $f(\mathbf{a}) \neq 0$. We aim at $\mathbf{a} \in V(J)$, so let $g \in V(J)$. We have $f \cdot g \in I \cdot J$, so, $(f \cdot g)(\mathbf{a}) = f(\mathbf{a}) \cdot g(\mathbf{a}) = 0$. Because $\mathbb{K}$ is a field and $f(\mathbf{a}) \neq 0$ we obtain $g(\mathbf{a}) = 0$.

(c) Proposition 1.48 b) applies just as well for families of ideals, so

$$\bigcap_{i\in\mathcal{I}} V(I_i) = V\left(\bigcup_{i\in\mathcal{I}} I_i\right).$$

By definition, the sum of the ideals is the ideal generated by the union so $\sum_{i\in\mathcal{I}} I_i = \left(\bigcup_{i\in\mathcal{I}} I_i\right)$, and we conclude by Proposition 1.48 e). $\qquad\square$

Remark 1.50. Proposition 1.49 b) shows two possibilities of describing the union of two Zariski closed sets. The first comes from $V(I) \cup V(J) = V(I \cap J)$ is useful because if I and J are radical, then so is $I \cap J$. This is of interest, because there is a one to one order reversing correspondence between algebraic sets and radical ideals of the polynomial ring. The second comes from $V(I) \cup V(J) = V(IJ)$ is more practical in nature: if we know generators of I and J, we know (by definition) the generators of fg as well.

Recall from Topology (see the Appendix), that the closure $\overline{S}$ of any subset $S \subseteq X$, where X is some topological space, is the intersection of all the closed subsets containing S. Proposition 1.49 shows that the algebraic subsets of $\mathbb{A}_{\mathbb{K}}^n$ satisfy the axioms of the closed sets of a topological space.

Definition 1.51. The algebraic sets of $\mathbb{A}_{\mathbb{K}}^n$ are called **Zariski closed sets**. A subset $U \subseteq \mathbb{A}_{\mathbb{K}}^n$ is called **Zariski open** if its complement $\mathbb{A}_{\mathbb{K}}^n \setminus U$ is Zariski closed. The set

$$\mathcal{T} := \{U \subseteq \mathbb{A}_K^n \ : \ U \text{ is Zariski open}\}$$

defines a topology on $\mathbb{A}_{\mathbb{K}}^n$ called the **Zariski topology**[2].

This topological structure brings a powerful new tool to the study of algebraic sets. One should be careful however, that the Zariski topology is very different from the usual topology on $\mathbb{R}^n$ or $\mathbb{C}^n$. For instance, any two nonempty Zariski open sets intersect, which means that this topology is not Hausdorff.

Lemma 1.52. (a) *For any ideal $I \subseteq \mathbb{K}[x_1,\dots,x_n]$ we have[3] $\sqrt{I} \subseteq I(V(I))$.*

(b) *Let $S \subseteq \mathbb{A}_{\mathbb{K}}^n$ be any subset. For the closure $\overline{S}$ of S in the Zariski topology we have $\overline{S} = V(I(S))$.*

Proof. (a) By definition we have $I \subseteq I(V(I))$, so $\sqrt{I} \subseteq \sqrt{I(V(I))}$. By Proposition 1.48 a) we know $I(S)$ is always radical. So, we have $\sqrt{I(V(I))} = I(V(I))$, and we conclude.

---

[2]Oscar Zariski was an American mathematician
[3]When $\mathbb{K}$ is algebraically close, we even have equality. This is essentially the Hilbert Nullstellensatz.

(b) By definition we have $S \subseteq V(I(S))$. Since $V(I(S))$ is closed, we also have $\overline{S} \subseteq V(I(S))$. To check the other inclusion, we have to show that $V(I(S)) \subseteq Z$, for every closed set containing S. So let $J \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and $Z = V(J) \supseteq S$ be the corresponding closed set. On the one hand, from $S \subseteq Z$ we get $I(S) \supseteq I(Z)$, from which we get

$$V(I(S)) \subseteq V(I(Z)).$$

On the other hand, from $Z = V(J)$ we get $J \subseteq I(Z)$, so

$$V(J) \supseteq V(I(Z)).$$

Putting the two together with $V(J) = Z$ we get $V(I(S)) \subseteq Z$.

$\square$

We have defined two maps:

$$\Phi : \quad \{\text{Algebraic sets in } \mathbb{A}^n_{\mathbb{K}}\} \quad \longrightarrow \quad \{\text{Radical ideals of } \mathbb{K}[x_1, \ldots, x_n]\}$$
$$Z \quad \longmapsto \quad I(Z)$$

$$\Psi : \quad \{\text{Radical ideals of } \mathbb{K}[x_1, \ldots, x_n]\} \quad \longrightarrow \quad \{\text{Algebraic sets in } \mathbb{A}^n_{\mathbb{K}}\}$$
$$I \quad \longmapsto \quad V(I)$$

In Lemma 1.52 b) shows that $\Psi \circ \Phi = \mathrm{id}$. In particular, this means that Φ is injective and Ψ is surjective. We will see later (in Hilbert's Nullstellensatz) that if $\mathbb{K}$ is algebraically closed, then also $\Phi \circ \Psi = \mathrm{id}$, so both are order reversing bijections, and we have a well-behaved correspondence between algebra and geometry. If $\mathbb{K}$ is not algebraically closed, we cannot expect this: over $\mathbb{R}$, we have $V((x^2 + 1)) = V((1)) = \emptyset$, so Ψ is not injective. In particular, this is also an example where the reverse inclusion in Lemma 1.52 fails: $\sqrt{(x^2 + 1)} \subsetneq I(V((x^2 + 1))) = I(\emptyset) = (1) = \mathbb{R}[x]$.

Examples. 1. We look at the axes in 3-space over $\mathbb{K}$: the x-axis is $\{(x, 0, 0) \in \mathbb{A}^3_{\mathbb{K}} : \}$, and analogously for the y- and z-axis. These algebraic sets, corresponding to the radical ideals $I_x = (y, z)$, $I_y = (x, z)$, and $I_z = (x, y)$. We have by Proposition 1.49

$$V(I_x \cdot I_y \cdot I_z) = V(I_x \cap I_y \cap I_z) = V(I_x) \cup V(I_y) \cup V(I_z)$$

is the union of the 3 axes, but $(x^2 y, x^2 z, xy^2, y^2 z, xz^2, yz^2, xyz) = (I_x \cdot I_y \cdot I_z) \subsetneq V(I_x \cap I_y \cap I_z) = (xy, xz, yz)$.

2. $I = (y^2 - x^3, z)$ and $J = (x, y)$.

For each point $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{K}}$, we define the maximal ideal

$$\mathfrak{m_a} := (x_1 - a_1, \ldots, x_n - a_n).$$

The ideal is maximal, because the quotient by it is isomorphic to $\mathbb{K}$. To see this, consider the surjective ring homomorphism $\mathrm{ev}_{\mathbf{a}} : \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}$ given by $f \mapsto f(\mathbf{a})$, whose kernel is $\mathfrak{m_a}$.

Remark 1.53. We have

$$I(\{\mathbf{a}\}) = \mathfrak{m_a} \qquad \text{and} \qquad V(\mathfrak{m_a}) = \{\mathbf{a}\}.$$

The first equality follows because $x_1 - a_1, \ldots, x_n - a_n \in I(\{\mathbf{a}\})$, thus $\mathfrak{m_a} \subseteq I(\{\mathbf{a}\}) \subsetneq (1)$, and from the maximality of $\mathfrak{m_a}$ we conclude. The second is obvious.

Lemma 1.54. *Let* $\mathbf{a} \in \mathbb{A}^n_{\mathbb{K}}$ *be a point and* $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *be an ideal. We have*

$$\mathbf{a} \in V(I) \iff I \subseteq \mathfrak{m_a}.$$

Proof. "$\Rightarrow$" From $\{\mathbf{a}\} \subseteq V(I)$ we have $\mathfrak{m_a} = I(\{\mathbf{a}\}) \supseteq I(V(I)) \supseteq I$.
"$\Leftarrow$" From $I \subseteq \mathfrak{m_a}$ we get $V(I) \supseteq V(\mathfrak{m_a}) = \{\mathbf{a}\}$.

$\square$

1.6.1 Hilbert's Nullstellensatz

We do not have developed yet all the technical instruments to prove this important theorem. In particular, we have not proven Noether normalization yet (see Theorem 8.20). I think it is nevertheless useful to have this crucial correspondence stated here. For (friendly) details on this I recommend the first chapter of Klaus Hulek's book *Introduction to Algebraic Geometry*.

Theorem 1.55. *Let $\mathbb{K}$ be an algebraically closed field and let $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$. Then the following hold.*

(1) *Every maximal ideal $\mathfrak{m} \subseteq \mathbb{K}[\mathbf{x}]$ is of the form*

$$\mathfrak{m}_{\mathbf{a}} = (x_1 - a_1, \ldots, x_n - a_n) = \mathcal{I}(\{\mathbf{a}\})$$

for some point $\mathbf{a} \in \mathbb{A}_{\mathbb{K}}^n$.

(2) *If $I \subsetneq \mathbb{K}[\mathbf{x}]$ is a proper ideal, then $V(I) \neq \emptyset$.*

(3) *For every ideal $I \subseteq \mathbb{K}[\mathbf{x}]$ we have*

$$\mathcal{I}(V(I)) = \sqrt{I}.$$

The following is an obvious consequence of Hilbert's Nullstellensatz, but I think it is worth stating in this form.

Remark 1.56. Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_r \in \mathbb{K}[\mathbf{x}]$ be finitely many polynomials, which we think of as polynomial equations in n variables. Then precisely one of the following holds:

(1) There exists a common solution $\mathbf{a} \in \mathbb{K}^n$, such that $f_1(\mathbf{a}) = \cdots = f_r(\mathbf{a}) = 0$.

(2) There exist $g_1, \ldots, g_r \in \mathbb{K}[\mathbf{x}]$, such that $g_1 f_1 + \cdots + g_r f_r = 1$.

The Hilbert Nullstellensatz also has the following consequence.

Corollary 1.57. *If $\mathbb{K}$ is algebraically closed, then the maps $V : \{\text{ideals of } \mathbb{K}[\mathbf{x}]\} \longrightarrow \{\text{subsets of } \mathbb{A}_{\mathbb{K}}^n\}$ and $\mathcal{I} : \{\text{subsets of } \mathbb{A}_{\mathbb{K}}^n\} \longrightarrow \{\text{ideals of } \mathbb{K}[\mathbf{x}]\}$ induce the following bijections:*

$$\{\text{algebraic subsets of } \mathbb{A}_{\mathbb{K}}^n\} \quad \overset{1:1}{\longleftrightarrow} \quad \{\text{ radical ideals of } \mathbb{K}[\mathbf{x}]\}$$
$$\cup\vert \qquad\qquad\qquad\qquad \cup\vert$$
$$\{\text{irred. alg. subsets of } \mathbb{A}_{\mathbb{K}}^n\} \quad \overset{1:1}{\longleftrightarrow} \quad \{\text{ prime ideals of } \mathbb{K}[\mathbf{x}]\}$$
$$\cup\vert \qquad\qquad\qquad\qquad \cup\vert$$
$$\{\text{points of } \mathbb{A}_{\mathbb{K}}^n\} \quad \overset{1:1}{\longleftrightarrow} \quad \{\text{ maximal ideals of } \mathbb{K}[\mathbf{x}]\}$$

1.6.2 The equivalence of categories

Algebras

We recall briefly the definition of algebra over a fixed ring R (commutative with identity).

Definition 1.58. An *R-algebra* is a pair $(S, \varphi : R \longrightarrow S)$, where S is a ring with identity element 1, but which is not necessarily commutative, and φ is a ring homomorphism.

It is a straight consequence of the definition, that if S is an $R-$algebra and T is an $S-$algebra, then T is an $R-$algebra. In particular, every quotient ring S/J of an $R-$algebra S is also an $R-$algebra. The setup that we care about is when $R = \mathbb{K}$ is a field an $S = \mathbb{K}[x_1, \ldots, x_n]$ or a quotient thereof.

Other important examples, the reader may be familiar with from linear algebra, are the $\mathbb{K}$-algebra of endomorphisms of a $\mathbb{K}$-vector space, or the $\mathbb{K}$-algebra of quadratic $n \times n$ matrices. Note that these two are however noncommutative.

In the definition of R-algebra it is not required for $\varphi : R \longrightarrow S$ to be injective. When R is a field this is always the case. In the general case we may replace R with $\varphi(R)$, which is a subring of S isomorphic to $R/\ker\varphi$. Any statement about the R-algebra S can be then recovered from a statement about the $R/\ker\varphi$-algebra S.

Assumption: It is thus convenient and not restrictive to assume that the structure morphism φ is injective, and identify R with $\varphi(R)$.

The R-algebra generated by a subset $\mathcal{S}$ of the R algebra S is the smallest R-algebra containing $\mathcal{S}$. Just as in the case of generating sets for other algebraic structures, it is a standard check that the algebra generated by $\mathcal{S}$ is the set of elements obtained by the permitted algebraic operations; in this case addition and multiplication in S and multiplication with elements form R. We write $R[\mathcal{S}]$ for this algebra. This means, that $R[\mathcal{S}]$ is the set of all polynomial expressions in the elements of $\mathcal{S}$ with coefficients from R.

In particular, if $\mathcal{S} = \{s_1, \ldots, s_n\}$ is finite, and $R = \mathbb{K}$, so we may identify $\mathbb{K}$ with its isomorphic image $\varphi(\mathbb{K})$ in S, we have
$$\mathbb{K}[\mathcal{S}] = \{f(s_1, \ldots, s_n) \ : \ f \in \mathbb{K}[x_1, \ldots, x_n]\}.$$

We call an R-algebra S a **finitely generated R-algebra**, or an R-algebra of **finite type**, if there exists a finite subset $\mathcal{S} = \{s_1, \ldots, s_n\}$ of S such that $S = R[\mathcal{S}]$. For this generating set there is a canonical R-algebra surjective homomorphism
$$\psi : R[x_1, \ldots, x_n] \longrightarrow R[s_1, \ldots, s_n] = S \qquad x_i \longmapsto s_i,$$

which implies by the first isomorphism theorem, that $S \simeq R/\ker\psi$.

In particular, every finitely generated $\mathbb{K}$-algebra is isomorphic to a quotient of the polynomial ring in finitely many variables and coefficients in $\mathbb{K}$. Such structures will play a central role in algebraic geometry and in the associated approach to commutative algebra.

If $(S, \varphi : R \longrightarrow S)$ and $(S', \varphi' : R \longrightarrow S')$ are two R-algebras, then a map $f : S \longrightarrow S'$ is a **homomorphism of R-algebras** if f is a ring homomorphism such that $f \circ \varphi = \varphi'$, that is it makes the following diagram commute:

$$
\begin{array}{ccc}
S & \xrightarrow{\ \ f\ \ } & S' \\
& \varphi \searrow \ \ \nearrow \varphi' & \\
& R &
\end{array}
\qquad . \tag{1.2}
$$

The ring of regular functions

If $Z \subseteq \mathbb{A}^n_\mathbb{K}$ is an algebraic set, then we are interested in the ring of **regular functions**[4] defined on Z:
$$\mathcal{O}(Z) := \{\varphi : Z \longrightarrow \mathbb{K} \ : \ \exists f \in \mathbb{K}[x_1, \ldots, x_n] \text{ with } \varphi(\mathbf{a}) = f(\mathbf{a}) \ \ \forall \mathbf{a} \in Z\}.$$

This has a ring structure with point-wise addition and multiplication. Furthermore, we can embed $\mathbb{K}$ into $\mathcal{O}(Z)$ by considering for each $c \in \mathbb{K}$ the corresponding constant function on Z. So $\mathcal{O}(Z)$ is a $\mathbb{K}$-algebra.

Clearly every polynomial in $\mathbb{K}[\mathbf{x}]$ defines a regular function. Two polynomials f, g take the same values at each point of Z, precisely when $f - g$ is vanishes at each point of Z, so if and only if $f - g \in \mathcal{I}(Z)$. In other words we have a surjective $\mathbb{K}$-algebra homomorphism $\mathbb{K}[\mathbf{x}] \longrightarrow \mathcal{O}(Z)$, whose kernel is $\mathcal{I}(Z)$. Thus
$$\mathcal{O}(Z) \simeq \mathbb{K}[\mathbf{x}]/\mathcal{I}(Z).$$

The regular functions on the whole space $x_i : \mathbb{A}^n_\mathbb{K} \longrightarrow \mathbb{K}$, with $x_i(\mathbf{a}) = a_i$, are called the coordinate functions. Their residue classes in $\mathbb{K}[\mathbf{x}]/\mathcal{I}(Z)$ are $\mathbb{K}$-algebra generators of this ring, thus by the canonical isomorphism above, they can be seen as $\mathbb{K}$-algebra generators of $\mathcal{O}(Z)$. For this reason, $\mathcal{O}(Z)$ is also referred to as the

---

[4] or *algebraic functions*, i.e. defined by polynomials.

coordinate algebra of Z.[5] It will be useful to regard the residue classes of the indeterminate as coordinate functions, so for every $\mathbf{a} \in ZK$ we have

$$\mathbf{a} = (a_1, \ldots, a_n) = (\bar{x}_1(\mathbf{a}), \ldots, \bar{x}_n(\mathbf{a})).$$

Regular maps

Let $Z \subseteq \mathbb{A}^n_{\mathbb{K}}$ and $W \subseteq \mathbb{A}^m_{\mathbb{K}}$ be two algebraic sets. A map $F : Z \longrightarrow W$ between them is a **regular map** if there exists polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, such that

$$F(\mathbf{a}) = (f_1(\mathbf{a}), \ldots, f_m(\mathbf{a})) \in W \qquad \forall \mathbf{a} \in Z.$$

Using the inclusion map $W \hookrightarrow \mathbb{A}^m_{\mathbb{K}}$, we can write $F(\mathbf{z}) = (F_1(\mathbf{z}), \ldots, F_m(\mathbf{z}))$ for any map $F : Z \longrightarrow W$. Thus, the map F is a regular map, precisely when all the functions $F_i : Z \longrightarrow \mathbb{K}$ are regular functions on Z.

Clearly regular maps satisfy the properties for morphisms in a category: composition, associativity and unitial properties. So for each (algebraically closed) field $\mathbb{K}$ we obtain a category $\mathrm{AffSets}(\mathbb{K})$ of affine algebraic subsets.

The equivalence of categories

Before we state the theorem, we want to define the **pullback** of a regular map $f : Z \longrightarrow W$. This is the map $f^* : \mathcal{O}(W) \longrightarrow \mathcal{O}(Z)$, which sends a regular function $g : W \longrightarrow K$ on W to the regular function $g \circ f : Z \longrightarrow \mathbb{K}$ on Z. This means

$$f^*(g) = g \circ f \in \mathcal{O}(Z) \qquad \forall g \in \mathcal{O}(W).$$

We have now all the ingredients to prove state the following corollary of Hilbert's Nullstellensatz.

Theorem 1.59. *Let $\mathbb{K}$ be an algebraically closed field. There is an equivalence of categories between $\mathrm{AffSets}(\mathbb{K})$ and the category of reduced finitely generated $\mathbb{K}$-algebras and $\mathbb{K}$-algebra homomorphisms, defined by the (contravariant) functor $\mathcal{F}$ which sends affine algebraic sets to their ring of regular functions and regular maps to their pullback.*

Proof. We will show that the functor $\mathcal{F}$ is fully faithful and essentially surjective[6]

$\mathcal{F}$ **is fully faithful**. We have to show that for any affine sets $Z \subseteq \mathbb{A}^n_{\mathbb{K}}$ and $W \subseteq \mathbb{A}^m_{\mathbb{K}}$ the following map is bijective:

$$\mathcal{F}_{Z,W} : \mathrm{Hom}_{\mathrm{AffSets}}(Z, W) \longrightarrow \mathrm{Hom}_{\mathbb{K}\text{-Alg}}(\mathcal{O}(W), \mathcal{O}(Z)).$$

We start with **injectivity**. Let $f, f' \in \mathrm{Hom}_{\mathrm{AffSets}}(Z, W)$ be maps with $f^* = (f')^*$. So for all $g \in \mathcal{O}(W)$ we have

$$f^*(g) = g \circ f = g \circ f' = (f')^*(g) \in \mathcal{O}(Z).$$

This means in particular, that for the coordinate functions $\bar{y}_1, \ldots, \bar{y}_m$ on $\mathcal{O}(W) \simeq \mathbb{K}[y_1, \ldots, y_m]/\mathcal{I}(W)$ and for all $\mathbf{a} \in Z$ we have

$$(\bar{y}_i \circ f)(\mathbf{a}) = \bar{y}_i(f(\mathbf{a})) = \bar{y}_i(f'(\mathbf{a}))$$

This implies that for every $\mathbf{a} \in Z$ that

$$f(\mathbf{a}) = (\bar{y}_1(f(\mathbf{a})), \ldots, \bar{y}_m(f(\mathbf{a}))) = (\bar{y}_1(f'(\mathbf{a})), \ldots, \bar{y}_m(f'(\mathbf{a}))) = f'(\mathbf{a}).$$

For **surjectivity**, let $\varphi : \mathcal{O}(W) \longrightarrow \mathcal{O}(Z)$ be a $\mathbb{K}$-algebra homomorphism. Denote for every $i = 1, \ldots, m$ the image of the coordinate functions of W by

$$s_i := \varphi(\bar{y}_i) \in \mathcal{O}(Z).$$

---

[5] One should think of the $\mathbb{K}$-algebra $\mathcal{O}(Z)$, as a way to describe Z without mentioning its embedding in the affine space $\mathbb{A}^n_{\mathbb{K}}$.

[6] Recall that a functor is **full** if it induces a surjective map on the sets of morphisms, it is **faithful** if it induces an injective map on the sets of morphisms, and a functor is essentially surjective if every object in the target category is isomorphic to an object in the image of the functor.

In particular, because φ is a $\mathbb{K}$-algebra morphism, for every residue class of a polynomial $h \in \mathbb{K}[y_1, \ldots, y_m]$ we have

$$\varphi([h]) = h(s_1, \ldots, s_m).$$

We define the map $f : Z \longrightarrow \mathbb{A}_{\mathbb{K}}^m$ through $f(\mathbf{a}) = (s_1(\mathbf{a}), \ldots, s_m(\mathbf{a}))$. This is by definition a regular map. It also satisfies $f^* = \varphi$, because as functions on W we have the following:

$$f^*(\bar{y}_i) = \bar{y}_i \circ f = s_i = \varphi(\bar{y}_i)$$

for every $i = 1, \ldots, m$ and the $\bar{y}_i$ are the $\mathbb{K}$-algebra generators of $\mathcal{O}(W)$.

We just need to check that $f(Z) \subseteq W$. As $W = V(\mathcal{I}(W))$, this means that we need to check for every $f(\mathbf{a})$, that we have

$$h(f(\mathbf{a})) = 0 \qquad \forall\, h \in \mathcal{I}(W).$$

As $h \in \mathcal{I}(W)$, it means that $[h] = 0 \in \mathcal{O}(W) = \mathbb{K}[y_1, \ldots, y_m]/\mathcal{I}(W)$. Because $\varphi : \mathcal{O}(W) \longrightarrow \mathcal{O}(Z)$ is a ring homomorphism, we have $\varphi([h]) = 0 \in \mathcal{O}[Z]$. In other words, $\varphi([h])$ is the zero function on Z. This implies that

$$h(f(\mathbf{a})) = h(s_1(\mathbf{a}), \ldots, s_m(\mathbf{a})) = \varphi(h)(\mathbf{a}) = 0.$$

Therefore $f(\mathbf{a}) \in W$.

Finally, for **effective surjectivity** we just need to show that every finitely generated reduced $\mathbb{K}$-algebra R is isomorphic to some $\mathcal{O}(Z)$ for some algebraic set $\mathcal{O}(Z)$. As R is a finitely generated $\mathbb{K}$-algebra, there exists some $n \in \mathbb{N}$ such that

$$R \simeq \mathbb{K}[x_1, \ldots, x_n]/I,$$

for some ideal $I \subseteq \mathbb{K}[\mathbf{x}]$. Being reduced is equivalent to I being radical, so by Hilbert's Nullstellensatz, we have $I = \mathcal{I}(V(I))$ and thus $R \simeq \mathbb{K}[\mathbf{x}]/I \simeq \mathcal{O}(V(I))$. $\qquad \square$

1.7 The spectrum of a ring

We just saw that Hilbert's Nullstellensatz gives more than a nice correspondence between maximal ideals and points in affine space. It gives an equivalence of categories, so one could "do geometry" just by working with reduced finitely generated $\mathbb{K}$-algebras over algebraically closed fields. This category is however not as large as one may want. There are constructions of families of such objects, which are geometric objects themselves. In order to study them properly one should thus enlarge the category on the algebra side of the correspondence. The topology on the prime spectrum of a ring is (first step towards) the answer to the question: *What category of geometric objects is equivalent to the category of commutative rings?*

One could have been tempted to keep just maximal ideals as the points in these geometric objects. One problem with this approach is given by Remark 1.18: the preimages of maximal ideals under ring homomorphisms are not necessarily maximal ideals again. But the preimages of prime ideals are prime. If one wants to mimic Theorem 1.59 for generic rings, one needs to define the a functor from the category of rings. Then morphisms should map points into points, and the natural way for doing this is by taking preimages.

Definition 1.60. For every ring R the (prime) **spectrum** of R is the set $\mathrm{Spec}(R)$ containing all prime ideals of R. For any ideal $I \subseteq R$, the **variety of I** is

$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R)\ :\ I \subseteq \mathfrak{p}\}.$$

The **maximal spectrum** of R is $\mathrm{MaxSpec}(R)$ is the set of all maximal ideals of R. Hilbert's Nullstellensatz (see later in these notes/ the Internet/ a book) tells us that $\mathrm{MaxSpec}(\mathbb{K}[x_1, \ldots, x_n])$ is in bijection with the points of $\mathbb{A}_{\mathbb{K}}^n$ when $\mathbb{K} = \overline{\mathbb{K}}$.

Remark 1.61. We have the following Properties of $\mathrm{Spec}\, R$:

1. $\operatorname{Spec}(R)$ is empty if and only if R is the zero ring.

2. If $I \subseteq J$ then $V(J) \subseteq V(I)$.

3. If $V(J) \subseteq V(I)$ then $I \subseteq \sqrt{J}$. (This is a consequence of Corollary 1.36).

4. $V(I) = V(J) \iff \sqrt{I} = \sqrt{J}$.

5. $V(I) \cup V(J) = V(I \cap J) = V(I \cdot J)$.

6. If $(I_i)_{i \in \mathcal{I}}$ is a family of ideals, then $\cap_{i \in \mathcal{I}} V(I_i) = V(\sum_{i \in \mathcal{I}} I_i)$.

7. $V((1)) = \emptyset$ and $V((0)) = \operatorname{Spec}(R)$.

Just as in the case of algebraic subsets of the affine space, the properties 5., 6., 7. of Remark 1.61 imply that the collection of subsets $\{V(I) \ : \ I \subseteq R \text{ ideal}\} \subseteq 2^{\operatorname{Spec} R}$ satisfies the closed-sets-axioms of a topology. We call the topology on $\operatorname{Spec}(R)$ with closed sets $V(I)$ (also) the **Zariski topology**. Moreover, the map $I \mapsto V(I)$ is an order-inverting bijection from the radical ideals to the closed sets.

Next we will describe a basis[7] for the Zariski topology (see Appendix A). Working with a basis simplifies many proofs.

Given an element $f \in R$ we define the **principal open set** (or **distinguished open set**[8]) associated to f as

$$D(f) := \operatorname{Spec}(R) \setminus V((f)).$$

Remark 1.62. By definition we have $\mathfrak{p} \notin V(I) \Leftrightarrow I \not\subseteq \mathfrak{p}$, so

$$\mathfrak{p} \in D(f) \iff \mathfrak{p} \notin V(f) \iff (f) \not\subseteq \mathfrak{p} \iff f \notin \mathfrak{p}.$$

Proposition 1.63. *The principal open sets form a basis of the Zariski topology on* $\operatorname{Spec}(R)$.

Proof. Let U be a Zariski open subset of $\operatorname{Spec}(R)$ and $\mathfrak{p} \in U$ be a point. This means that there exists an ideal $I \subseteq R$ such that $U = \operatorname{Spec}(R) \setminus V(I)$ and that $\mathfrak{p} \notin V(I)$. The latter implies by the definition of $V(I)$ that $I \not\subseteq \mathfrak{p}$. In particular, there exists an element $f \in I$ such that $f \notin \mathfrak{p}$. By Remark 1.62 this is equivalent to $\mathfrak{p} \in D(f)$. Because $f \in I$, we also have $(f) \subseteq I$ and thus $V(f) \supseteq V(I)$. By elementary set theory we have

$$D(f) = \operatorname{Spec}(R) \setminus V(f) \subseteq \operatorname{Spec}(R) \setminus I = U.$$

$\square$

The previous proposition can be used in particular to show that the union of all distinguished open sets the whole spectrum is. Distinguished open sets also have the following property:

$$D(f) \cap D(g) = D(fg). \tag{1.3}$$

This holds, because $\mathfrak{p} \in D(f) \cap D(g) \iff f, g \notin \mathfrak{p}$, which, because $\mathfrak{p}$ is a prime ideal, is equivalent to $fg \notin \mathfrak{p}$. These two properties (covering of the space and closure under intersection) mean that one can define a topology on $\operatorname{Spec}(R)$ by taking all possible unions of distinguished open sets. As we have seen in Propostion 1.63, this topology is the Zariski topology.

The principal open sets also satisfy the following.

---

[7] A **basis for a given topology** $\mathcal{T}$ on a set X is a collection $\mathcal{B}$ of subsets of X such that

$$\forall \, U \in \mathcal{T} \text{ and } \forall \, x \in U \ \ \exists \, B \in \mathcal{B} \text{ such that } x \in B \subseteq U.$$

[8] hence the letter "D" in the notation $D(\bullet)$. In [AM69] these sets are called *basic open sets* and denoted by X_f.

Remark 1.64. (a) $D(f) = \emptyset \iff f$ is nilpotent.

(b) $D(f) = \mathrm{Spec}(R) \iff f$ is a unit.

(c) $D(f) = D(g) \iff \sqrt{(f)} = \sqrt{(g)}$.

Proposition 1.65. *For any ring R, the topological space $\mathrm{Spec}(R)$ is quasi-compact[9].*

Proof. Let $(I_\alpha)_{\alpha \in A}$ be a family of ideals, and denote for each $\alpha \in A$ by $U_\alpha = \mathrm{Spec}(R) \setminus V(I_\alpha)$ the corresponding open set. Assume that

$$\mathrm{Spec}(R) = \bigcup_{\alpha \in A} U_\alpha.$$

This is equivalent to $\bigcap_{\alpha \in A} V(I_\alpha) = \emptyset$. As $\bigcap_{\alpha \in A} V(I_\alpha) = V(\sum_{\alpha \in A} I_\alpha)$, we obtain that

$$\sum_{\alpha \in A} I_\alpha \text{ is not contained in any prime ideal of } R.$$

This implies it must be the whole ring, so $1 \in \sum_{\alpha \in A} I_\alpha$. This means, there exist finitely many indices $\alpha_1, \ldots, \alpha_r$, and for each index an element $f_i \in I_{\alpha_i}$ such that $f_1 + \cdots + f_r = 1$. This implies

$$\sum_{i=1}^r I_{\alpha_i} = (1).$$

So, reasoning as above, but in reverse, we get $\mathrm{Spec}(R) = \bigcup_{i=1}^r U_{\lambda_i}$. $\qquad \square$

Furthermore, every $D(f)$ is quasi-compact, and any open subset of $\mathrm{Spec}(R)$ is quasi compact if and only if it is the finite union of principal open sets.

In the usual topology on $\mathbb{R}^n$ or $\mathbb{C}^n$, as well as in the Zariski topology on $\mathbb{A}^n_{\mathbb{K}}$, all the sets consisting of exactly one point were closed. This is no longer true in general for the spectrum of a ring.

Proposition 1.66. *Let R be a ring and $\mathfrak{p} \in \mathrm{Spec}(R)$.*

(a) *The set $\{\mathfrak{p}\}$ is closed in $\mathrm{Spec}(R) \iff$ the prime ideal $\mathfrak{p}$ is maximal.*

(b) *The closure of a point is $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$.*

(c) *For another prime ideal $\mathfrak{q} \subseteq R$ we have $\mathfrak{q} \in \overline{\{\mathfrak{p}\}} \iff \mathfrak{p} \subseteq \mathfrak{q}$.*

(d) $\mathrm{Spec}(R)$ *is a T_0-space[10].*

(e) $\mathrm{Spec}(R)$ *is irreducible $\iff \sqrt{0}$ is a prime ideal.*

(f) *The irreducible components of $\mathrm{Spec}(R)$ are the closed sets $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of R.*

For every ring homomorphism $\varphi : R \longrightarrow S$, there exists a natural map $\varphi^* : \mathrm{Spec}(S) \longrightarrow \mathrm{Spec}(R)$, given by

$$\varphi^*(\mathfrak{q}) := \varphi^{-1}(\mathfrak{q}).$$

Note that the same procedure does not work in general for the MaxSpec, that is MaxSpec does not behave functorially.

Proposition 1.67. *Let R and S be rings, and denote by $X := Spec(R)$ and $Y := \mathrm{Spec}(S)$. Let $f : R \longrightarrow S$ be a ring homomorphism, and $\varphi^* : Y \longrightarrow X$ the associated map. We have the following.*

(a) φ^* *is continuous.*

(b) *If $I \subseteq R$ is an ideal, then $(\varphi^*)^{-1}(V(I)) = V(I^e)$.*

---

[9] A topological space is **quasi-compact** if and only if each open covering of X has a finite subcovering. The term *compact* means quasi-compact and Hausdorff.

[10] A space X is T_0 if for any $x, y \in X$ there exists an open set U such that $(x \in U$ and $y \notin U)$ or $(x \notin U$ and $y \in U)$.

(c) *If $J \subseteq S$ is an ideal, then $\overline{\varphi^*(V(J))} = V(J^c)$.*

(d) *If φ is surjective, then φ^* is a homeomorphism of Y onto the closed subset $V(\mathrm{Ker}(\varphi))$ of X. In particular, $\mathrm{Spec}(R/I)$ and $V(I)$, as well as $\mathrm{Spec}(R)$ and $\mathrm{Spec}(R/\sqrt{(0)})$ are naturally homeomorphic.*

(e) *If φ is injective, then $\varphi^*(Y)$ is dense in X. More precisely, $\varphi^*(Y)$ is dense in X if and only if $\mathrm{Ker}(\varphi) \subseteq \sqrt{(0)}$.*

(f) *If $\psi : S \longrightarrow T$ is another ring homomorphism, then $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.*

This proposition shows that Spec is a contravariant functor from **Ring** to **Top**.

Chapter 2

Modules

Modules are to rings what vector spaces are to fields. There are two major examples of modules over a ring R: ideals and quotient rings. This alone should be reason enough to have a closer look at modules.

2.1 The category of modules

Definition 2.1. Let R be a ring. An R-module is a pair (M, μ) where M is an Abelian group and μ is an external operation $\mu : R \times M \longrightarrow M$, for which we write $rx := \mu(r, x)$, such that the following axioms are satisfied:

(M1) $r(x + y) = rx + ry$,

(M2) $(r + s)x = rx + sx$,

(M3) $(rs)x = r(sx)$,

(M4) $1x = x$, $\qquad\qquad\qquad \forall\ r, s \in R$ and $\forall\ x, y \in M$.

Remark 2.2. Denote by $\mathrm{End}_{\mathbf{Ab}}(M)$ the (usually not commutative) ring of endomorphisms of the Abelian group M. Maps $\varphi : R \longrightarrow \mathrm{End}_{\mathbf{Ab}}(M)$ from the commutative ring R to $\mathrm{End}_{\mathbf{Ab}}(M)$ are in one-to-one correspondence with actions of R on M: $rx \longleftrightarrow (\varphi(r))(x)$. Through this correspondence, M is an R-module if and only if φ is a ring homomorphism. In other words, one could define an R-module as a pair (M, φ) where M is an Abelian group and $\varphi : R \longrightarrow \mathrm{End}_{\mathbf{Ab}}(M)$ is a ring homomorphism.

Examples.   1. If $I \subseteq R$ is an ideal, then I is an R-module. In particular, R is an R-module and the trivial group 0 is an R-module.

2. If $R = \mathbb{K}$ is a field, then an R-module is a $\mathbb{K}$-vector space.

3. The category of $\mathbb{Z}$-modules is equivalent to the category of Abelian groups.

4. If $R = \mathbb{K}[x]$, with $\mathbb{K}$ a field, then R-modules are $\mathbb{K}$-vector spaces together with a $\mathbb{K}$-vector-space-endomorphism.

5. A ring homomorphism $\varphi : R \longrightarrow S$ defines a R-module structure on S by setting

$$rs := \varphi(r) \cdot s.$$

In particular, for every ideal $I \subseteq R$ we have that R/I is an R-module via the canonical projection $\pi : R \longrightarrow R/I$.

6. For every ring R the Abelian Group $(R^n, +)$, where the addition is component-wise has a natural structure of R-module. This is called the standard free R-module of rank n.

7. If G is a finite group, and $\mathbb{K}[G]$ is the group algebra over the field $\mathbb{K}$, then $\mathbb{K}[G]$-modules are $\mathbb{K}$-representations of G.

Remark 2.3. Let R be a ring and M and R-module. For all $r \in R$ and $x \in M$ we have

(a) $r0 = 0x = 0$,

(b) $a(-x) = (-a)x = -(ax)$.

If $R = \mathbb{K}$ is a field, then we also have from linear algebra $rx = 0 \Rightarrow r = 0$ or $x = 0$. This fails in general for modules: $0 \neq \hat{2} \in \mathbb{Z}/4\mathbb{Z}$ und $0 \neq 2 \in \mathbb{Z}$. We will come back to these annihilating elements.

Definition 2.4. Let M, N be two R-modules. An **R-module homomorphism** (or **R-linear map**) is a map $f : M \longrightarrow N$ satisfying

(MHom1) $f(x + y) = f(x) + f(y)$,

(MHom2) $f(rx) = rf(x)$.

for all $r \in R$ and all $x, y \in M$.

In particular, an R-linear map is a group homomorphism which is compatible with the action of R. The composition of R-module homomorphisms is again an R-module homomorphism.

In linear algebra the set of linear maps $\mathrm{Hom}_{\mathbb{K}}(V, W)$ has a natural structure of $\mathbb{K}$-vector space. Analogously, for any two R-modules M and N, the set of all R-linear maps

$$\mathrm{Hom}_R(M, N) := \{f : M \longrightarrow N \ : \ f \text{ is } R\text{-linear}\}$$

has a structure of R-module with the operations $f + g$ and rf defined by:

$$\begin{aligned} (f + g)(x) &:= f(x) + g(x) \\ (rf)(x) &:= rf(x) \end{aligned}$$

for any $f, g \in \mathrm{Hom}_R(M, N)$, $r \in R$ and $x \in M$. The neutral element for addition is the zero homomorphism $0 : M \longrightarrow N$, given by $x \mapsto 0$.

Remark 2.5. Let M, M', N, N' be R-modules.

$$\begin{aligned} \text{For } u : M \longrightarrow M' \quad &\text{define} \quad u^* : \mathrm{Hom}_R(M', N) \longrightarrow \mathrm{Hom}_R(M, N) \quad u^*(f) := f \circ u \\ \text{For } v : N \longrightarrow N' \quad &\text{define} \quad v_* : \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M, N') \quad v_*(f) := v \circ f \end{aligned}$$

Both u^* and v_* are R-linear maps. Therefore, for fixed R-modules M and N, $\mathrm{Hom}_R(-, N)$ and $\mathrm{Hom}_R(M, -)$ are functors from **R-Mod** to **R-Mod**, with the first being contravariant and the second covariant.

Modules which have identical (indistinguishable) structures are called isomorphic. The "correct"[1] definition of an isomorphism is the following.

Definition 2.6. Let R be a ring and M, N be R-modules. An R-linear map $f : M \longrightarrow N$ is an **isomorphism of R-modules** if there exists an R-linear map $f' : N \longrightarrow M$ such that $f \circ f' = \mathrm{id}_N$ and $f' \circ f = \mathrm{id}_M$.

Exercise. Show that an R-module homomorphism is an isomorphism if and only it is bijective.

Remark 2.7. For any R-module M there is a natural isomorphism

$$\mathrm{Hom}_R(R, M) \cong M$$

given by $\mathrm{Hom}_R(R, M) \ni f \longmapsto f(1)$.

---

[1] By "correct" we mean it works for any category. The point for doing this is that not in all categories bijective homomorphisms are isomorphisms. An easy abstract example is in the category of Posets with order preserving maps as homomorphisms: $P = \{a, b, c\}$ with $a \leq b$ and $a \leq c$, but b and c incomparable, and $Q = \{1, 2, 3\}$ with the natural order. The map $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 3$ is a bijective homomorphism, but the inverse (in **Set**) is not a homomorphism of posets. There are also examples from algebraic geometry, where bijective continuous maps are not always homeomorphisms (the isomorphisms between topological spaces).

2.2 Submodules and Quotient Modules

Definition 2.8. Let R be a ring and M an R-module. An R-**submodule** of M is a subset $N \subseteq M$ such that

(SM1) $N \neq \emptyset$,

(SM2) $\forall\, x, y \in N$ we have $x + y \in N$,

(SM3) $\forall\, r \in R$ and $\forall x \in N$ we have $rx \in N$.

In particular, an R-submodule is an R-module. For any $x \in N$ we have $-x = (-1)x \in N$ and $0x = 0 \in N$, so a submodule is a subgroup which is closed under multiplication with elements from R. Notice that this works even if R is the zero ring: By the module axiom (M 4) we have for all $x \in M$ that $x = 1x = 0x = 0$, so $M = 0$.

Any ring R is an R-module, and the R-submodules of R are exactly the ideals of R.

If N is a R-submodule of M, then the Abelian group M/N inherits an R-module structure defined by

$$r(x + N) := rx + N \qquad \forall\, r \in R.$$

The R-module M/N is called the **quotient module of M by N**. By directly checking the definition, one can see that the canonical projection $\pi : M \longrightarrow M/N$ is an R-module homomorphism.

Remark 2.9. There is a one-to-one order-preserving correspondence

$$\{\text{Submodules of } M \text{ containing } N\} \leftrightarrow \{\text{ Submodules of } M/N \}.$$

Lemma 1.10 is just a particular case of this statement.

Let $f : M \longrightarrow N$ be an R-module homomorphism.

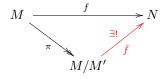The **kernel** of f is the set $\mathrm{Ker}(f) := \{x \in M \ : \ f(x) = 0\}$.

The **image** of f is the set $\mathrm{Im}(f) := f(M) = \{y \in N \ : \ \exists\, x \in M \text{ such that } f(x) = y\}$.

It is a very easy check to see that $\mathrm{Ker}(f)$ is a submodule of M and $\mathrm{Im}(f)$ is a submodule of N.

The **cokernel**[2] of f is the R-module $\mathrm{Coker}(f) := N/\mathrm{Im}(f)$.

Just as for groups and rings, the quotient module satisfies a universal property:

Theorem 2.10. *Let R be a ring, M an R-module and $M' \subseteq M$ a submodule. Let $\pi : M \longrightarrow M/M'$ be the canonical surjection. For every R-module N and every R-module homomorphism $f : M \longrightarrow N$ with the property that $M' \subseteq \mathrm{Ker}(f)$, there exists a unique homomorphism $\overline{f} : M/M' \longrightarrow N$, such that $f = \overline{f} \circ \pi$. That is we have the following commutative diagram*

Furthermore,

1. $\overline{f}$ *is injective* $\Leftrightarrow \mathrm{Ker}\, f = M'$.

2. $\overline{f}$ *is surjective* $\Leftrightarrow f$ *is surjective.*

Theorem 2.10 has several consequences. We will start with the Isomorphism Theorems. Later on (cf. 2.36) we will see more consequences.

---

[2]If you think of "kernels" as measures of how far a homomorphism is from being injective, then "cokernels" give a measure of how far a homomorphism is from being surjective. They play an important role in duality, and are useful in homological algebra, where they fit certain diagrams in the most natural way.

Corollary 2.11 (The First Isomorphism Theorem for Modules/Fundamental Theorem of Homomorphisms). *If $f : M \longrightarrow N$ is an R-module homomorphism, then $M/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.*

A further corollary is the so-called *Second Isomorphism Theorem*[3]. Some authors pack in this statement Remark 2.9 as well.

Corollary 2.12 (The Second Isomorphism Theorem for Modules). *If $N \subseteq M \subseteq L$ are R-modules, then*

$$\frac{L/N}{M/N} \cong \frac{L}{M}.$$

Proof. We define the map $f : L/N \longrightarrow L/M$ by

$$f(x + N) := x + M.$$

The map f is well defined, because if $x + N = y + N$, then $x - y \in N \subseteq M$, so $x + M = y + M$. It is clearly an R-module homomorphism, and $x + N \in \operatorname{Ker}(f)$ if and only if $x \in M$, so $\operatorname{Ker}(f) = M/N$. We conclude by The First Isomorphism Theorem 2.11. $\qquad\square$

The sum of two submodules $M_1, M_2 \subseteq M$ is $M_1 + M_2 = \{x_1 + x_2 \; : \; x_i \in M_i\}$. (Cf. Section 2.3, Definition 2.14 for more details and a generalization to arbitrary families.)

Corollary 2.13 (The Third Isomorphism Theorem For Modueles). *If M_1, M_2 are R-submodules of M, then*

$$\frac{M_1 + M_2}{M_1} \cong \frac{M_2}{M_1 \cap M_2}.$$

Proof. Consider the inclusion map $\imath : M_2 \longrightarrow M_1 + M_2$, given by $x \mapsto x$, and the canonical projection $\pi : M_1 + M_2 \longrightarrow (M_1 + M_2)/M_1$. The composition $f = \pi \circ \imath$ is surjective and its kernel is $M_1 \cap M_2$. We conclude by The First Isomorphism Theorem 2.11. $\qquad\square$

2.3 Operations on Submodules

We may extend most operations from Section 1.2 to modules. Let M be and R-module and $(M_i)_{i \in \mathcal{I}}$ be a (possibly infinte) family of submodules of M. An immediate check shows $\bigcap_{i \in \mathcal{I}} M_i$ is an R-submodule of M as well.

Definition 2.14. (a) The **sum** of the family $(M_i)_{i \in \mathcal{I}}$ is the smallest R-submodule of M containing all of them:

$$\sum_{i \in \mathcal{I}} M_i \quad := \quad \bigcap_{M' \supseteq \bigcup_i M_i} M'$$
$$= \quad \Big\{ \sum x_i \; : \; \text{all finite sums with } x_i \in M_i \Big\}.$$

(b) We cannot define the product of submodules because we cannot (internally) multiply elements in a module. What we can do is multiply elements of a (sub)module with elements of R. For an ideal $I \subseteq R$ and an R-module M we define

$$IM := \Big\{ \sum r_k x_k \; : \; \text{all finite sums with } r_k \in I, \text{ and } x_i \in M \Big\}.$$

(c) The **colon** of two R-submodules $N, P \subseteq M$ is the <u>ideal of R</u> defined as

$$N : P := \{a \in R \; : \; aP \subseteq N\}.$$

---

[3]The exact names are not universally accepted, and vary in the literature. However the generic name of these results as *The Isomorphism Theorems* is widely spread.

(d) The **annihilator** of the R-module M is the ideal of R defined as

$$\mathrm{Ann}_R(M) := 0 : M = \{a \in R \ : \ aM = 0\}.$$

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

(e) An element $x \in M$ is called **torsion element** if $\mathrm{Ann}_R(x) \neq 0$. The **torsion submodule** of M is

$$\mathrm{Tors}(M) = \{x \in M \ : \ \mathrm{Ann}_R(x) \neq 0\}.$$

(Exercise: Check it is actually a submodule.) An R-module M is called **torsion free** if $\mathrm{Tors}(M) = 0$, and it is called **torsion module** if $\mathrm{Tors}(M) = M$.

Warning: Torsion free is not the same as faithful. Exercise: Which is stronger?

(f) The submodule **generated by** an element $x \in M$ is $Rx := \{rx \ : \ r \in R\}$. It is also denoted by $\langle x \rangle$ or by $\mathrm{Span}_R\{x\}$.

(g) We say that the subset $S = \{x_i \mid i \in \mathcal{I}\}$ of M is a **set of generators** of M if

$$\mathrm{Span}_R(S) := \sum_{i \in \mathcal{I}} Rx_i = M.$$

This means that every element of M can be expressed (not necessarily uniquely) as a finite linear combination of elements of S with coefficients from R. We say that S is a **minimal set of generators** of M if no proper subset generates M.

(h) An R-module is called **finitely generated** if it has a finite set of generators.

Remark 2.15. For an R-module M and any ideal $I \subseteq \mathrm{Ann}_R(M)$, we may regard M as an R/I-module as well. The action is given by

$$(r + I)x := rx, \quad \text{for all } r + I \in R/I \text{ and } x \in M.$$

The only thing to check is that it is well defined: If $r + I = r' + I$, then $r - r' \in I \subseteq \mathrm{Ann}_R(M)$, so $(r - r')x = rx - r'x = 0$ for all $x \in M$. We thus have that every R-module M is a faithful $R/\mathrm{Ann}_R(M)$ module.

Remark 2.16. Let M, N be R-modules. It is an easy Exercise to prove that:

(a) $\mathrm{Ann}(M + N) = \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$.

(b) $M : N = \mathrm{Ann}\left(\frac{N+M}{M}\right)$.

2.4 Direct Sum and Direct Product

Let $\mathcal{I} \neq \emptyset$ be a possibly infinite index set, and let $(M_i)_{i \in \mathcal{I}}$ be a family of R-modules indexed by $\mathcal{I}$. The Cartesian product

$$\bigtimes_{i \in \mathcal{I}} M_i := \{f : \mathcal{I} \longrightarrow \cup_{i \in \mathcal{I}} M_i \ : \ f(i) \in M_i, \forall \, i \in \mathcal{I}\} = \{(x_i)_{i \in \mathcal{I}}\}$$

together with component-wise addition and scalar multiplication is an R-module called the **direct product** of the family $(M_i)_{i \in \mathcal{I}}$.

The subset

$$\bigoplus_{i \in \mathcal{I}} M_i := \left\{(x_i)_{i \in \mathcal{I}} \in \bigtimes_{i \in \mathcal{I}} M_i \ : \ x_i \neq 0 \text{ for finitely many } i \in I\right\}$$

is a submodule of the direct product called the **direct sum** of the family $(M_i)_{i \in \mathcal{I}}$. In particular, the direct sum and the direct product coincide if $\mathcal{I}$ is finite.

For an index set $\mathcal{I}$ we denote by $M^{\oplus \mathcal{I}} := \bigoplus_{i \in \mathcal{I}} M$ the direct sum of the family indexed by $\mathcal{I}$ in which each member is M. If $\mathcal{I}$ is finite of cardinality n we write M^n for $M^{\oplus \{1,\ldots,n\}}$. The convention is that the empty direct sum is the zero module, so $M^0 = 0$.

For every family $(M_i)_{i \in \mathcal{I}}$ of R-modules and for every $k \in \mathcal{I}$ we define the maps
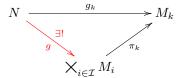
$$
\begin{aligned}
j_k : M_k &\longrightarrow \bigoplus_{i \in \mathcal{I}} M_i \\
x &\longmapsto (x_i)_{i \in \mathcal{I}} \text{ with } x_i = \begin{cases} x, & \text{if } i = k \\ 0, & \text{if otherwise,} \end{cases}
\end{aligned}
$$

and the maps

$$
\begin{aligned}
\pi_k : \bigtimes_{i \in \mathcal{I}} M_i &\longrightarrow M_k \\
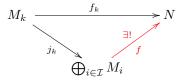(x_i)_{i \in \mathcal{I}} &\longmapsto x_k.
\end{aligned}
$$

Remark 2.17 (The universal property of the direct product). For any R-module N and any collection of R-linear maps $(g_k : N \longrightarrow M_k)_{k \in \mathcal{I}}$, there is a unique homomorphism $g \colon N \longrightarrow \bigtimes_{i \in \mathcal{I}} M_i$ such that the following diagrams commute for every $k \in \mathcal{I}$:

$$
\begin{array}{ccc}
N & \xrightarrow{\quad g_k \quad} & M_k \\
& \searrow{\scriptstyle g} \quad \nearrow{\scriptstyle \pi_k} & \\
& \bigtimes_{i \in \mathcal{I}} M_i &
\end{array}
$$

In other words,

$$
\operatorname{Hom}_R \left(N, \bigtimes_{i \in \mathcal{I}} M_i \right) \cong \bigtimes_{i \in \mathcal{I}} \operatorname{Hom}_R(N, M_i).
$$

Remark 2.18 (The universal property of the direct sum). For any R-module N and any collection of R-linear maps $(f_k : M_k \longrightarrow N)_{k \in \mathcal{I}}$, there is a unique homomorphism $f \colon \bigoplus_{i \in \mathcal{I}} M_i \longrightarrow N$ such that the following diagrams commute for every $k \in \mathcal{I}$:

$$
\begin{array}{ccc}
M_k & \xrightarrow{\quad f_k \quad} & N \\
& \searrow{\scriptstyle j_k} \quad \nearrow{\scriptstyle f} & \\
& \bigoplus_{i \in \mathcal{I}} M_i &
\end{array}
$$

In other words,

$$
\operatorname{Hom}_R \left(\bigoplus_{i \in \mathcal{I}} M_i, N \right) \cong \bigtimes_{i \in \mathcal{I}} \operatorname{Hom}_R(M_i, N).
$$

If $R = \bigtimes_{i=1}^{n} R_i$ is the finite direct product of the rings R_i, then we have for each $i = 1, \ldots, n$ the following ideals of R:

$$
I_i := \{(0, \ldots, 0, a_i, 0, \ldots, 0) \ : \ a_i \in R_i\}.
$$

These are proper ideals if $n \geq 2$. Then R, as an R-module, is the direct sum of the ideals I_i. Conversely, given an R-module decomposition of R as

$$
R = I_1 \oplus \cdots \oplus I_n
$$

as a direct sum of ideals, we have

$$
R \cong R/J_1 \times \cdots \times R/J_n,
$$

where $J_k := \bigoplus_{i \neq k} I_i$.

2.5 Free Modules and Finitely Generated Modules

One should be careful that relation between matrices and endomorphisms of R-modules is not as good for modules as it is for vector spaces. This is because modules may have minimal generating sets which are not linearly independent, so R-modules may not have any basis. This means, in particular, that presenting elements as a linear combination of minimal generators is no longer unique. So, when defining homomorphisms, one cannot pick just any image for the minimal generators and extend by linearity.

Example 2.19. Let us take $R = \mathbb{K}[x, y]$ and the R-module $I = (x, y)$. This is not a free R-module. While $\{x, y\}$ is a minimal generating set, it is not linearly independent over R. This means in particular, we cannot define an R-linear map on I just by picking any images for x and y and then extend by linearity. For instance, if we want to define a map $f : I \longrightarrow I$ by $f(x) := y$ and $f(y) := x$ we would get by $\mathbb{K}[x, y]$-linearity

$$f(0) = f(y \cdot x - x \cdot y) = yf(x) - xf(y) = y^2 - x^2 \neq 0.$$

A **basis** of an R-module M is a set of generators $\{x_i\}_{i \in \mathcal{I}}$ of M which are linearly independent, i.e. any finite linear combination which gives zero must be trivial. An R-module M is a **free R-module** if it is isomorphic to $R^{\oplus \mathcal{I}}$ for some index set $\mathcal{I}$. Free modules are more similar to vector spaces, because they always have a basis: for the R-module $R^{\oplus \mathcal{I}}$ there is always the canonical basis $\{e_i \mid i \in \mathcal{I}\}$. In fact, for any R-module being free is equivalent to having a basis. This means, that for every R-module M and any family of elements $(m_i)_{i \in \mathcal{I}}$ from M, one can always define the R-linear map $\varphi : R^{\oplus \mathcal{I}} \longrightarrow M$ by setting $\varphi(e_i) := m_i$ and extending by linearity (Exercise: check that this works when there is a basis).

Remark 2.20. Let $r, s \in \mathbb{N}$. If there exists a surjective R-linear map $\varphi : R^r \longrightarrow R^s$, then $r \geq s$. In particular, $R^r \cong R^s$ if and only if $r = s$. Exercise: Can you also deduce that $r \leq s$ if φ is injective?

We can thus define the **rank of a free R-module** M as the unique r for which $M \cong R^r$. In particular,

$$\operatorname{rank} R^r := r.$$

The zero module is by convention free. Being free is a rather strong requirement as the next result should suggest.

Lemma 2.21. *Let R be a ring. An non-zero ideal $0 \neq I \subseteq R$ is free as an R-module if and only if I is a principal ideal generated by a non-zero-divisor.*

Proof. "$\Rightarrow$" Let $\varphi : R^n \longrightarrow I$ be the isomorphism which makes I a free R-module. If $n = 1$, then I is principal generated by $\varphi(1)$. If $\varphi(1)$ were a zero divisor, there would exist $r \neq 0$ in R such that $r \cdot \varphi(1) = \varphi(r) = 0$, a contradiction to the bijectivity of φ. If $n > 1$ denote by $f_i := \varphi(e_i)$. As φ is injective, $f_i \neq 0$ for all i, so in particular we have the element $x = (f_2, -f_1, 0, \ldots, 0) = f_2 \cdot e_1 - f_1 \cdot e_2 \neq 0$ of R^n with

$$\varphi(x) = f_2 f_1 - f_1 f_2 = 0,$$

a contradiction to the injectivity of φ.

"$\Leftarrow$" If $I = (a)$ is principal, then $\varphi : R \longrightarrow I$, given by $\varphi(r) := ra$ is surjective (always) and injective because a is a non-zero-divisor. $\qquad \square$

Proposition 2.22. *An R-module M is finitely generated if and only if M is isomorphic to some quotient of R^n for some $n \in \mathbb{N}$.*

Proof. "$\Rightarrow$" If $M = \langle x_1, \ldots, x_n \rangle$ then the map $\varphi : R^n \longrightarrow M$ defined by $\varphi(a_1, \ldots, a_n) := a_1 x_1 + \cdots + a_n x_n$ is R-linear and surjective, so $M \cong R^n / \ker(\varphi)$.
"$\Leftarrow$" Composing the canonical projection $R^n \longrightarrow R^n / N$ and the isomorphism $R^n / N \longrightarrow M$, we get a surjective map $\psi : R^n \longrightarrow M$, so $M = \langle \psi(e_1), \ldots, \psi(e_n) \rangle$. $\qquad \square$

Remark 2.23. If V is a finite dimensional vector space and $W \subseteq V$ a subspace, then $\dim(W) \leq \dim(V)$, with equality if and only if $W = V$. Modules in general do not behave this way, and this is not only because dimension is not defined, but it may happen that a submodule of a finitely generated module is no longer finitely generated: Take $R = \{f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Q}[x] \ : \ \forall \ n \in \mathbb{N} \text{ with } a_0 \in \mathbb{Z}\}$ and $I = \{f \in R \ : \ f(0) = 0\}$ (i.e. the constant term is zero). (Exercise: I is not a finitely generated R-module.)

2.6 The Cayley-Hamilton Theorem and the Nakayama Lemma

Recall from linear algebra, that for any commutative ring with identity, and for any $n \times n$-matrix $A \in \mathrm{Mat}_n(R)$ we can define the determinant $\det(A)$, and the **adjugate** $\mathrm{adj}(A)$ (or *classical adjoint*), which is defined as

$$\mathrm{adj}(A) = \left((-1)^{i+j} \det(A^{(ji)}) \right)_{i,j=1,\ldots,n},$$

where $A^{(ji)}$ is the submatrix of A obtained by deleting the jth row and the ith column. We have that

$$\mathrm{adj}(A) \cdot A = \det(A) \cdot I_n. \tag{2.1}$$

For the next result, we will be particularly interested in matrices with entries in the polynomial ring $R[t]$. The determinant is thus a polynomial in one variable t, which we will evaluate at some endomorphism[4] φ of some finitely generated R-module M. For any matrix $A \in \mathrm{Mat}_n(R)$, the characteristic polynomial of A is

$$\chi_A(t) = \det(tI_n - A) \in R[t].$$

While not every matrix defines an R-linear map, associating a matrix to a map which we *know* is R-linear is possible and enough to obtain a general Cayley-Hamilton Theorem for finitely generated R-modules, even if the association is not unique.

Theorem 2.24 (Cayley-Hamilton). *Let $M = \langle x_1, \ldots, x_n \rangle$ be finitely generated R-module and $\varphi \in \mathrm{End}_R(M)$. If $A \in \mathrm{Mat}_n(R)$ is a matrix such that $\varphi(x_i) = \sum_{j=1}^n a_{ij} x_j$ for all $i = 1, \ldots, n$, then $\chi_A(\varphi) = 0 \in \mathrm{End}_R(M)$.*

Proof. We are going to consider the matrix $B = tI_n - A \in \mathrm{Mat}_n(R[t])$. Using $\varphi \in \mathrm{End}_R(M)$, we can regard M as an $R[t]$-module, by setting $t \cdot x := \varphi(x), \ \forall \ x \in M$. So also M^n is an $R[x]$-module, and if we denote by $\mathbf{x} := (x_1, \ldots, x_n)^\top \in M^n$ the column vector with entries the generators of M, we have

$$B \cdot \mathbf{x} = 0.$$

If we multiply the relation above with $\mathrm{adj}(B)$ on the left, we get

$$(\mathrm{adj}(B) \cdot B) \cdot \mathbf{x} = (\det(B) \cdot I_n)\mathbf{x} = 0.$$

Thus $\det(B) \cdot x_i = 0, \ \forall \ i = 1, \ldots, n$, and this means $\det(B) \cdot M = 0$. As $\det(B) = \chi_A(t) \in R[t]$, the last equality is equivalent to $\chi_A(\varphi) = 0$. $\qquad\square$

Corollary 2.25. *Let $M = \langle x_1, \ldots, x_n \rangle$ be a finitely generated R-module and I an ideal of R.*

(a) *If φ is an R-module endomorphism of M such that $\varphi(M) \subseteq IM$, then there exist $a_0, \ldots, a_{n-1} \in I$ such that*

$$\varphi^n + a_{n-1} \varphi^{n-1} + \cdots + a_0 = 0.$$

(b) *If $IM = M$, then there exists $x \equiv 1 \mod I$ such that $xM = 0$.*

Proof.   (a) If $M = \langle x_1, \ldots, x_n \rangle$, then $y \in IM$ is equivalent to $y = \sum_{i=1}^n a_i x_i$ with $a_i \in I$. This means that the matrix in Theorem 2.24 can be chosen with entries in I, and we are done.

---

[4]The evaulation map $\mathrm{ev}_\varphi : R[t] \longrightarrow \mathrm{End}_R(M)$ is the unique ring homomoprhism with $t \mapsto \varphi$

(b) Just apply point (a) to the identity of M and choose $x = 1 + a_0 + \cdots + a_{n-1}$.

$\square$

Finite generation is used above to define the matrix. The next example shows that without it, the result may not hold.

Example 2.26. Consider the $\mathbb{Z}$-module $\mathbb{Q}$ and $I = (2)$. We have $(2)\mathbb{Q} = \mathbb{Q}$, but for any odd number $u \equiv 1 \mod 2$ we have $u\mathbb{Q} = \mathbb{Q}$.

There are some stronger conditions however which make the Nakayama Lemma hold even without finite generation (for example when I is nilpotent or in the graded setting).

Lemma 2.27 (Nakayama - version 1). *Let M be a finitely generated R-module and $I \subseteq \mathcal{J}_R$ and ideal contained in the Jacobson radical of R. If $IM = M$, then $M = 0$.*

Proof. By Corollary 2.25 part (b) there exists $x \equiv 1 \mod I$, so $x \equiv 1 \mod \mathcal{J}_R$, such that $xM = 0$. By Proposition 1.31 we have that x is invertible, so $M = x^{-1}(xM) = 0$. $\square$

Proof. (alternative) Suppose $M \neq 0$. Then it has a nonempty *minimal* finite set of generators: $\{x_1, \ldots, x_n\}$. Since $M = IM$, for each of them, so in particular for x_n we have $x_n = a_1 x_1 + \cdots + a_n x_n$. This implies

$$(1 - a_n)x_n = a_1 x_1 + \cdots + a_{n-1} x_{n-1}$$

As $a_n \in \mathcal{J}_R$, by Proposition 1.31 $1 - a_n$ is invertible, so $x_n \in \langle x_1, \ldots, x_{n-1} \rangle$, a contradiction to minimality. (For $n = 1$ we get $x_1 = 0$). $\square$

Corollary 2.28 (Nakayama - version 2). *Let M be a finitely generated R-module and $I \subseteq \mathcal{J}_R$ an ideal contained in the Jacobson radical of R, and $N \subseteq M$ a submodule of M. If $IM + N = M$, then $M = N$.*

Proof. Because $N \subseteq M$, we may consider the quotient module M/N. We show first a bit more than we need, namely that: $IM + N = M$ if and only if $I(M/N) = M/N$. The left-to-right-inclusion holds in both equalities, because $N \subseteq M$. So we just need to check the equivalence between the right-to-left-inclusions. Let $m \in M$ and $[m]_N$ denote the residue class modulo N. We have

$$
\begin{aligned}
m \in IM + N \quad &\Leftrightarrow \quad m = (\textstyle\sum a_k x_k) + n, \quad \text{with } a_k \in I, x_k \in M, n \in N \\
&\Leftrightarrow \quad [m]_N = [\textstyle\sum a_k x_k]_N \\
&\Leftrightarrow \quad [m]_N = \textstyle\sum a_k [x_k]_N \\
&\Leftrightarrow \quad [m]_N \in I(M/N).
\end{aligned}
$$

Since M is finitely generated, so is M/N. From $IM + N = M$ we get $I \cdot M/N = M/N$, and, because $I \subseteq \mathcal{J}_R$, we conclude by Lemma 2.27 that $M/N = 0$. This implies $M = N$.

$\square$

Proposition 2.29 (Nakayama - version 3). *Let M be a finitely generated R-module, let $I \subseteq \mathcal{J}_R$ be an ideal contained in the Jacobson radical of R, and let $p : M \longrightarrow M/IM$ be the canonical projection. If $p(x_1), \ldots, p(x_n)$ generate the R-module M/IM, then $x_1, \ldots, x_n$ generate M.*

Proof. Let $N = \langle x_1, \ldots, x_n \rangle \subseteq M$. Composing the canonical injection and the canonical projection:

$$N \xrightarrow{\ \iota\ } M \xrightarrow{\ \pi\ } M/IM$$

we obtain a homomorphism of R-modules which maps the generators of N onto the generators of M/IM, and is thus surjective. This means, for every $x \in M$, there exists $y \in N$ such that $x - y \in IM$, so $x \in N + IM$. As the other inclusion is always true, we get $M = N + IM$. Because $I \subseteq \mathcal{J}_R$ we conclude by Corollary 2.28. $\square$

Here is one rather practical consequence of the Nakayama Lemma. It shows one friendly aspect of finite dimensional vector spaces which still works for finitely generated modules.

Proposition 2.30. *Let M be a finitely generated R-module. If an endomorphism of M is surjective, then it is an isomorphism.*

Proof. Use the endomorphism φ to define an $R[t]$-module structure, with t acting as φ. Then take $I = (t)$, so we have $M = IM$ as $R[t]$-modules. Then there exists an element $x = 1 - tf(t)$ such that $xM = 0$. Then φ^{-1} will correspond to $f(t)$. $\qquad\square$

Corollary 2.31. *If $\{x_1, \ldots, x_n\}$ are generators of the free module R^n, then they are a basis.*

For endomorphisms of finite dimensional vector spaces we have injective $\Leftrightarrow$ surjective $\Leftrightarrow$ bijective. For finitely generated modules Proposition 2.30 is the best we can get: $\mathbb{Z} \longrightarrow \mathbb{Z}$ with $x \mapsto 2x$ is $\mathbb{Z}$-linear and injective but not bijective.

An important application of the Nakayama Lemma is the connection in brings with vector spaces in the local setting. For a local ring $(R, \mathfrak{m})$, denote by $\mathcal{K} = R/\mathfrak{m}$ the residue field. As $\mathfrak{m}$ annihilates $M/\mathfrak{m}M$, we have that $M/\mathfrak{m}M$ is a $R/\mathfrak{m}$-module, that is a $\mathcal{K}$-vector space. In particular, if M is a finitely generated $(R, \mathfrak{m})$-module, then $M/\mathfrak{m}M$ is a finite dimensional $\mathcal{K}$-vector space.

Proposition 2.32 (Nakayama for Local Rings)**.** *Let $(R, \mathfrak{m})$ be a local ring with residue field $\mathcal{K} = R/\mathfrak{m}$, and let $p : M \longrightarrow M/\mathfrak{m}M$ be the canonical projection. Then $\{p(x_1), \ldots, p(x_n)\}$ is a basis of the $\mathcal{K}$-vector space $M/\mathfrak{m}M$ if and only if $\{x_1, \ldots, x_n\}$ is a minimal set of generators for M.*

Proof. If $x_1, \ldots, x_n$ are generators of M then clearly $p(x_1), \ldots, p(x_n)$ are generators of $M/\mathfrak{m}M$ as an R-module, and, because scalars from $\mathfrak{m}$ multiply everything to zero in $M/\mathfrak{m}M$, they are $\mathcal{K}$-vs generators as well. In particular, if $x_1, \ldots, x_n$ are not minimal, then neither are $p(x_1), \ldots, p(x_n)$. This gives us "$\Leftarrow$" and the minimality in "$\Rightarrow$". The rest follows from Proposition 2.29, which we may use because R is local so $\mathfrak{m} = \mathcal{J}_R$. $\qquad\square$

2.6.1 Applications of Nakayama

Reading chronologically, one may not yet have all the definitions needed for the following statements. They may be repeated later in this text.

Proposition 2.33. *If $(R, \mathfrak{m})$ is a Noetherian local ring and if $\mathfrak{m}^{n+1} = \mathfrak{m}^n$, then $\mathfrak{m}^n = 0$.*
If R is an Noetherian integral domain and $\mathfrak{p} \subset R$ is a prime ideal, then all the powers $\mathfrak{p}^n$ with $n \geqslant 1\}$ are distinct.

Proof. The first statement is immediate consequence of the first version of Nakayama, with $I = \mathfrak{m}$ and $M = \mathfrak{m}^n$.

For the second statement, since R is a domain, all localization morphisms $R \longrightarrow R_{\mathfrak{p}}$ are injective. If $\mathfrak{p}^m = \mathfrak{p}^n$ for some $m > n$, then given the inclusions $\mathfrak{p}^m \subseteq \cdots \subseteq \mathfrak{p}^n$, we also obtain that $\mathfrak{p}^{n+1} = \mathfrak{p}^n$. We may then localize at $\mathfrak{p}$ and apply the first part to get $\mathfrak{p}^n = 0$. This is a contradiction, because R is a domain. $\qquad\square$

Proposition 2.34. *If $(R, \mathfrak{m})$ is a Noetherian local ring then $\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n = 0$.*
If R is a Noetherian integral domain and $\mathfrak{p} \subset R$ is a prime ideal, then $\bigcap_{n \in \mathbb{N}} \mathfrak{p}^n = 0$.

Proof. Write $J = \bigcap_{n \in \mathbb{N}} \mathfrak{m}^n$ and consider a primary decomposition of $\mathfrak{m}J = \bigcap Q_i$. We will show that $J = \mathfrak{m}J$, for which it is enough to show that $J \subseteq Q_i$ for all i. Let $x \in J \setminus Q_i$. If $\sqrt{Q_i} \neq \mathfrak{m}$, then there exists $y \in \mathfrak{m} \setminus \sqrt{Q_i}$. Then $xy \in \mathfrak{m}J \subseteq Q_i$, but $x \notin Q_i$ and $y \notin \sqrt{Q_i}$, which contradicts Q_i being primary. If $\sqrt{Q_i} = \mathfrak{m}$, then $J \subseteq \mathfrak{m}^n \subseteq Q_i$ for some n. In both cases we have shown $J \subseteq Q_i$.
For the second part, it is enough to localize just as in the previous proof. $\qquad\square$

Proposition 2.35. *A finitely generated projective module P over a local ring $(R, \mathfrak{m})$ is free.*

Proof. We can write $P \oplus Q = R^n$ for some F and n. We then have

$$P/\mathfrak{m}E \oplus Q/\mathfrak{m}Q = (R/\mathfrak{m})^n$$

as $\mathcal{K}$-vector spaces, with $\mathcal{K} = R/\mathfrak{m}$. We can choose $\mathcal{K}$-bases $\overline{x_1}, \ldots, \overline{x_r}$ and $\overline{y_1}, \ldots, \overline{y_s}$ for $P/\mathfrak{m}E$ and $Q/\mathfrak{m}Q$ respectively. This means $r + s = n$. By the third version of Nakayama we have that $x_1, \ldots, x_r$ and $y_1, \ldots, y_s$ generate E and F as R-modules. We will show that these are also R-bases.

We can write each x_i and y_j as a column vector from R^n and obtain an $n \times n$ matrix. Reducing this matrix modulo $\mathfrak{m}R^n$ these column vectors form a basis, hence the determinant is a unit in R. This means the $n \times n$ matrix is invertible over R, which means that the vectors x_i, y_j are linearly independent. $\qquad \square$

2.7 Exact Sequences

2.7.1 Some preliminaries

Recall, for an arbitrary category $\mathcal{C}$, a homomorphism f is an **epimorphism** if

$$g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2, \quad \forall g_1, g_2 \text{ homomorphisms,}$$

and it is a **monomorphism** if

$$f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2, \quad \forall g_1, g_2 \text{ homomorphisms.}$$

Epimorphisms and monomorphisms are categorical versions of surjection and injection. In any basic course you have (probably) seen that, in **Set**, being surjective is equivalent to being an epimporphism, and being injective is equivalent to being a monomorphism. This does not hold for arbitrary categories whose objects are structured and whose homomorphisms respect the structure.

Fix a ring R. In the category of R-modules epimorphisms and monomorphisms are equivalent to surjective R-linear maps, respectively injective R-linear maps (Exercise[5]).

Before we move on to exact sequences, we state one further consequence of the Universal Property of Quotient Modules (Theorem 2.10) which will turn out useful. From a formal point of view, it is often useful to think of the Cokernel not as given by equivalence classes, but as a module C together with an epimorphism $\pi : N \longrightarrow C$, such that $\pi \circ f = 0$, and which satisfies the following universal property.

Corollary 2.36 (The Universal Property of Cokernels)**.** *Let $f : M \longrightarrow N$ be an R-module homomorphism, and $\pi : N \longrightarrow \mathrm{Coker}(f) = N/\mathrm{Im}(f)$ the canonical projection. For every R-module P and every map $g : N \longrightarrow P$, with the property that $g \circ f = 0$ (i.e. $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$), there exists a unique map $\overline{\pi} : \mathrm{Coker}(f) \longrightarrow P$ such that $g = \overline{\pi} \circ \pi$, i.e. such that the following diagram commutes.*

$$M \xrightarrow{\ f\ } N \xrightarrow{\ \pi\ } \mathrm{Coker}(f)$$

Furthermore, this property uniquely determines the Cokernel of f.

Proof. This is an extra problem on Sheet 6. It is recommended you try to prove it on your own first.

The existence and uniqueness of $\overline{\pi}$ is directly implied by Theorem 2.10. To see that this property uniquely determines $\mathrm{Coker}(f)$, we use assume there exist two R-modules epimorphisms $\pi_1 : N \longrightarrow C_1$ and $\pi_2 : N \longrightarrow C_2$, with $\pi_1 \circ f = \pi_2 \circ f$ satisfying the universal property. We then get

$$\overline{\pi}_1 \circ \pi_1 = \pi_2 \quad \text{and} \quad \overline{\pi}_2 \circ \pi_2 = \pi_1.$$

---

[5] Hint: use the forgetful functor in one direction, and the cokernel, respectively the kernel for the other

2.7.2 Exact sequences

A sequence of R-modules and R-linear maps

$$\cdots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots \qquad (2.2)$$

is **exact at** M_i (or in position i) if $\operatorname{Im}(f_{i-1}) = \operatorname{Ker}(f_i)$. The whole sequence is exact if it exact at every M_i.

Remark 2.37. For any R-modules M, N, P we have

(a) $0 \longrightarrow M_1 \xrightarrow{f_1} M_2$ is exact $\iff f_1$ is injective.

(b) $M_1 \xrightarrow{f_1} M_2 \longrightarrow 0$ is exact $\iff f_1$ is surjective.

(c) $0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$ is exact $\iff M_1$ is canonically isomorphic to $\operatorname{ker}(f_2)$ (i.e., the isomorphism is induced by f_1.) This is because the injectivity of f_1 is equivalent to f_1 inducing an isomorphism $M_1 \cong \operatorname{Im}(f_1)$, and exactness at M_2 is equivalent to $\operatorname{Im}(f_1) = \operatorname{Ker}(f_2)$.

(d) $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$ is exact $\iff M_3$ is canonically isomorphic to $\operatorname{Coker}(f_1)$ (i.e., the isomorphism is induced by f_2.) This is because: the surjectivity of f_2 is equivalent to $M_3 = \operatorname{Im}(f_2)$, by the First Isomorphism Theorem 2.11 we have $\operatorname{Im}(f_2) \cong M_2/\operatorname{Ker}(f_2)$, and exactness at M_2 is equivalent to $M_2/\operatorname{Ker}(f_2) = M_2/\operatorname{Im}(f_1)$.

(e) $0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$ is exact $\iff f_1$ is injective, f_2 is surjective, and f_2 and f_1 induce a isomorphisms $\operatorname{Coker}(f_1) \cong M_3$ and $\operatorname{Ker}(f_2) \cong M_1$.

An exact sequence as in Remark 2.37(e) is called a **short exact sequence**. Any long exact sequence (2.2) can be split into short exact sequences. We have $\operatorname{Ker}(f_i) = \operatorname{Im}(f_{i-1}) \subseteq M_i$, and we can build.

$$0 \longrightarrow \operatorname{Ker}(f_i) \longrightarrow M_i \xrightarrow{f_i} \operatorname{Im}(f_i) \longrightarrow 0$$

So all these fit together as

$$(2.3)$$

Proposition 2.38. (a) *Let M_1, M_2, M_3 be R-modules and consider the sequence*

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0 \ . \tag{2.4}$$

The sequence (2.4) is exact, if and only if, for every R-module N, the sequence (2.5) below is exact:

$$0 \longrightarrow \mathrm{Hom}_R(M_3, N) \xrightarrow{f_2^*} \mathrm{Hom}_R(M_2, N) \xrightarrow{f_1^*} \mathrm{Hom}_R(M_1, N) \tag{2.5}$$

(b) *Let N_1, N_2, N_3 be R-modules and consider the sequence*

$$0 \longrightarrow N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} N_3 \ . \tag{2.6}$$

The sequence (2.4) is exact, if and only if, for every R-module M, the sequence (2.5) below is exact:

$$0 \longrightarrow \mathrm{Hom}_R(M, N_1) \xrightarrow{f_{1*}} \mathrm{Hom}_R(M, N_2) \xrightarrow{f_{2*}} \mathrm{Hom}_R(M, N_3) \tag{2.7}$$

Proof. (a) One can check exactness step by step, and in both directions. But it is more elegant to combine Remark 2.37 and the Universal Property of Cokernels. Then we get the following equivalent statements

- (2.4) is exact.
- f_2 induces an isomorphism $M_3 \cong \mathrm{Coker}(f_1)$.
- $\forall \, N$ and $\forall \, \varphi_2 : M_2 \longrightarrow N$ with $\varphi_2 \circ f_1 = 0$, there exists a unique $\overline{\varphi}_2 : M_3 \longrightarrow N$ with

$$\overline{\varphi}_2 \circ f_2 = \varphi.$$

- $\forall \, N$ and $\forall \, \varphi_2 \in \mathrm{Hom}_R(M_2, N)$ with $f_1^*(\varphi_2) = 0$, there exists a unique $\overline{\varphi}_2 \in \mathrm{Hom}_R(M_3, N)$ with

$$f_2^*(\overline{\varphi}_2) = \varphi.$$

- f_2^* induces an isomorphism $\mathrm{Hom}_R(M_3, N) \cong \mathrm{Ker}(f_1^*)$.
- (2.5) is exact.

(b) Works analogously.

$\square$

Lemma 2.39 (Snake Lemma)**.** *Every commutative diagram of R-modules with exact rows of the form*

$$
\begin{array}{ccccccc}
M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\
\downarrow{\gamma_1} & & \downarrow{\gamma_2} & & \downarrow{\gamma_3} & & \\
0 \longrightarrow & N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 &
\end{array}
$$

yields an exact sequence of kernels and cokernels of the vertical maps, which fit together as follows:

Furthermore, if f_1 is injective, then so is the restriction to $\mathrm{Ker}(\gamma_1)$ and if g_2 is surjective, then so is $\overline{g}_2$.

Proof. We only show how δ is defined. Let $x \in \mathrm{Ker}(\gamma_3)$, so $\gamma_3(x) = 0$. We are looking for an element in $\mathrm{Coker}(\gamma_1)$. Because f_2 is surjective, there exists an $x_2 \in M_2$ such that $f_2(x_2) = x$. By the commutativity of the diagram we have $g_2 \circ \gamma_2 = \gamma_3 \circ f_2$, so $g_2(\gamma_2(x_2)) = \gamma_3(f_2(x_2)) = \gamma_3(x) = 0$. So $\gamma_2(x_2) \in \mathrm{Ker}(g_2) = \mathrm{Im}(g_1)$, where the last equality is given by the exactness in the second row. So there exists an $y_1 \in N_1$ such that $g(y_1) = \gamma_2(x_2)$. We define

$$\delta(x) := \pi_1(y_1)$$

where $\pi_1 : N_1 \longrightarrow \mathrm{Coker}(\gamma_1)$ is the canonical projection. The verification that δ is well-defined, that the sequence

$$\mathrm{Ker}(\gamma_1) \xrightarrow{f_1} \mathrm{Ker}(\gamma_2) \xrightarrow{f_2} \mathrm{Ker}(\gamma_1) \xrightarrow{\delta} \mathrm{Coker}(\gamma_1) \xrightarrow{\overline{g}_1} \mathrm{Coker}(\gamma_1) \xrightarrow{\overline{g}_2} \mathrm{Ker}(\gamma_1)$$

is exact, the injectivity on the left when f_1 is injective and the surjectivity on the right when g_2 is surjective are left as an exercise. $\qquad\square$

We discuss now briefly one important application of exact sequences. Let $\mathcal{C}$ be a class of R-modules, and let λ be a function on $\mathcal{C}$ with values in $\mathbb{Z}$. For instance, if $R = \mathbb{K}$, consider the class $\mathcal{C}$ of finite dimensional $\mathbb{K}$-vector spaces, and λ to be the function which gives the dimension: $\lambda(V) := \dim_{\mathbb{K}}(V)$.

Definition 2.40. We say that λ is an **additive function** if for every short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ with M_i in $\mathcal{C}$, we have $\lambda(M_1) - \lambda(M_2) + \lambda(M_3) = 0$.

In the case of finite dimensional $\mathbb{K}$-vector spaces, the additivity of dimension was one of the key theorems of Linear Algebra. The next proposition shows that additivity extends to arbitrary long exact sequences.

Proposition 2.41. *Let $\mathcal{C}$ be a class of R-modules and λ an additive function on $\mathcal{C}$. For every exact sequence*
$$0 \longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} M_n \longrightarrow 0 \quad \text{of R-modules from $\mathcal{C}$, in which all kernels also belong to $\mathcal{C}$}$$
we have
$$\sum_{i=0}^{n}(-1)^i \lambda(M_i) = 0.$$

Proof. Split the long exact sequence as in (2.3), to obtain the short exact sequences

$$0 \to Ker(f_i) = \mathrm{Im}(f_{i-1}) \to M_i \to \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1}) \to 0$$

We now apply the additivity of λ to each short exact sequence to obtain

$$\lambda(\mathrm{Ker}(f_0)) - \lambda(M_0) + \lambda(\mathrm{Im}(f_0) = 0$$
$$\vdots$$
$$\lambda(\mathrm{Ker}(f_n)) - \lambda(M_0) + \lambda(\mathrm{Im}(f_n) = 0.$$

Taking an alternating sum, using $\mathrm{Ker}(f_0) = 0$ and $\mathrm{Im}(f_n) = 0$, and that $\lambda(0) = 0$ (which is a consequence of additivity) we obtain the desired equality. $\qquad\square$

2.8 The Tensor Product of Modules

Let M_1, M_2, N be three R-modules. A map $\varphi : M_1 \times M_2 \longrightarrow N$ is said to be a *R*-**bilinear map** if it is linear in each of the arguments, that is if
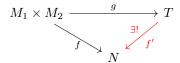
$$\varphi(rx_1 + sy_1, x_2) = r\varphi(x_1, x_2) + s\varphi(y_1, x_2)$$
$$\varphi(x_1, ux_2 + vy_2) = u\varphi(x_1, x_2) + v\varphi(x_1, y_2)$$

for all $r, s, u, v \in R$, und $x_i, y_i \in M_i$. Notice that $\varphi : M_1 \times M_2 \longrightarrow N$ is **not an R-module homomorphism**, but a map between sets with extra properties.

The goal of this section is to construct an R-module $M_1 \otimes_R M_2$ with the minimal number of relations to define a canonical bilinear map $M_1 \times M_2 \longrightarrow M_1 \otimes_R M_2$, such that every bilininear map from $M_1 \times M_2$ factors canonically through an R-module homomorphism defined on $M_1 \otimes_R M_2$. In other words, for every R-module N, there will be a one-to-one correspondence between R-bilinear maps $M_1 \times M_2 \longrightarrow N$ and R-module homomorphisms $M_1 \otimes_R M_2 \longrightarrow N$. To this aim, we first prove a proposition, which at the same time gives a construction of the tensor product.

Proposition 2.42. *Let M_1, M_2 be two R-modules. There exists a pair (T, g), where T is an R-module and g is an R-bilinear map $g : M_1 \times M_2 \longrightarrow T$, with the following property:*
For any R-module N and any R-bilinear map $f : M_1 \times M_2 \longrightarrow N$, there exists a unique R-module homomorphism $f' : T \longrightarrow N$ such that $f = f' \circ g$, i.e. such that the following diagram commutes:

$$
\begin{array}{ccc}
M_1 \times M_2 & \xrightarrow{\quad g \quad} & T \\
& \searrow_{f} \quad \swarrow_{\exists! \, f'} & \\
& N &
\end{array}
$$

Furthermore, if (T, g) and (T', g') both satisfy the above property, then there exists a unique isomorphism $j : T \longrightarrow T'$ such that $j \circ g = g'$.

Proof. Existence: Let C denote the free R-module $R^{\oplus(M_1 \times M_2)}$; that is C has a basis $\{e_{(x_1, x_2)} \; : \; (x_1, x_2) \in M_1 \times M_2\}$ indexed by all the elements of $M_1 \times M_2$. Every element of $c \in C$ is thus a finite linear combination of the form

$$c = \sum_{i=1}^{n} r_i e_{(x_{i_1}, x_{i_2})}, \quad \text{with } r_i \in R, \text{ and } x_{i_j} \in M_j.$$

Let D be the R-submodule of C generated by all elements of the form

$$
\begin{aligned}
&e_{(x_1 + y_1, x_2)} - e_{(x_1, x_2)} - e_{(y_1, x_2)} \\
&e_{(x_1, x_2 + y_2)} - e_{(x_1, x_2)} - e_{(x_1, y_2)} \\
&e_{(r x_1, x_2)} - r e_{(x_1, x_2)} \\
&e_{(x_1, r x_2)} - r e_{(x_1, x_2)}
\end{aligned}
$$

where $x_i, y_i \in M_i$ and $r \in R$. We define $T := C/D$ and denote by $x_1 \otimes x_2 := \pi(e_{(x_1, x_2)})$, where $\pi : C \longrightarrow C/D$ is the canonical projection. This means that $\{x_1 \otimes x_2 \; : \; x_i \in M_i\}$ is a generating set of T, and by construction we have

$$
\begin{aligned}
(x_1 + y_1) \otimes (x_2 + y_2) &= x_1 \otimes x_2 + x_1 \otimes y_2 + y_1 \otimes x_2 + y_1 \otimes y_2 \\
(r x_1) \otimes (s x_2) &= (rs) \cdot (x_1 \otimes x_2).
\end{aligned}
$$

This implies, that the map $g : M_1 \times M_2 \longrightarrow T$ defined by $g(x_1, x_2) := x_1 \otimes x_2$ is R-bilinear.

If N is an R-module, then any map $f : M_1 \times M_2 \longrightarrow N$ extends by linearity to an R-linear map $\overline{f} : C \longrightarrow P$, by sending $e_{(x_1, x_2)} \mapsto f(x_1, x_2)$. This means that if f is R-bilinear, then $\overline{f}(D) = 0$. By the universal property of the quotient module there exists an R-linear map $f' : T = C/D \longrightarrow N$ such that $f'(x_1 \otimes x_2) = f(x_1, x_2)$, that is such that the following diagram commutes:

$$
D \subseteq \operatorname{Ker}(\overline{f}) \quad \Rightarrow \quad
\begin{array}{ccc}
C & \xrightarrow{\quad \pi \quad} & T = C/D \\
& \searrow_{\overline{f}} \quad \downarrow_{\exists! \, f'} & \\
& N &
\end{array}
$$

Uniqueness: If (T, g) and (T', g') are two pairs we get the following diagram:

$$
\begin{array}{ccc}
M_1 \times M_2 & \xrightarrow{\;g\;} & T \;\circlearrowright\, \mathrm{id}_T \\
& \searrow\, g' \quad \scriptstyle j' \big\uparrow \big\downarrow j & \\
& & T' \;\circlearrowright\, \mathrm{id}'_T
\end{array}
$$

The uniqueness of the red maps, implies that j' and j are the isomorphisms we are looking for. $\qquad\square$

Analogously, for any positive integer $n \in \mathbb{N}_{>0}$ and any n R-modules $M_1, \ldots, M_n$ one may define R-multilinear maps from $M_1 \times \cdots \times M_n \longrightarrow N$, for any R-module N, and prove an analogue of Proposition 2.42 (cf. [AM69, Proposition 2.12*]).

Definition 2.43. Let M_1, M_2 be two R-modules. The unique R-module T from Proposition 2.42 is called the **tensor product** of the R-modules M_1 and M_2, and is denoted by $M_1 \otimes_R M_2$.

Let $n \in \mathbb{N}_{>0}$ and $M_1, \ldots, M_n$ be R-modules. The unique module T from analogue of Proposition 2.42, [AM69, Proposition 2.12*], is the tensor product of the R-modules $M_1, \ldots, M_n$ and is denoted by $M_1 \otimes_R \cdots \otimes_R M_n$.

Notice that we used as a definition for the tensor product its universal property, and not the explicit construction given in the proof of Proposition 2.42.

Remark 2.44. (a) If there is no ambiguity about R, or if R is not relevant in the discussion, then we write simply $M_1 \otimes M_2$ for $M_1 \otimes_R M_2$.

(b) The elements of $M_1 \otimes M_2$ are not only of the form $x_1 \otimes x_2$. Every element of $M_1 \otimes M_2$ may be expressed (usually in many ways as) a finite sum $\sum x_{1,i} \otimes x_{2,i}$. Furthermore, it is generally not trivial to decide if two different sums $\sum x_{1,i} \otimes x_{i_2}$ and $\sum x'_{1,j} \otimes x'_{2,j}$ are equal. Another consequence is that, if $\{x_{k,i}\}_{i \in \mathcal{I}_k}$ generate M_k, then $\{x_{1,i} \otimes x_{2,j} \;:\; (i,j) \in \mathcal{I}_1 \times \mathcal{I}_2\}$ generate $M_1 \otimes M_2$. Thus, if M_1 and M_2 are finitely generated, then so is $M_1 \otimes M_2$.

(c) $0 \otimes x = 0 \in M_1 \otimes M_2$.

(d) The notation $x_1 \otimes x_2$ is very ambiguous unless the tensor product to which it belongs is specified. For instance $2 \otimes [1]_2 = 2 \cdot (1 \otimes [1]_2) = 1 \otimes [2]_2 = 0 \in \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, but $2 \otimes [1]_2 \neq 0$ in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.

Lemma 2.45. *Let $x_{j,i} \in M_j$, with $j = 1,2$ and $i = 1, \ldots, n$, such that $\sum_{i=1}^{n} x_{1,i} \otimes x_{2,i} = 0 \in M_1 \otimes M_2$. Then, there exist finitely generated submodules $M'_j \subseteq M_j$ such that $\sum_{i=1}^{n} x_{1,i} \otimes x_{2,i} = 0 \in M'_1 \otimes M'_2$.*

Proof. If $\sum_{i=1}^{n} x_{1,i} \otimes x_{2,i} = 0 \in M_1 \otimes M_2$, then, using the notation from the proof or Proposition 2.42, we have $\sum_{i=1}^{n} e_{(x_{1,i}, x_{2,i})} \in D$. In particular, $\sum_{i=1}^{n} e_{(x_{1,i}, x_{2,i})}$ is a finite sum of generators of D. For $j = 1, 2$, take M'_j to be the submodule generated by the $x_{j,i}$ and by the finitely many elements which appear as in the jth coordinate in these generators of D. This means, that $\sum_{i=1}^{n} x_{1,i} \otimes x_{2,i} = 0 \in M'_1 \otimes M'_2$. $\qquad\square$

The most important aspect about the tensor product is not its construction, but its defining universal property, as well as the rules for handling the $x_1 \otimes x_2$. The following can also be seen as standard properties of the tensor product, and are given by so-called canonical isomorphisms.

Proposition 2.46. *Let M_1, M_2, M_3, M be R-modules. There exist unique isomorphisms:*

(a) $M_1 \otimes M_2 \longrightarrow M_2 \otimes M_1$ *such that*

$$x_1 \otimes x_2 \mapsto x_2 \otimes x_1.$$

(b) $(M_1 \otimes M_2) \otimes M_3 \longrightarrow M_1 \otimes (M_2 \otimes M_3) \longrightarrow M_1 \otimes M_2 \otimes M_3$ *such that*

$$(x_1 \otimes x_2) \otimes x_3 \mapsto x_1 \otimes (x_2 \otimes x_3) \mapsto x_1 \otimes x_2 \otimes x_3.$$

(c) $R \otimes_R M \longrightarrow M$ *such that*

$$r \otimes x \mapsto rx.$$

(d) $(M_1 \oplus M_2) \otimes M_3 \longrightarrow (M_1 \otimes M_3) \oplus (M_2 \otimes M_3)$ *such that*

$$(x_1, x_2) \otimes x_3 \mapsto (x_1 \otimes x_3, x_2 \otimes x_3).$$

(e) *In general, for any family* $(M_i)_{i \in \mathcal{I}}$ *of R-modules and any R-module M, we have*

$$M \otimes (\bigoplus_{i \in \mathcal{I}} M_i) \cong \bigoplus_{i \in \mathcal{I}} (M \otimes M_i),$$

but this does not hold in general for arbitrary direct products.

Proof. The trick in all cases is to define a bilinear map, and then use the UP from Proposition 2.42 to construct the isomorphism. We will show here only how the isomorphism $f : (M_1 \otimes M_2) \otimes M_3 \longrightarrow M_1 \otimes M_2 \otimes M_3$, with $f((x_1 \otimes x_2) \otimes x_3) = x_1 \otimes x_2 \otimes x_3$ is constructed. For this, fix first $x_3 \in M_3$, and define the map $f'_{x_3} : M_1 \times M_2 \longrightarrow M_1 \otimes M_2 \otimes M_3$ by sending $(x_1, x_2) \mapsto x_1 \otimes x_2 \otimes x_3$. This is clearly bilinear, so it induces therefore a unique homomorphism of R-modules $f_3 : M_1 \otimes M_2 \longrightarrow M_1 \otimes M_2 \otimes M_3$. Now consider the map $f' : (M_1 \otimes M_2) \times M_3 \longrightarrow M_1 \otimes M_2 \otimes M_3$ given by $(y, x_3) \mapsto f_{x_3}(y)$, where $y \in M_1 \otimes M_2$. This is again bilinear, and induces the desired R-module homomorphism f. To construct the inverse of f, one can start directly with the multilinear map $g' : M_1 \times M_2 \times M_3 \to (M_1 \otimes M_2) \otimes M_3$ with $g'(x_1, x_2, x_3) = (x_1 \otimes x_2) \otimes x_3$, which induces the inverse of f. $\square$

An immediate consequence of the above isomorphisms is that for any free R-module $R^{\oplus \mathcal{I}}$ we have

$$R^{\oplus \mathcal{I}} \otimes_R M \cong M^{\oplus \mathcal{I}}.$$

Remark 2.47. If R, S are two rings, an (R,S)-**bimodule** M is simultaneously an R-module and an S-module, in such a way that the two scalar multiplications are compatible[6]: $r(xs) = (rx)s$, for all $r \in R$, $x \in M$, $s \in S$. Let M_1 be an R-module, M_2 be an (R, S)-bimodule, and M_3 be an S-module. Then $M_1 \otimes_R M_2$ has a natural structure of S-module, by setting $(x_1 \otimes x_2)s := x_1 \otimes x_2 s$. Similarly, $M_2 \otimes_S M_3$ is an R-module. We have

$$(M_1 \otimes_R M_2) \otimes_S M_3 \cong M_1 \otimes_R (M_2 \otimes_S M_3).$$

2.8.1 Restriction and Extension of Scalars

Throughout this subsection, fix a ring-homomorphism $f : R \longrightarrow S$.

An S-module N has a natural structure of R-modules defined by

$$ry := f(r)y, \quad \forall\, r \in R, y \in N.$$

This R-module N is said to be obtained from the S-module N by **restriction of scalars** (via f). In particular, S is an R-module via f.

Proposition 2.48. *With the above assumptions, if N is a finitely generated S-module and S is a finitely generated R-module, then the R-module N obtained by restriction of scalars is finitely generated.*

Proof. If $\mathrm{Span}_S(y_1, \ldots, y_n) = N$, and $\mathrm{Span}_R(x_1, \ldots, x_m) = S$, then $\mathrm{Span}_R(x_i y_j\ :\ i = 1, \ldots, m\ \ j = 1, \ldots, n) = N$. $\square$

---

[6]Note that we may not have a way to multiply elements from R and from S.

Let M be an R-module. Since S is also an R-module, we can define the R-module

$$M_S := S \otimes_R M.$$

Furthermore, we can define an S-module structure on M_S by setting:

$$s(s' \otimes x) := ss' \otimes x, \quad \forall \, s, s' \in S, x \in M.$$

The S-module M_S is said to be obtained from the R-module M by **extension of scalars** (via f).

Proposition 2.49. *If M is a finitely generated R-module, then M_S is a finitely generated S-module.*

Proof. If $\mathrm{Span}_R(x_1, \ldots, x_m) = M$, then $\mathrm{Span}_S(1 \otimes x_1, \ldots, 1 \otimes x_m) = M_B$. $\qquad\qquad\square$

2.8.2   The Tensor Product as a Functor

Let M_1, M_2, N_1, N_2 be R-modules, and $f_i : M_i \longrightarrow N_i$ be R-linear maps. Define $f : M_1 \times M_2 \longrightarrow N_1 \otimes N_2$ by

$$f(x_1, x_2) := f_1(x_1) \otimes f_2(x_2).$$

Clearly f is R-bilinear, so we obtain an R-linear map $f_1 \otimes f_2 : M_1 \otimes M_2 \longrightarrow N_1 \otimes N_2$, given by

$$(f_1 \otimes f_2)(x_1 \otimes x_2) = f_1(x_1) \otimes f_2(x_2), \quad \forall x_i \in M_i.$$

If $g_i : N_i \longrightarrow P_i$, for $i = 1, 2$, are two more R-linear maps, then

$$(g_1 \circ f_1) \otimes (g_2 \circ f_2) = (g_1 \otimes g_2) \circ (f_1 \otimes f_2).$$

It is enough to verify what happens with elements of the form $(x_1 \otimes x_2) \in M_1 \otimes M_2$, which generate $M_1 \otimes M_2$, and this is an easy check. So, for any R-module N, we have that $- \otimes_R N$ defines a functor from the category of R-modules to itself. We will now see that this functor is left-adjoint to the functor $\mathrm{Hom}_R(N, -)$:

The module $M_1 \otimes_R M_2$ was constructed so that, for any R-module N, there is a one-to-one correspondence between

$$\mathrm{Hom}_R(M_1 \otimes_R M_2, N) \leftrightarrow B := \{f : M_1 \times M_2 \longrightarrow N \mid R - \text{bilinear}\}.$$

On the other hand, for any $f : M_1 \times M_2 \longrightarrow N$, and any $x_1 \in M_1$, the map $f(x_1, \bullet) : M_2 \longrightarrow N$, with $x_2 \mapsto f(x_1, x_2)$ is R-linear, i.e. $f(x_1, \bullet) \in \mathrm{Hom}_R(M_2, N)$. So, since f is linear in x_1, and $\mathrm{Hom}_R(M_2, N)$ is an R-module, we have that f defines an element from $\mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, N))$. Conversely, for every $\varphi \in \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, N))$, we can define an R-bilinear map

$$(x_1, x_2) \mapsto (\varphi(x_1))(x_2),$$

which gives one-to-one correspondence. We have thus a canonical isomoprhism

$$Hom_R(M_1 \otimes M_2, N) \cong \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M_2, N)). \tag{2.8}$$

The next proposition will show that the functor $- \otimes_R N$ is right exact.

Proposition 2.50. *Let $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ be an exact sequence of R-modules, and N be any R-module. Then, the following sequence is also exact:*

$$M_1 \otimes N \xrightarrow{f_1 \otimes \mathrm{id}_N} M_2 \otimes N \xrightarrow{f_2 \otimes \mathrm{id}_N} M_3 \otimes N \longrightarrow 0$$

Proof. Since $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ is exact, by Proposition 2.38 we have that, for any R-module P, the sequence

$$0 \longrightarrow \operatorname{Hom}_R(M_3, \operatorname{Hom}_R(N, P)) \xrightarrow{\overline{f_2}} \operatorname{Hom}_R(M_2, \operatorname{Hom}_R(N, P)) \xrightarrow{\overline{f_1}} \operatorname{Hom}_R(M_1, \operatorname{Hom}_R(N, P))$$

is also exact. By (2.8) we get that the exact sequence

$$0 \longrightarrow \operatorname{Hom}_R(M_3 \otimes N, P) \xrightarrow{\overline{f_2 \otimes \operatorname{id}_N}} \operatorname{Hom}_R(M_2 \otimes N, P) \xrightarrow{\overline{f_1 \otimes \operatorname{id}_N}} \operatorname{Hom}_R(M_1 \otimes N, P)$$

is exact, which, again by Proposition 2.38, is equivalent to our claim. $\square$

In general, the functor $- \otimes_R N$ is not exact. That is, if $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$ is exact, it does not imply in general that $M_1 \otimes N \xrightarrow{f_1 \otimes \operatorname{id}_N} M_2 \otimes N \xrightarrow{f_2 \otimes \operatorname{id}_N} M_3 \otimes N$ is exact. Here is a counterexample.

Example 2.51. Let $R = \mathbb{Z}$ and $0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}$ be the exact sequence given by the multiplication with 2. If we tensor with $N = \mathbb{Z}/2\mathbb{Z}$, then we obtain $0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/2\mathbb{Z}$ which is no longer exact.

2.8.3 Flat Modules

An R-module N is **flat** if the functor $- \otimes_R N$ is exact, that is if for any exact sequence of R-modules $\ldots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \ldots$, the sequence

$$\ldots \longrightarrow M_{i-1} \otimes_R N \xrightarrow{f_{i-1} \otimes \operatorname{id}_N} M_i \otimes_R N \xrightarrow{f_i \otimes \operatorname{id}_N} M_{i+1} \otimes N \xrightarrow{f_{i+1} \otimes \operatorname{id}_N} \ldots$$

is also exact.

Proposition 2.52. *Let R be a ring and N an R-module. The following are equivalent.*

(a) *N is flat.*

(b) *Every short exact sequence of R-modules stays exact after tensoring with N.*

(c) *If for every injective homomorphism of R modules $f : M_1 \longrightarrow M_2$, the homomorphism $f \otimes \operatorname{id}_N : M_1 \otimes N \longrightarrow M_2 \otimes N$ is also injective.*

(d) *If for every injective homomorphism between finitely generated R modules $f : M_1 \longrightarrow M_2$, the homomorphism $f \otimes \operatorname{id}_N : M_1 \otimes N \longrightarrow M_2 \otimes N$ is also injective.*

Proof. (a)$\Leftrightarrow$(b) follows from splitting long exact sequences into short ones 2.3.
(b)$\Leftrightarrow$(c) follows from Proposition 2.50.
(c)$\Rightarrow$(d) is trivial.
(d)$\Rightarrow$(c) follows from Lemma 2.45: Let $u = \sum_{i=1}^n x_i \otimes y_i \in M_1 \otimes N$ with $(f \otimes \operatorname{id}_N)(u) = 0$, which means $\sum_{i=1}^n f(x_i) \otimes y_i = 0 \in M_2 \otimes N$. Define $M_1' := \langle x_1, \ldots, x_n \rangle$ and define M_2' as the finitely generated R-module of M_2 constructed in the proof of Lemma 2.45 such that $\sum_{i=1}^n f(x_i) \otimes y_i = 0 \in M_2' \otimes N$. Notice that M_2' contains $f(M_1')$, and that the restriction of f is still injective: $f' : M_1' \longrightarrow M_2'$. So we have $f' \otimes \operatorname{id}_N(u) = 0$, which by (d) implies that $u = 0 \in M_1' \otimes N$ so $u = 0 \in M_1 \otimes N$. $\square$

Remark 2.53. If $f : R \longrightarrow S$ is a ring homomorphism and N is a flat R-module, then $N_S = S \otimes_R N$ is a flat S-module. Indeed, let $f : M_1 \longrightarrow M_2$ be an injective homomorphisms of S-modules. Then

$$f \otimes \operatorname{id}_{N_S} N : M_1 \otimes_S (S \otimes_R N) \longrightarrow M_2 \otimes_S (S \otimes_R N)$$

which is equivalent by Remark 2.47 to

$$f \otimes \mathrm{id}_S \otimes \mathrm{id}_N : (M_1 \otimes_S S) \otimes_R N \longrightarrow (M_2 \otimes_S S) \otimes_R N$$

and by Proposition 2.46 part (c) to

$$f \otimes \mathrm{id}_N N : M_1 \otimes_R N \longrightarrow M_2 \otimes_R N.$$

2.8.4 Tensor Product of Algebras

An R-algebra $R \xrightarrow{\varphi} S$ is automatically an R-module with $r \cdot s := \varphi(r) \cdot s$. One could say, that an R-algebra is an R-module which has a ring structure compatible with the R-module structure. In particular, if $R = \mathbb{K}$ is a field, then any $\varphi : \mathbb{K} \longrightarrow S$ must be injective, so a $\mathbb{K}$ is isomorphic to a subring of S. Furthermore, just as every Abelian group is a $\mathbb{Z}$-module, every ring (commutative with 1) is a $\mathbb{Z}$-algebra. Any R-algebra homomorphism (cf. (1.2)) is a ring homomorphism which is also an R-linear map.

Definition 2.54. Let $\varphi : R \longrightarrow S$ be a ring homomorphism. The homomorphism φ and the R-algebra S are both called **finite** if S is a finitely generated R-module (via the structure given by φ).
The homomorphism φ is of **finite type** and S is a **finitely generated R-algebra** if there exists a finite set $\{s_1, \ldots, s_n\} \subseteq S$ such that every element of S can be written as the evaluation at $(s_1, \ldots, s_n)$ of a polynomial in n variables with coefficients[7] in $\varphi(R)$; equivalently, if there exists a surjective R-algebra homomorphism $R[x_1, \ldots, x_n] \longrightarrow S$.
We say that R is a **finitely generated ring** if it is a finitely generated $\mathbb{Z}$-algebra.

Let $R \xrightarrow{\varphi_1} S_1$ and $R \xrightarrow{\varphi_2} S_2$ be two R-algebras. The tensor product of the R-modules $T = S_1 \otimes_R S_2$ also has an R-algebra structure given by

$$(s_1 \otimes s_2)(s_1' \otimes s_2') := (s_1 s_1') \otimes (s_2 s_2'). \tag{2.9}$$

One still needs to check that this can be extended linearly to T and that is it gives an R-bilinear map $\mu : T \times T \longrightarrow T$. To check this, consider the map from $S_1 \times S_2 \times S_1 \times S_2$ to T given by

$$(s_1, s_2, s_1', s_2') \mapsto (s_1 s_1') \otimes (s_2 s_2').$$

This is easy to check to be R-multilinear, so, by the UP of the tensor product we get an R-linear map from $S_1 \otimes S_2 \otimes S_1 \otimes S_2$ to T. Using the "associativity" of the tensor product, we get an R-linear map $T \otimes T \longrightarrow T$, which corresponds exactly to the map $T \times T \longrightarrow T$ given in (2.9). So we can say that

$$\left(\sum_i (s_{1i} \otimes s_{2i}) \right) \left(\sum_j (s_{1j}' \otimes s_{2j}') \right) = \sum_{ij} (s_{1i} s_{1j}') \otimes (s_{2i} s_{2j}').$$

It is an easy check to see that this turns $T = S_1 \otimes_R S_2$ into a ring, with identity $1 \otimes 1$. Furthermore, $S_1 \otimes_R S_2$ we have the following commutative diagram

where $u_1(s_1) := s_1 \otimes 1$ and $u_2(s_2) := 1 \otimes s_2$.

---
[7]while $\varphi(R)$ is not a ring, we may still consider only polynomials with coefficients in $\varphi(R)$.

Chapter 3

Rings and Modules of Fractions

The motivation behind the notions introduced in this chapter is geometric. The methods we will develop shape up to one of the most powerful tools in commutative algebra: localization. The idea was to find a way to look at arbitrarily small Zariski-neighborhoods of a point p on an algebraic set X. Such neighborhoods are obtained by removing from X large algebraic sets Y which do not contain p. The largest such sets are given thus by a polynomial f not vanishing at p, and in order to give these sets an algebraic structure one has to invert f. You are strongly encouraged to read the introduction to Chapter 2 in Eisenbud's book [**?**][p.57-59] for more on the history and the motivation.

3.1 Definitions and First Properties

What we will practically do is generalize the definition of fractions to arbitrary rings and modules, using as a prototype the construction of the field of rational numbers starting from the integers. Rational numbers can be interpreted as equivalence classes of pairs of integers $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus 0)$. So $(a, b) \equiv (c, d) \iff \frac{a}{b} = \frac{c}{d} \iff ad - bc = 0$. Transitivity in this case is proven as follows: If $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$, then

$$
\begin{aligned}
ad - bc &= 0 \\
cf - de &= 0.
\end{aligned}
$$

Multiplying the first equation with f and the scond with b and subtracting, we get $adf - bde = d(af - be) = 0$, which implies $af - be = 0$ because d is a nonzero divisor. In particular, we cannot extend this definition ad literam if the ring is not an integral domain. The way to overcome this is the following.

Definition 3.1. Let R be a ring. A **multiplicatively closed set** is a subset $U \subseteq R$ closed under taking products, including empty products. That is U has to satisfy:

    i. $1 \in U$

    ii. for all $x, y \in U$ we have $xy \in U$.

These will be the sets of denominators. Notice that, contrary to what you learned in school, we do not prohibit $0 \in U$. The point is, that if $0 \in U$ we get the zero ring, which is allowed (but while not very useful to do). The properties of multiplicatively closed sets will be needed to provide a ring structure on the fractions, as well as to prove transitivity of the following binary relation.

Definition 3.2. Let R be a ring and $U \subseteq R$ a multiplicatively closed set. Define the binary relation $\equiv$ on $R \times U$ as follows:

$$(a, s) \equiv (b, t) \iff \exists u \in U \text{ such that } u(at - bs) = 0.$$

Remark 3.3. The above binary relation is an equivalence relation on $R \times U$. It is obviously reflexive and it is symmetric because the ring is commutative. To check transitivity, let $(a, s) \equiv (b, t)$ and $(b, t) \equiv (c, v)$. So there exist $u, w \in U$ such that

$$
\begin{aligned}
u(at - bs) &= 0 \\
w(bv - ct) &= 0.
\end{aligned}
$$

Multiplying the first equation with vw and the second with us, then add the two to obtain

$$ uwt(av - cs) = 0, $$

which, because $u, w, t \in U$, so $uwt \in U$, is equivalent to $(a, s) \equiv (c, v)$.

We will denote the equivalence class of (a, s) with $\frac{a}{s}$, and we will denote by $U^{-1}R$ the set of equivalence classes.

Definition 3.4. The set equivalence classes $U^{-1}R$ has a ring structure with the operations:

$$
\begin{aligned}
\frac{a}{s} + \frac{b}{t} &:= \frac{at + bs}{st} \\
\frac{a}{s} \cdot \frac{b}{t} &:= \frac{ab}{st}
\end{aligned}
$$

The check that this definition does not depend on the representatives and the check of the ring axioms are elementary. The zero will be $\frac{0}{s}$ and the one will be $\frac{1}{1}$. Notice that closure under multiplication and $1 \in U$ are essential for this. The ring $U^{-1}R$ is called the **ring of fractions** of R with respect to U.

Remark 3.5. We have

(a) $\frac{s}{s} = \frac{1}{1}$, for all $s \in U$.

(b) If $s, t \in U$ then $\frac{s}{t}$ is a unit, with $(\frac{s}{t})^{-1} = \frac{t}{s}$.

(c) If $f : R \longrightarrow U^{-1}R$, then every element in $U^{-1}R$ is of the form $f(a)f(s)^{-1}$ with $s \in U$, thus for every $s \in U$, $f(s)$ is a unit.

(d) $U^{-1}R = 0 \iff 0 \in U$.

(e) If $0 \notin U$, and if $s, t \in R \setminus 0$ with $s \in U$ and $st = 0$, then $t \notin U$.

(f) $\frac{0}{s} = \frac{0}{t}$ for all $s, t \in U$.

(g) If $\frac{a}{s} = 0$, then there exists $t \in U$ such that $at = 0$. In particular, if R is a domain and $0 \notin U$, then $\frac{a}{s} = \frac{0}{t} = 0$ implies $a = 0$.

(h) The other way around, if $s \in U$ is a zero divisor, then for every $t \in R$ with $ts = 0$ we have $\frac{t}{1} = 0 \in U^{-1}R$. This is what needs to happen in order to consistently turn all the elements in U into units in $U^{-1}R$.

Remark 3.6. We have a canonical ring homomorphism $f : R \longrightarrow U^{-1}R$ given by $f(a) := \frac{a}{1}$. Notice that this is not always injective.

Examples. 1. If R is a domain, then $U = R \setminus \{0\}$ is a multiplicatively closed. In this case, $U^{-1}R$ is a field, called the field of fractions.

2. For $f \in R$, the set $U = \{f^n\}_{n \in \mathbb{N}}$ is a multiplicatively closed set. In this case, we denote the ring of fractions by $R_f := U^{-1}R$.

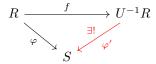3. For any ideal $I \subseteq R$, the set $1 + I = \{1 + a \ : \ a \in I\}$ is a multiplicatively closed set.

4. Taking $U = \{\text{nonzero divisors in } R\} \subseteq R$ is a multiplicatively closed set. In this case, the ring $U^{-1}R$ is called the **total quotient ring** or R, and it is the biggest quotient ring of R such that $f : R \longrightarrow U^{-1}R$ is an injection.

5. For any ideal $\mathfrak{p} \subseteq R$ we have

$$U := R \setminus \mathfrak{p} \text{ is multiplicatively closed} \iff \mathfrak{p} \in \operatorname{Spec}(R).$$

In this case we denote by $R_{\mathfrak{p}} := U^{-1}R$ and call this ring the **localization** of R at $\mathfrak{p}$. We use this name because $\{\frac{a}{s} \mid a \in \mathfrak{p}\}$ is the unique maximal ideal of $R_{\mathfrak{p}}$, so $R_{\mathfrak{p}}$ is a local ring : If $b \notin \mathfrak{p}$, then $b \in U$, so $\frac{b}{t}$ is a unit.

6. If $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$ then $\mathbb{Z}_{(p)}$ is the ring of all rational numbers $\frac{m}{n}$ with m, n coprime and p does not divide n.

7. If $f \in \mathbb{Z}$ is some integer, then $\mathbb{Z}_f$ is the ring of all rational numbers which can be written with denominator a power of f.

8. Local rings in algebraic geometry.

Proposition 3.7 (The Universal Property of the Ring of Fractions). *Let R be a ring, $U \subseteq R$ a multiplicatively closed set, $f : R \longrightarrow U^{-1}R$ the canonical homomorphism. For any ring homomorphism $\varphi : R \longrightarrow S$ such that $\varphi(U) \subseteq S^{\times}$, there exists a unique ring homomorphism $\varphi' : U^{-1}R \longrightarrow S$ such that $\varphi' \circ f = \varphi$, that is such that the following diagram commutes:*

$$
\begin{array}{ccc}
R & \xrightarrow{\quad f \quad} & U^{-1}R \\
& {\scriptstyle \varphi} \searrow & \downarrow {\scriptstyle \varphi'} \\
& & S
\end{array}
$$

Furthermore, this property uniquely determines $U^{-1}R$, that is if R' is another ring with $g : R \longrightarrow R'$ satisfying $g(U) \subseteq (R')^{\times}$ and the above universal property, then there exists a unique isomorphism $\psi : U^{-1}R \longrightarrow R'$ such that $\psi \circ f = g$.

Proof. Existence of φ': We define $\varphi'(\frac{a}{s}) := \varphi(a) \cdot \varphi(s)^{-1}$. This is allowed if and only if $\varphi(U) \subseteq S^{\times}$. The compatibility with the ring structure is immediate, as long as the map is well defined, i.e. independent of the choice of representative. Let thus $\frac{a}{s} = \frac{a'}{s'}$. Then, there exists $t \in U$ such that $t(as' - a's) = 0$. Applying φ to the equation we get

$$\varphi(t)\Big(\varphi(a)\varphi(s') - \varphi(a')\varphi(s)\Big) = 0$$

which, as $\varphi(t)$ is a unit, implies $\varphi(a)\varphi(s)^{-1} = \varphi(a')\varphi(s')^{-1}$.

Uniqueness of φ': For any ring homomorphism φ' satisfying $\varphi = \varphi' \circ f$, we must have $\varphi'(\frac{a}{1}) = \varphi'(f(a)) = \varphi(a)$, for every $a \in R$. Hence, again because we have a homomorphism, $\varphi'(\frac{1}{s}) = \varphi'((\frac{s}{1})^{-1}) = (\varphi'(\frac{s}{1}))^{-1} = \varphi(s)^{-1}$ whenever $s \in U$. Combining the two, we conclude that any ring homomorphism with the required property must send $\frac{a}{s}$ to $\varphi(a)\varphi(s)^{-1}$.

Universality of $U^{-1}R$: Follows exactly as in Proposition 2.42. $\qquad\square$

Corollary 3.8. *An immediate consequence of the above proposition is the following:*

$$U^{-1}R \cong R \iff U \subseteq R^{\times}.$$

We thus have for the canonical homomorphism $f : R \longrightarrow U^{-1}R$ the following properties:

(i) $f(U) \subseteq (U^{-1}R)^{\times}$,

(ii) $f(a) = 0$ if and only if there exists $s \in U$ with $as = 0$,

(iii) every element of $U^{-1}R$ is of the form $f(a) \cdot (f(s))^{-1}$.

These properties uniquely determine the ring of fractions of R with respect to U, as the next statement shows.

Corollary 3.9. *If $g : R \longrightarrow R'$ is another ring homomorphism with*

(i) *$g(U) \subseteq (R')^\times$,*

(ii) *$g(a) = 0$ if and only if there exists $s \in U$ with $as = 0$,*

(iii) *every element of R' is of the form $g(a) \cdot (g(s))^{-1}$,*

then there exists a unique isomorphism $\psi : U^{-1}R \longrightarrow R'$ such that $\psi \circ f = g$.

Proof. The ring homomorphism ψ is given by the Universal Property 3.7 and thus works as $\psi(\frac{a}{b}) = g(a)(g(b))^{-1}$. Surjectivity is given by (iii), and injectivity follows from Remark 3.5) 3.5 and (ii). $\qquad\square$

For any multiplicatively closed set $U \subseteq R$ we can extend the definition of fractions to any R-module M, by defining the binary relation $\equiv$ on $M \times U$ as

$$(m, s) \equiv (n, t) \iff \exists \, u \in U \text{ such that } u(mt - ns) = 0.$$

Similarly to fractions for rings, we denote the equivalence classes as $\frac{m}{s}$, define addition as

$$\frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'}, \quad \forall \, m, m' \in M \text{ and } s, s' \in U$$

and scalar multiplication as

$$\frac{r}{t} \cdot \frac{m}{s} := \frac{rm}{st}, \quad \forall \, r \in R, m \in M, s, t \in U.$$

This turns $U^{-1}M$ into an $U^{-1}R$-module, and thus through $f : R \longrightarrow U^{-1}R$ into an R-module as well. For the special cases in which $U = R \setminus \mathfrak{p}$, respectively $U = \{f^n\}_{n \in \mathbb{N}}$ we write $M_{\mathfrak{p}}$, respectively M_f.

3.2 Functoriality

Given an R-module homomorphism $\varphi : M \longrightarrow N$, and a multiplicatively closed set U we have an $U^{-1}R$-module homomorphism

$$U^{-1}M \xrightarrow{\;U^{-1}\varphi\;} U^{-1}N$$

$$\frac{m}{s} \longmapsto \frac{\varphi(m)}{s}$$

Obviously $U^{-1}\,\mathrm{id}_M = \mathrm{id}_{U^{-1}M}$ and, if we have $M \xrightarrow{\;\varphi\;} N \xrightarrow{\;\psi\;} P$, then $U^{-1}(\psi \circ \varphi) = (U^{-1}\psi) \circ (U^{-1}\varphi)$. So $U^{-1}\bullet$ defines a covariant functor from R-mod to R-mod for every multiplicatively closed set U.

Proposition 3.10. *Let U be a multiplicatively closed set of the ring R. The functor $U^{-1}\bullet : R-mod \longrightarrow R-mod$ is exact, that is, for every exact sequence $M_1 \xrightarrow{\;f_1\;} M_2 \xrightarrow{\;f_2\;} M_3$, the sequence*

$$U^{-1}M_1 \xrightarrow{\;U^{-1}f_1\;} U^{-1}M_2 \xrightarrow{\;U^{-1}f_2\;} U^{-1}M_3$$

is also exact.

Proof. We have $U^{-1}f_2 \circ U^{-1}f_1 = U^{-1}(f_2 \circ f_1) = U^{-1}0 = 0$, which implies $\mathrm{Im}(U^{-1}f_1) \subseteq \mathrm{Ker}(U^{-1}f_2)$.
For $\mathrm{Im}(U^{-1}f_1) \supseteq \mathrm{Ker}(U^{-1}f_2)$, let $\frac{m_2}{s} \in \mathrm{Ker}(U^{-1}f_2)$. This means $\frac{f_2(m_2)}{s} = 0 \in U^{-1}M_3$, so there exists $t \in U$ such that $tf_2(m_2) = 0 \in M_3$. This means $f_2(tm_2) = 0$, and thus $tm_2 \in \mathrm{Ker}\, f_2 = \mathrm{Im}\, f_1$, so there exists $m_1 \in M_1$ such that $f_1(m_1) = tm_2$. So $\frac{m_2}{s} = \frac{f_1(m_1)}{ts} = U^{-1}f_1(\frac{m_1}{ts}) \in \mathrm{Im}(U^{-1}f_1)$. $\qquad\square$

Corollary 3.11. *Fractions preserve submodules, sums, finite intersections and quotient modules. That is, for any multiplicatively closed set U of the ring R, and for any R-submodules N, P of M we have:*

(a) $U^{-1}N$ *is an $U^{-1}R$-submodule o $U^{-1}M$.*

(b) $U^{-1}(N + P) = U^{-1}N + U^{-1}P$.

(c) $U^{-1}(M/N) \cong U^{-1}M/U^{-1}N$ *as $U^{-1}R$-submodules.*

(d) $U^{-1}(N \cap P) = U^{-1}N \cap U^{-1}P$.

Proof. The first three points are direct consequences of the definitions and Propostion 3.10.
For (iv), one automatically has $\subseteq$ by (i), so let $x \in U^{-1}N \cap U^{-1}P$, that is there exists $n \in N$, $p \in P$ and $s, t \in U$ such that $x = \frac{n}{s} = \frac{p}{t}$. This implies, there exists $u \in U$ such that $u(nt - ps) = 0 \Leftrightarrow unt = ups$. Hence we have

$$x = \frac{unt}{stu} = \frac{ups}{stu} \in U^{-1}(N \cap P).$$

$\square$

3.3 Fractions and the Tensor Product

Proposition 3.12. *Let $U \subseteq R$ be a multiplicatively closed set and M and R-module. There exists a unique $U^{-1}R$-module isomorphism*

$$f : U^{-1}R \otimes_R M \xrightarrow{\sim} U^{-1}M,$$

such that $f(\frac{a}{s} \otimes m) = \frac{am}{s}$, for all $a \in R, s \in U, m \in M$.

Proof. The map $f' : U^{-1}R \times M \longrightarrow U^{-1}M$ with $(\frac{a}{s}, m) \mapsto \frac{am}{s}$ is R-bilinear, so it induces an R-linear map f as in the statement. We have $\frac{m}{s} = f(\frac{1}{s} \otimes m)$, so f is surjective. To check injectivity, we first show that every element of $U^{-1}R \otimes_R M$ is of the form $\frac{1}{s} \otimes m$. Let $\sum_{i=1}^n \frac{a_i}{s_i} \otimes m_i$ be an arbitrary element in $U^{-1}R \otimes_R M$. Define $s := \prod_{i=1}^n s_i$ and for every $j = 1, \ldots, n$ define $t_j := \prod_{i \neq j} s_i$. We have

$$\sum_{i=1}^n \frac{a_i}{s_i} \otimes m_i = \sum_{i=1}^n \frac{t_i a_i}{s} \otimes m_i = \sum_{i=1}^n \frac{1}{s} \otimes t_i a_i m_i = \frac{1}{s} \otimes \sum_{i=1}^n t_i a_i m_i.$$

Now assume that $f(\frac{1}{s} \otimes m) = 0$. This means that $\frac{m}{s} = 0$, so there exists $t \in U$ such that $tm = 0$. This allows us to compute:

$$\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0.$$

So f is bijective, and thus an R-isomorphism, which also implies an $U^{-1}R$-isomoprhism. $\square$

Corollary 3.13. *For every ring and every multiplicatively closed set $U^{-1}R$ is a flat R-module.*

Proof. Combine Proposition 3.12 and Proposition 3.10. $\square$

Corollary 3.14. *If M, N are two R-modules, and U is a multiplicatively closed set, then there is a unique isomorphism of $U^{-1}R$-modules $f : U^{-1}M \otimes_{U^{-1}R} U^{-1}N \xrightarrow{\sim} U^{-1}(M \otimes_R N)$ such that*

$$f\left(\frac{m}{s} \otimes \frac{n}{t}\right) = \frac{m \otimes n}{st}.$$

In particular, for every prime ideal $\mathfrak{p} \subseteq R$ we have

$$M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}} \cong (M \otimes N)_{\mathfrak{p}}.$$

Proof. Using a combination of Proposition 3.12, Remark 2.47, and Proposition 2.46 we obtain:

$$
\begin{aligned}
U^{-1}M \otimes_{U^{-1}R} U^{-1}N &\cong \left(U^{-1}R \otimes_R M\right) \otimes_{U^{-1}R} \left(U^{-1}R \otimes_R N\right) \\
&\cong \left(M \otimes_R U^{-1}R\right) \otimes_{U^{-1}R} \left(U^{-1}R \otimes_R N\right) \\
&\cong M \otimes_R \left(U^{-1}R \otimes_{U^{-1}R} \left(U^{-1}R \otimes_R N\right)\right) \\
&\cong M \otimes_R \left(\left(U^{-1}R \otimes_{U^{-1}R} U^{-1}R\right) \otimes_R N\right) \\
&\cong M \otimes_R \left(U^{-1}R \otimes_R N\right) \\
&\cong U^{-1}R \otimes_R \left(M \otimes_R N\right) \\
&\cong U^{-1}\left(M \otimes_R N\right).
\end{aligned}
$$

$\square$

3.4   Local Properties

A property $\mathcal{P}$ of an R-module M is called a **local property** if

$$M \text{ has } \mathcal{P} \iff M_{\mathfrak{p}} \text{ has } \mathcal{P} \text{ for every prime ideal } \mathfrak{p} \in \operatorname{Spec}(R).$$

One can talk about local properties of rings or of homomorphisms. The following results provide some examples of such properties.

Proposition 3.15. *Let M be an R-module. The following are equivalent*

(a) $M = 0$.

(b) $M_{\mathfrak{p}} = 0$, *for all $\mathfrak{p} \in \operatorname{Spec}(R)$.*

(c) $M_{\mathfrak{m}} = 0$, *for all $\mathfrak{m} \in \operatorname{MaxSpec}(R)$.*

Proof. Clearly (a)$\Rightarrow$ (b)$\Rightarrow$ (c). We prove now (c)$\Rightarrow$ (a):
Assume $M \neq 0$, so there exists $0 \neq x \in M$. Consider $I := \operatorname{Ann}_R(x)$. Because $1 \cdot x \neq 0$, we have $I \neq (1)$, so there exists $\mathfrak{m} \in \operatorname{MaxSpec}(R)$ with $I \subseteq \mathfrak{m}$. Consider the image of x in the localisation at $\mathfrak{m}$: $\frac{x}{1} \in M_{\mathfrak{m}} = (R \setminus \mathfrak{m})^{-1}M$. Since $M_{\mathfrak{m}} = 0$, we have $\frac{x}{1} = 0$, that is there exists $t \in R \setminus \mathfrak{m}$ such that $tx = 0$, which implies $t \in \operatorname{Ann}_R(x) = I \subseteq \mathfrak{m}$, a contradiction. $\square$

Proposition 3.16. *Let $\varphi : M \longrightarrow N$ be an R-module homomorphism. The following are equivalent.*

(a) $\varphi : M \longrightarrow N$ *is injective (respectively surjective).*

(b) $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$ *is injective (respectively surjective) for all $\mathfrak{p} \in \operatorname{Spec}(R)$.*

(c) $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}$ *is injective (respectively surjective) for all $\mathfrak{m} \in \operatorname{MaxSpec}(R)$.*

Proof. (a)$\Rightarrow$(b) follows from Proposition 3.10 and Remark 2.37.
(b)$\Rightarrow$(c) is trivial.
(c)$\Rightarrow$(a) We show the statement for injectivity. Consider the following exact sequence

$$0 \longrightarrow \operatorname{Ker}(\varphi) \longrightarrow M \xrightarrow{\varphi} N$$

Let $\mathfrak{m} \in \operatorname{MaxSpec}(R)$ be any maximal ideal. By Proposition 3.10 we have the following sequence is also exact:

$$0 \longrightarrow (\operatorname{Ker}(\varphi))_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \xrightarrow{\varphi_{\mathfrak{m}}} N_{\mathfrak{m}} \ .$$

As $\varphi_{\mathfrak{m}}$ is injective by hypothesis, because the sequence is exact, we must have $(\mathrm{Ker}(\varphi))_{\mathfrak{m}} = 0$. As this holds for all $\mathfrak{m} \in \mathrm{MaxSpec}(R)$, by Proposition 3.15 we obtain $\mathrm{Ker}(\varphi) = 0$ so we conclude.

Surjectivity follows analogously by considering the exact sequence $M \xrightarrow{\varphi} N \longrightarrow \mathrm{Coker}(\varphi) \longrightarrow 0$. $\qquad\square$

Exercise. Is it true that $\mathrm{Ker}(\varphi)_{\mathfrak{m}} = \mathrm{Ker}(\varphi_{\mathfrak{m}})$ and $\mathrm{Coker}(\varphi)_{\mathfrak{m}} = \mathrm{Coker}(\varphi_{\mathfrak{m}})$ in general?

Proposition 3.17. *Flatness is a local property. In particular, for any R-module M the following are equivalent.*

  (a) *M is a flat R-module.*

  (b) *$M_{\mathfrak{p}}$ is a flat $R_{\mathfrak{p}}$-module for every $\mathfrak{p} \in \mathrm{Spec}(R)$.*

  (c) *$M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module for every $\mathfrak{m} \in \mathrm{MaxSpec}(R)$.*

Proof. (a)$\Rightarrow$(b) follows from Proposition 3.12 and Remark 2.53.
(b)$\Rightarrow$(c) is trivial.

(c)$\Rightarrow$(a) By Proposition 2.52 we have to show that the map $N \otimes M \xrightarrow{f \otimes \mathrm{id}} P \otimes M$ is injective for any injective R-linear map $N \xrightarrow{f} P$. Let $\mathfrak{m}$ be any maximal ideal of R. By Proposition 3.16 we have that $N_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} P_{\mathfrak{m}}$ is injective. As $M_{\mathfrak{m}}$ is by hypothesis a flat $R_{\mathfrak{m}}$-module, Proposition 2.52 implies that

$$N_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}} \otimes \mathrm{id}} P_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}}$$

is also injective. Proposition 3.14 gives us that $(N \otimes_R M)_{\mathfrak{m}} \xrightarrow{(f \otimes \mathrm{id})_{\mathfrak{m}}} (P \otimes_R M)_{\mathfrak{m}}$ is injective. As $\mathfrak{m}$ was arbitrarily chosen in $\mathrm{MaxSpec}(R)$, we conclude by Proposition 3.16. $\qquad\square$

3.5 Extended and Contracted Ideals in the Ring of Fractions

Fix for this section a ring R and a multiplicatively closed set $U \subseteq R$, and denote by $f : R \longrightarrow U^{-1}R$ the canonical homomorphism with $x \mapsto {}^x/{}_1$. We will denote by

$$
\begin{aligned}
\mathcal{C} &= \{ \text{ contracted ideals of } R\} \\
\mathcal{E} &= \{ \text{ extended ideals in } U^{-1}R\}.
\end{aligned}
$$

Remark 3.18. For any ideal $I \subseteq R$, its extension in $U^{-1}R$ is $I^e = U^{-1}I$. Indeed, let $x \in I^e$, that is

$$x = \sum_i^n \frac{r_i}{t_i} \cdot \frac{a_i}{s_i}, \quad \text{with } r_i \in R, t_i, s_i \in U, \text{ and } a_i \in I,$$

so x can be expressed as a fraction with denominator $t_1 \ldots t_n s_1 \ldots s_n$ and numerator in I.

Remark 3.19. It will be useful for the next proofs to highlight the following:

$$\frac{x}{t} \in U^{-1}M \Leftrightarrow \exists u \in U \text{ such that } ux \in M.$$

Proof.

$$
\begin{aligned}
\frac{x}{t} \in U^{-1}M &\Leftrightarrow \exists s \in U, m \in M \text{ such that } \frac{x}{t} = \frac{m}{s} \\
&\Leftrightarrow \exists s, u' \in U, m \in M \text{ such that } u'(sx - tm) = 0 \\
&\Leftrightarrow \exists u \in U, \text{ such that } ux \in M
\end{aligned}
$$

The direction $\Rightarrow$ is clear. The only non-obvious implication is the one from line 3 to line 2. This works because

$$ux \in M \Rightarrow \exists m \in M \text{ such that } ux - m = 0 \Rightarrow u'(ux - 1 \cdot m) = 0 \forall\ u' \in U.$$

$\qquad\square$

Proposition 3.20. *Let $I \subseteq R$ and $J \subseteq U^{-1}R$ be ideals. We have*

(a) $J \in \mathcal{E}$.

(b) $I^{ec} = \bigcup_{s \in U}(I : s)$.

(c) $I^e = (1) \iff I \cap U \neq \emptyset$.

(d) $I \in \mathcal{C} \iff U \cap \{$*zero divisors of* $R/I\} = \emptyset$.

Proof. (a) Since $J^{ce} \subseteq J$ in general by Proposition 1.44, we need to show only the reverse inclusion. Let $x/s \in J$. So $s/1 \cdot x/s = x/1 \in J$. This means, that $x \in J^c$, so $1/s \cdot x/1 = x/s \in J^{ce}$.

(b) We the following chain of equivalence, where the second is given by Remark 3.19.

$$
\begin{aligned}
x \in I^{ec} = (U^{-1}I)^c \quad &\Leftrightarrow \quad \frac{x}{1} \in U^{-1}I \\
&\Leftrightarrow \quad ux \in I \text{ for some } u \in U. \\
&\Leftrightarrow \quad x \in \bigcup_{u \in U}(I : u).
\end{aligned}
$$

(c) If $u \in U \cap I$, then I^e would contain the unit $u/1$. Conversely, if $I^e = (1)$, then $I^{ec} = R$, so by part (b) $1 \in \bigcup_{u \in U}(I : u)$, so there exists $u \in U$ with $1 \cdot u \in I$.

(d) By Proposition 1.44 we have $I \subseteq I^{ec}$, so

$$
\begin{aligned}
I \in \mathcal{C} \quad &\Leftrightarrow \quad I^{ec} \subseteq I \\
&\Leftrightarrow \quad \text{if } x \in R \text{ satisfies } \frac{x}{1} \in U^{-1}I \text{ then } x \in I. \\
&\Leftrightarrow \quad \text{if } sx \in I \text{ for some } s \in U, \text{ then } x \in I \\
&\Leftrightarrow \quad \text{if } s \cdot x = 0 \in R/I \text{ for some } s \in U, \text{ then } x = 0 \in R/I. \\
&\Leftrightarrow \quad S \cap \{\text{zero divisors of } R/I\} = \emptyset.
\end{aligned}
$$

$\square$

Proposition 3.21. *The map of sets* $^e : \{\mathfrak{p} \in \operatorname{Spec}(R) \ : \ \mathfrak{p} \cap U = \emptyset\} \longrightarrow \operatorname{Spec}(U^{-1}R)$ *given by*

$$
\mathfrak{p} \mapsto \mathfrak{p}^e = U^{-1}\mathfrak{p}
$$

is bijective, with inverse $^c : \operatorname{Spec}(U^{-1}R) \longrightarrow \{\mathfrak{p} \in \operatorname{Spec}(R) \ : \ \mathfrak{p} \cap U = \emptyset\}$ *given by* $U^{-1}\mathfrak{p} \longrightarrow (U^{-1}\mathfrak{p})^c$*, where the contraction is taken over the canonical map* $f : R \longrightarrow U^{-1}R$.

Proof. Using Proposition 3.20 (a) and Remark 1.44 (c) we just have to make sure that extension and contraction restrict properly to the sets we are considering. Bijectivity is then implied.

First, we have to show that if $\mathfrak{p}$ is prime and disjoint from U, then $U^{-1}\mathfrak{p}$ is prime. We know that $R/\mathfrak{p}$ is a domain. By Corollary 3.11 we have $U^{-1}R/U^{-1}\mathfrak{p} \cong U^{-1}(R/\mathfrak{p}) = [U]^{-1}(R/\mathfrak{p})$, where $[U]$ is the image of U in $R/\mathfrak{p}$. By assumption $\mathfrak{p} \cap U = \emptyset$, so $[0]_\mathfrak{p} \notin [U]$, and thus $[U]^{-1}(R/\mathfrak{p})$ is not the zero ring. It is thus a nontrivial subring of the field of fractions of the integral domain $R/\mathfrak{p}$, thus it is an integral domain, which implies that $U^{-1}\mathfrak{p} \in \operatorname{Spec}(U^{-1}R)$. So the map ^{e} is properly defined (i.e. it sends elements to the codomain).

For the inverse first notice that J^c is always prime when J is prime (cf. Remark 1.18). If there existed $u \in U \cap f^{-1}(U^{-1}I)$, then $U^{-1}I = (1)$ would not be prime. So the restriction of ^{c} is also properly defined. $\square$

Proposition 3.22. *For any ideals $I_1, I_2,$ and I of R we have*

(a) $U^{-1}(I_1 \cap I_2) = U^{-1}I_1 \cap U^{-1}I_2$

(b) $U^{-1}(I_1 + I_2) = U^{-1}I_1 + U^{-1}I_2$

(c) $U^{-1}(I_1 I_2) = (U^{-1}I_1)(U^{-1}I_2)$

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

Proof. (a) is a particular case of Corollary 3.11.

(b) and (c) are by Remark 3.18 equivalent to Remark 1.45.

(d) Again by Remark 1.45 we get $U^{-1}\sqrt{I} = (\sqrt{I})^e \subseteq \sqrt{I^e} = \sqrt{U^{-1}I}$.

For the other inclusion:

$$
\begin{aligned}
{}^r/_s \in \sqrt{U^{-1}I} &\Leftrightarrow \exists\, n \in \mathbb{N} \text{ such that } {}^{r^n}/_{s^n} \in U^{-1}I \\
&\Leftrightarrow \exists\, n \in \mathbb{N}, \exists\, u \in U \text{ such that } ur^n \in I \\
&\Rightarrow \exists\, n \in \mathbb{N}, \exists\, u \in U \text{ such that } (ur)^n \in I \\
&\Leftrightarrow \exists\, u \in U \text{ such that } ur \in \sqrt{I} \\
&\Leftrightarrow {}^r/_s \in U^{-1}\sqrt{I}
\end{aligned}
$$

$\qquad\square$

Corollary 3.23. *If $\mathcal{N}_R$ is the nilradical of R, then $U^{-1}\mathcal{J}_R$ is the nilradical of $U^{-1}R$.*

Corollary 3.24. *If $\mathfrak{p}$ is a prime ideal of R, then the prime ideals in the localization $R_\mathfrak{p}$ are in one to one correspondence to the prime ideals contained in $\mathfrak{p}$.*

Remark 3.25. The prime spectrum of a ring can be thought of as a **p**artially **o**rdered **set** (**poset**) by inclusion. Localization at a prime $\mathfrak{p}$ keeps exactly those primes smaller or equal than $\mathfrak{p}$, so the interval $(-\infty, \mathfrak{p}] = \{\mathfrak{q} \in \mathrm{Spec}(R) : \mathfrak{q} \subseteq \mathfrak{p}\}$. Quotienting by $\mathfrak{p}$ keeps exactly those primes which are larger or equal than $\mathfrak{p}$, so the interval $[\mathfrak{p}, \infty) = \{\mathfrak{q} \in \mathrm{Spec}(R) : \mathfrak{p} \subseteq \mathfrak{q}\}$. For $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}(R)$ with $\mathfrak{q} \subseteq \mathfrak{p}$, we have by Corollary 3.11

$$R_\mathfrak{p}/\mathfrak{q}_\mathfrak{p} = (R/\mathfrak{q})_\mathfrak{p}$$

and the spectrum of this ring is thus the interval $[\mathfrak{q}, \mathfrak{p}] = \{\mathfrak{p}' \in \mathrm{Spec}(R) : \mathfrak{q} \subseteq \mathfrak{p}' \subseteq \mathfrak{p}\}$. In the special case that $\mathfrak{q} = \mathfrak{p}$, we end up with a field $\mathcal{K}$ which is called the **residue field at $\mathfrak{p}$**. It can be viewed as both the field of fractions of the integral domain $R/\mathfrak{p}$, or the residue field of the local ring $R_\mathfrak{p}$. In the even more special case when $\mathfrak{p} = \mathfrak{m}$ is maximal, we have thus $(R/\mathfrak{m})_\mathfrak{m} = R/\mathfrak{m}$.

Proposition 3.26. *Let U be a multiplicatively closed set of the ring R and M a finitely generated R-module. We have*

$$U^{-1}(\mathrm{Ann}_R(M)) = \mathrm{Ann}_{U^{-1}R}(U^{-1}M).$$

Proof. If $M = \langle m \rangle$ is generated by a single element, then we have

$$0 \to \mathrm{Ann}_R(M) \to R \to M \to 0$$

$$1 \mapsto m$$

So, if we denote by $I := \mathrm{Ann}_R(M)$ we have $M \cong R/I$ as R-modules. We get by Corollary 3.11

$$U^{-1}M = U^{-1}R/U^{-1}I,$$

and thus $\mathrm{Ann}_{U^{-1}R} U^{-1}M = U^{-1}I = U^{-1}\mathrm{Ann}_R(M)$. To extend this now to any finitely generated module, it is enough to show that if the proposition is true for M_1 and M_2, then it is true for $M_1 + M_2$ as well. Combining Corollary 3.11 and Remark 2.16 with the hypothesis $U^{-1}(\mathrm{Ann}_R(M_i)) = \mathrm{Ann}_{U^{-1}R}(U^{-1}M_i)$ for $i = 1, 2$ we get

$$U^{-1}\big(\mathrm{Ann}_R(M_1 + M_2)\big) \quad = \quad U^{-1}\big(\mathrm{Ann}_R(M_1) \cap \mathrm{Ann}_R(M_2)\big)$$

$$
\begin{aligned}
&= & U^{-1}\big(\operatorname{Ann}_R(M_1)\big) \cap U^{-1}\big(\operatorname{Ann}_R(M_2)\big) \\
&= & \operatorname{Ann}_{U^{-1}R}(U^{-1}M_1) \cap \operatorname{Ann}_{U^{-1}R}(U^{-1}M_2) \\
&= & \operatorname{Ann}_{U^{-1}R}(U^{-1}M_1 + U^{-1}M_2) \\
&= & \operatorname{Ann}_{U^{-1}R}(U^{-1}(M_1 + M_2))
\end{aligned}
$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Corollary 3.27. *Let M be an R-module and $N, P \subseteq M$ submodules, with P finitely generated. We have*

$$
U^{-1}(N : P) = (U^{-1}N : U^{-1}P).
$$

Proof. By Remark 2.16 we have $N : P = \operatorname{Ann}_R(N + P/P)$. As $(N+P)/P = P/N \cap P$, we have finite generation and may apply Proposition 3.26 to conclude. $\qquad\square$

Proposition 3.28. *Let S be an R-algebra with $\varphi : R \longrightarrow S$ and $\mathfrak{p} \in \operatorname{Spec}(R)$. We have that $\mathfrak{p}$ is the contraction of a prime ideal of S if and only if $\mathfrak{p} = \mathfrak{p}^{ec}$.*

Proof. If $\mathfrak{p} = \mathfrak{q}^c$, then $\mathfrak{p}^{ec} = \mathfrak{q}^{cec} = \mathfrak{q}^c = \mathfrak{p}$.
Let $\mathfrak{p}^{ec} = \mathfrak{p}$. Define $U' := R \setminus \mathfrak{p}$, and $U := \varphi(U') \subseteq S$, which is a multiplicatively closed set because U' is one. By definition $\mathfrak{p}^e \cap U = \emptyset$, therefore we can further extend $\mathfrak{p}^e$ to a proper ideal $U^{-1}\mathfrak{p}^e$ of $U^{-1}S$. So there exists a maximal ideal $\mathfrak{m}$ of $U^{-1}S$ containing $U^{-1}\mathfrak{p}^e$. Then, the contraction of $\mathfrak{m} \subseteq U^{-1}S$ to S is a prime ideal $\mathfrak{q} = \mathfrak{m}^c$, with $\mathfrak{q} \subseteq U = \emptyset$, and $\mathfrak{p}^e \subseteq \mathfrak{q}$, thus $\mathfrak{p} = \mathfrak{p}^{ec} = \mathfrak{q}^c$ is thus the contraction of a prime ideal. $\qquad\square$

Chapter 4

Primary Decomposition

Primary decomposition is a generalization of the fundamental theorem of arithmetic. Elements are replaced with ideals, powers of prime numbers with primary ideals, and the product with the intersection. The problem is, it does not always exist for arbitrary rings, but when it does it satisfies some uniqueness theorems which will be the main results in this chapter.

4.1   Primary Ideals

Definition 4.1. An ideal $\mathfrak{q}$ of a ring R is called a **primary ideal** if it is proper and if

$$xy \in \mathfrak{q} \Rightarrow x \in \mathfrak{q} \ \text{ or } \ \exists\, n \in \mathbb{N} \text{ such that } y^n \in \mathfrak{q}.$$

Equivalently, if $R/\mathfrak{q} \neq 0$ and every zero divisor in $R/\mathfrak{q}$ is nilpotent.

Remark 4.2.   (a) Every prime ideal is primary.

(b) If $f : R \longrightarrow S$ is a ring homomorphism and if $\mathfrak{q} \subseteq S$ is a primary ideal, then $\mathfrak{q}^c$ is a primary ideal of R. The reason for this is that $R/\mathfrak{q}^c$ is isomoprhic to a subring of $S/\mathfrak{q}$.

Proposition 4.3. *Let $\mathfrak{q} \subseteq R$ be a primary ideal. Then $\sqrt{\mathfrak{q}}$ is prime. In particular, it is the smallest prime ideal containing $\mathfrak{q}$.*

Proof. Let $x, y \in R$ with $xy \in \sqrt{\mathfrak{q}}$. Then $\exists\, m \in \mathbb{N}$ such that $(xy)^m = (x^m)(y^m) \in \mathfrak{q}$. As $\mathfrak{q}$ is primary, either $x^m \in \mathfrak{q}$ or $\exists\, n \in \mathbb{N}$ such that $(y^m)^n = y^{mn} \in \mathfrak{q}$. So either $x \in \sqrt{\mathfrak{q}}$ or $y \in \sqrt{\mathfrak{q}}$. $\qquad\square$

The converse of Proposition 4.3 does not hold, as we will see soon enough. (Otherwise, it would have been a nicer definition). Anyway, the radical of a primary ideal plays an important role, and that is why, if $\sqrt{\mathfrak{q}} = \mathfrak{p}$, then $\mathfrak{q}$ is called $\mathfrak{p}$-**primary**.

Examples.   1. The primary ideals of $\mathbb{Z}$ are (0) and (p^n), for p a prime integer.

2. Let $S = \mathbb{K}[x, y]$, $\mathfrak{q} = (x, y^2)$. Then $S/\mathfrak{q} \cong \mathbb{K}[y]/(y^2)$, so all the zero divisors are multiples of y, and hence nilpotent. So here we have $\mathfrak{p} = \sqrt{\mathfrak{q}} = (x, y)$ and the strict inclusions

$$\mathfrak{p}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}.$$

This shows that not all primary ideals are powers of primes.

3. It gets worse: not all prime powers are necessarily primary, although the radical is a prime ideal. For example, take $R = \mathbb{K}[x, y, z]/(xy - z^2)$ and let $[f]$ denote the image of a polynomial under the canonical projection to R. The ideal $\mathfrak{p} = ([x], [z])$ is prime, since $R/\mathfrak{p} \cong \mathbb{K}[y]$. But we have

$$[x][y] = [z^2] \in \mathfrak{p}^2$$

while $[x] \notin \mathfrak{p}^2$ and $[y] \notin \sqrt{\mathfrak{p}^2} = \mathfrak{p}$; hence $\mathfrak{p}^2$ is not primary.

Proposition 4.4. *If $\sqrt{I}$ is maximal, then I is primary. In particular, the powers of a maximal ideal $\mathfrak{m}$ are $\mathfrak{m}$-primary.*

Proof. Denote $\sqrt{I}$ by $\mathfrak{m}$. In general, the image of $\sqrt{I}$ under the canonical projection $R \longrightarrow R/I$, is the nilradical of R/I. The preimage of every prime ideal of R/I is a prime ideal of R which contains $\mathfrak{m}$, so there is only one prime ideal in R/I. In particular, an element of R/I is either a unit, or nilpotent. $\qquad\square$

Lemma 4.5. *If $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are $\mathfrak{p}$-primary ideals, then $\bigcap_{i=1}^n \mathfrak{q}_i$ is also $\mathfrak{p}$-primary.*

Proof. First of all, $\sqrt{\bigcap_{i=1}^n \mathfrak{q}_i} = \bigcap_{i=1}^n \sqrt{\mathfrak{q}_i} = \mathfrak{p}$. We will use this to prove that the intersection is primary. Let $xy \in \bigcap_{i=1}^n \mathfrak{q}_i$. Assume $x \notin \bigcap_{i=1}^n \mathfrak{q}_i$, i.e. there exists i_0 such that $x \notin \mathfrak{q}_{i_0}$, but $xy \in \mathfrak{q}_{i_0}$. Because $\mathfrak{q}_{i_0}$ is $\mathfrak{p}$-primary, it follows $y \in \sqrt{\mathfrak{q}_{i_0}} = \mathfrak{p} = \sqrt{\bigcap_{i=1}^n \mathfrak{q}_i}$. $\qquad\square$

Lemma 4.6. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal of R, and let $x \in R$. We have*

(a) *If $x \in \mathfrak{q}$, then $\mathfrak{q} : x = R$.*

(b) *If $x \notin \mathfrak{p}$, then $\mathfrak{q} : x = \mathfrak{q}$.*

(c) *If $x \notin \mathfrak{q}$, then $\mathfrak{q} : x$ is $\mathfrak{p}$-primary.*

Proof.   (a) This is true for any ideal.

(b) "$\supseteq$" is always true. For "$\subseteq$", let $y \in \mathfrak{q} : x$, so $xy \in \mathfrak{q}$. As $x \notin \mathfrak{p} = \sqrt{\mathfrak{q}}$, we must have $y \in \mathfrak{q}$.

(c) We first show $\sqrt{\mathfrak{q} : x} = \mathfrak{p}$. Let $y \in \mathfrak{q} : x$, so $xy \in \mathfrak{q}$. As $x \notin \mathfrak{q}$, we have $y \in \sqrt{idq} = \mathfrak{p}$. So, given that $I \subseteq I : J$ in general, we get

$$\mathfrak{q} \subseteq \mathfrak{q} : x \subseteq \mathfrak{p} \quad \Rightarrow \quad \mathfrak{p} = \sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{q} : x} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}.$$

Now, let $yz \in \mathfrak{q} : x$, so $xyz \in \mathfrak{q}$. Assume that $z \notin \sqrt{idq : x} = \mathfrak{p}$. Then, as $\mathfrak{q}$ is $\mathfrak{p}$-primary, we get $xy \in \mathfrak{q}$, so $y \in \mathfrak{q} : x$.

$\qquad\square$

4.2   Decompositions

Definition 4.7. Let $I \subseteq R$ be an ideal. A **primary decomposition** of I is an expression of I as a *finite* intersection of primary ideals:

$$I = \bigcap_{i=1}^n \mathfrak{q}_i,$$

with $\mathfrak{q}_i$ being $\mathfrak{p}_i$-primary for every i. A primary decomposition is called **minimal** (or irredundant) if

(i) all the $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ are distinct, and

(ii) $\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$ for every $i = 1, \ldots, n$.

An ideal is called a **decomposable ideal** if it has some primary decomposition.

Remark 4.8. (a) Not all ideals are decomposable. We will see an example later in the lecture, or during the exercise session.

(b) Every primary decomposition can be reduced to a minimal one using Lemma 4.5 and leaving out redundant ideals in the intersection.

Theorem 4.9 (First Uniqueness Theorem)**.** *Let $I \subseteq R$ be a decomposable ideal and let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition of I, with $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$ for $i = 1, \ldots, n$. Then we have*

$$\big\{ \mathfrak{p}_1, \ldots, \mathfrak{p}_n \big\} = \big\{ \sqrt{I : x} \mid x \in R \big\} \cap \operatorname{Spec}(R).$$

In particular, the ideals $\mathfrak{p}_i$ are independent of the primary decomposition.

Proof. For every $x \in R$ we have $I : x = \big(\bigcap_{i=1}^n \mathfrak{q}_i : x \big) = \bigcap_{i=1}^n (\mathfrak{q}_i : x)$. Taking radicals, we get

$$\sqrt{I : x} = \bigcap_{i=1}^n \sqrt{\mathfrak{q}_i : x} = \bigcap_{\substack{i=1 \\ \mathfrak{q}_i \not\ni x}}^n \sqrt{\mathfrak{q}_i : x} = \bigcap_{\substack{i=1 \\ \mathfrak{q}_i \not\ni x}}^m \mathfrak{p}_i, \tag{4.1}$$

where the second and third equalities follow from Lemma 4.6 (c).

$\boxed{\supseteq}$ If $\sqrt{I : x} \in \operatorname{Spec}(R)$, then by the Prime Avoidance Lemma 1.39 it must be one of the $\mathfrak{p}_i$.

$\boxed{\subseteq}$ Since the decomposition is minimal, for every $i = 1, \ldots, n$, we have $\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$, so there exists an $x_i \notin \mathfrak{q}_i$ with $x_i \in \bigcap_{\substack{j=1 \\ j \neq i}}^n \mathfrak{q}_j$. In particular, there is just one prime ideal on the righ hand side in (4.1), and we conclude that $\mathfrak{p}_i = \sqrt{I : x_i}$. $\qquad\square$

The unique primes from Theorem 4.9 are called the **associated primes** of I, and the set of associated primes is denoted by $\operatorname{Ass}(I)$. An associated prime is called a **minimal prime** of I (or *isolated prime* of I), if it is a minimal element of $\operatorname{Ass}(I)$ with respect to inclusion. The set of minimal primes is denoted by $\operatorname{Min}(I)$. The non-minimal associated primes are called **embedded primes**; they are thus the elements of the set $\operatorname{Ass}(I) \setminus \operatorname{Min}(I)$.

Remark 4.10. An ideal is primary if and only if it has just one associated prime.

While associated primes are unique, minimal primary decompositions are not:

Example 4.11. Let $R = \mathbb{K}[x, y]$, and $I = (x^2, xy)$. We have

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

The primes involved are: $\mathfrak{p}_1 = (x)$ and $\mathfrak{p}_2 = (x, y)$, thus we have an inclusion: $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$. So

$$\operatorname{Ass}(I) = \{(x), (x, y)\} \qquad \operatorname{Min}(I) = \{(x)\}$$

and (x, y) is an embedded prime of I. You can think of the line $V(x)$ as an irreducible component of the variety of $V(I)$, and the point given by the maximal ideal (x, y), as a subvariety of $V(I)$, thus a so-called "embedded" component.

The radical of I is (x), thus a prime ideal, but I is not primary.

Proposition 4.12. *Let $I \subseteq R$ be a decomposable ideal, and $\mathfrak{p}$ a prime ideal with $I \subseteq \mathfrak{p}$. Then, there exists $\mathfrak{p}_i \in \operatorname{Min}(I)$ such that $\mathfrak{p}_i \subseteq \mathfrak{p}$. In particular,*

$$\operatorname{Min}(I) = \min\{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \subseteq \mathfrak{p}\}.$$

Proof. Let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition of I with $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Taking radicals, over $\bigcap_{i=1}^n \mathfrak{q}_i \subseteq \mathfrak{p}$, we get $\bigcap_{i=1}^n \mathfrak{p}_i \subseteq \mathfrak{p}$, and by the Prime Avoidance Lemma 1.39 we get $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i, so $\mathfrak{p}$ must contain a minimal prime. $\qquad\square$

Proposition 4.13. *Let $I \subseteq R$ be a decomposable ideal. We have*

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass}(I)} \mathfrak{p} = \{x \in R \mid (I : x) \neq I\}.$$

In particular, if (0) is decomposable then

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass}((0))} = \{zero\ divisors\ of\ R\} =: D.$$

Proof. If I is decomposable as $I = \bigcap \mathfrak{q}_i$, then (0) is decomposable in R/I as $(0) = \bigcap \bar{\mathfrak{q}}_i$, where $\bar{\mathfrak{q}}_i$ is the image of $\mathfrak{q}_i$ in R/I. Clearly, because $(R/I)/\bar{\mathfrak{q}}_i \cong R/\mathfrak{q}_i$, we have that $\bar{\mathfrak{q}}_i$ is primary. So it is enough to prove the particular statement. By Proposition 1.40 we have $D = \bigcup x \neq 0 \sqrt{0 : x}$. From (4.1) in the proof of Theorem 4.9 we have

$$\sqrt{0 : x} = \bigcap_{\substack{i=1 \\ \mathfrak{q}_i \not\ni x}}^{m} \mathfrak{p}_i \subseteq \mathfrak{p}, \text{ for some } \mathfrak{p} \in \operatorname{Ass}(0),$$

hence $D \subseteq \bigcap_{\mathfrak{p} \in \operatorname{Ass}(0)} \mathfrak{p}$. Also from the last part of the proof of Theorem 4.9 we have that every $\mathfrak{p} \in \operatorname{Ass}(0)$ is of the form $\sqrt{0 : x}$ for some x, and this way we get the other inclusion. $\qquad\square$

So, if (0) is decomposable in R we get

$$D = \{\text{zero divisors of } R\} \quad = \bigcup_{\mathfrak{p} \in \operatorname{Ass}(0)} \mathfrak{p}$$

$$\mathcal{N}_R = \{\text{nilpotents of } R\} \quad = \bigcap_{\mathfrak{p} \in \operatorname{Min}(0)} \mathfrak{p}$$

4.3   Decompositions and Localizations

Proposition 4.14. *Let U be a multiplicatively closed set of R and $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal.*

(a) *If $U \cap \mathfrak{p} \neq \emptyset$, then $U^{-1}\mathfrak{q} = U^{-1}R$.*

(b) *If $U \cap \mathfrak{p} = \emptyset$, then $U^{-1}\mathfrak{q}$ is $U^{-1}\mathfrak{p}$-primary, and $(U^{-1}\mathfrak{q})^c = \mathfrak{q}$.*

Proof. (a) clear, since both $\mathfrak{p}$ and $\mathfrak{q}$ would contain a unit.

(b) Recall, that $\mathfrak{q}^e = U^{-1}\mathfrak{q}$. From Propositions 3.22 and 3.20 we have

$$\sqrt{\mathfrak{q}^e} = \sqrt{U^{-1}\mathfrak{q}} = U^{-1}\sqrt{\mathfrak{q}} = U^{-1}\mathfrak{p}.$$

So it remains to see that $\mathfrak{q}^e$ is actually primary. This follows from $U^{-1}R/U^{-1}\mathfrak{q} = U^{-1}(R/\mathfrak{q})$, and the equivalent definition for primary ideals.

For the last part: If $au \in \mathfrak{q}$ with $u \in U$, then, as $u \cap \mathfrak{p} = \emptyset$, we have $u^n \notin \mathfrak{q}$ for all n, so $a \in \mathfrak{q}$. 3.20 (b) we have $\mathfrak{q}^{ec} = \mathfrak{q}$.

$\qquad\square$

Proposition 4.15. *Let U be a multiplicatively closed set of R and I a decomposable ideal with a minimal primary decomposition $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$, where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Suppose that we labeled the primary ideals such that there exists an $m \in 1 \ldots n$ with $U \cap \mathfrak{p}_i = \emptyset \Leftrightarrow i \leq m$. Then we have the minimal primary decompositions:*

$$U^{-1}I = \bigcap_{i=1}^{m} U^{-1}\mathfrak{q}_i \qquad\qquad (U^{-1}I)^c = \bigcap_{i=1}^{m} \mathfrak{q}_i.$$

Proof. It follows from Proposition 3.22 and Proposition 4.14. □

A subset Σ of a partially ordered set $(\mathcal{P}, \leq)$, is called a **lower set**, if $x \in \Sigma$ and $y \in \mathcal{P}$ with $y \leq x$ imply $y \in \Sigma$. That is, if once it contains an element, it contains also all elements smaller or equal to it. The set of associated primes of a decomposable ideal $I \subseteq R$ is partially ordered by inclusion. A lower set $\Sigma \subseteq \operatorname{Ass}(I)$ is called in this case **isolated set**.

For any decomposable ideal I and any isolated set $\Sigma \subseteq \operatorname{Ass}(I)$, the set

$$U_\Sigma := R \setminus \bigcap_{\mathfrak{p} \in \Sigma} \mathfrak{p}$$

is multiplicatively closed, with the property that $\forall\, \mathfrak{p} \in \operatorname{Ass}(I)$ we have

$$\mathfrak{p} \in \Sigma \Leftrightarrow \mathfrak{p} \cap U_\Sigma = \emptyset.$$

As a corollary of Propostion 4.15 we get another statement about uniqueness in decompositions.

Theorem 4.16 (Second Uniqueness Theorem). *Let $I \subseteq R$ be a decomposable ideal, and let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition of I. If the set $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ is an isolated subset of $\operatorname{Ass}(I)$, then $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$ is independent of the chosen decomposition. In particular, the isolated primary components, i.e. those corresponding to the minimal primes, are uniquely determined by I.*

Proof. By Propositon 4.15 we have that $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m} = (U_\Sigma^{-1} I)^c$, so, as $\operatorname{Ass}(I)$ and the contraction are uniquely determined, is itself uniquely determined. □

We will see that for the embedded components one may have infinitely many choices.

Chapter 5

Chain Conditions

We have stated, without examples, that not all ideals admit a primary decomposition. There is however a hugely important family of rings for which primary decompositions always exist: Noetherian rings, called this way in honor of Emmy Noether, who proved the existence of primary decompositions under the so-called ascending chain conditions. Descending chain conditions for modules were studied by Emil Artin; in his honor we call rings with the descending chain conditions Artinian. These ascending and descending conditions apply both to rings and modules. Apparently there is a perfect symmetry between the two, however we shall see that in the case of (ideals in) rings, this symmetry disappears.

Let $(\mathcal{P}, \leq)$ be a poset. We say that $\mathcal{P}$ satisfies:

The ascending chain condition if every increasing sequence $x_1 \leq x_2 \leq \ldots$ is stationary (i.e. $\exists\, n$ such that $x_n = x_{n+1} = \ldots$).

- **The descending chain condition** if every decreasing sequence $x_1 \geq x_2 \geq \ldots$ is stationary (i.e. $\exists\, n$ such that $x_n = x_{n+1} = \ldots$).

- **The maximal condition** if every nonempty subset of $\mathcal{P}$ has a maximal element.

- **The minimal condition** if every nonempty subset of $\mathcal{P}$ has a minimal element.

Proposition 5.1. *For any poset $(\mathcal{P}, \leq)$ the ascending chain condition is equivalent to the maximal condition and the descending chain condition is equivalent to the minimal condition.*

Proof. Easy Exercise. $\qquad\square$

Definition 5.2. Let M be an R-module. Let $\mathcal{P}_{\subseteq}(M)$ be the poset of submodules of M ordered by inclusion.

(a) The module M is called **Noetherian** if $\mathcal{P}_{\subseteq}(M)$ satisfies the ascending chain condition.

(b) The module M is called **Artinian** if $\mathcal{P}_{\subseteq}(M)$ satisfies the descending chain condition.

Examples.   1. Any finite Abelian group is both a Noehterian and an Artinian $\mathbb{Z}$-module.

2. $\mathbb{Z}$, as $\mathbb{Z}$-module, is Noetherian, but not Artinian:

$$(a) \supsetneq (a^2) \supsetneq \cdots \supsetneq (a^n) \supsetneq \ldots$$

3. Fix a prime $p \in \mathbb{Z}$, and let $G := \{x \in \mathbb{Q}/\mathbb{Z} \ : \ \mathrm{ord}(x) = p^n \text{ for some } n\}$. Then, for each $n \in \mathbb{N}$, G has exactly one subgroup of order p^n: $G_n = \{x \in G \mid p^n x = 0\}$, and these are all the subgroups. We have

$$G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n \subsetneq \ldots$$

so the Z-module G is not Noetherian, but G is Artinian.

4. If $\mathbb{K}$ is a field, then $\mathbb{K}[x]$ is Noetherian, but not Artinian.

5. The polynomial ring in (coutably) infinitely many variables $\mathbb{K}[x_1, x_2, \dots]$ is neither Noetherian nor Artinian:

$$(x_1) \subsetneq (x_1, x_2) \subsetneq \dots$$
$$(x_1) \supsetneq (x_1^2) \supsetneq \dots$$

6. We will see later that for rings, Artinian implies Noetherian, but, as we have seen above, not the other way around. This is the broken symmetry we were referring to at the beginning of this chapter.

The following proposition is the crucial property of Noetherian modules. It shows that being Noetherian is the "right" finiteness assumption one needs for modules and rings.

Proposition 5.3. *An R-module M is Noetherian if and only if every submodule of M is finitely generated.*

Proof. $\boxed{\Rightarrow}$ Let $N \subseteq M$ be a submodule, and $\mathcal{P}_{\subseteq}^{f.g.}(N)$ the set of all finitely generated submodules of N. As $0 \in \mathcal{P}_{\subseteq}^{f.g.}(N) \subseteq \mathcal{P}_{\subseteq}(M)$, it is a nonempty subset, therefor by Proposition 5.1 it has at least one maximal element: N_0. If $N_0 \neq N$, there exists $x \in N \setminus N_0$, so $N + \langle x \rangle \in \mathcal{P}_{\subseteq}^{f.g.}(N)$ contradicts the maximality of N_0. Thus $N = N_0 \in \mathcal{P}_{\subseteq}^{f.g.}(N)$, and thus N is finitely generated.

$\boxed{\Leftarrow}$ Let $M_1 \subseteq M_2 \subseteq \dots$ be an ascending chain of submodules of M. Then $N := \bigcup_{i=1}^{\infty} M_n$ is a submodule of M (because we are taking the union over an ascending chain), hence finitely generated. Let $N = \langle x_1, \dots, x_r \rangle$, and define $n_0 := \min\{i \in \mathbb{N} \mid x_j \in M_i \text{ for all } j = 1 \dots r\}$. This is well defined by the way N was defined. So $M_n = M_{n_0} = N$ for all $n \geq n_0$, and thus the chain is stationary. $\square$

5.1 Common Formal Properties of Artinian and Noetherian Modules

Proposition 5.4. *Let $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ be a short exact sequence of R-modules. Then M_2 is Noetherian (resp. Artinian) if and only if M_1 and M_3 are Notherian (resp. Artinian).*

Proof. We shall proof the statement only for Artinian modules. The Noehterian case is analogous, (and it is done in Antiyah-Macdonald Proposition 6.3).
For every $i = 1, 2, 3$ let

$$\mathcal{C}_i : \qquad M_{i,1} \supsetneq M_{i,2} \supsetneq \dots$$

be a descending chain in M_i.
$\boxed{\Rightarrow}$ If $\mathcal{C}_i$ were not stationary in M_i for $i = 1, 3$, then $f_1(\mathcal{C}_1)$, respectively $f_2^{-1}(\mathcal{C}_3)$, would not be stationary in M_2.
$\boxed{\Leftarrow}$ Looking at the chains $f_1^{-1}(\mathcal{C}_2)$ and $f_2(\mathcal{C}_2)$, we get that there exists some $n_0 \in \mathbb{N}$ such that $f_1^{-1}(M_{2,n}) = f_1^{-1}(M_{2,n_0})$ and $f_2(M_{2,n}) = f_2(M_{2,n_0})$ for all $n \geq n_0$. We want to show that $M_{2,n} = M_{2,n_0}$ for all $n \geq n_0$. As we have a descending chain, it is enough to prove that $M_{2,n_0} \subseteq M_{2,n}$.
Let $x \in M_{2,n_0}$ and $n \geq n_0$. We have $f_2(x) \in f_2(M_{2,n_0}) = f_2(M_{2,n})$, so there exists $y \in M_{2,n}$ such that $f_2(x) = f_2(y)$. That is $f_2(x - y) = 0$, which, by exactness, implies that there exists a $z \in M_1$ such that $f_1(z) = x - y$. As $x - y \in M_{2,n_0}$, we have $z \in f_1^{-1}(M_{2,n_0}) = f_1^{-1}(M_{2,n})$. That is $f_1(z) = x - y \in M_{2,n}$, and thus $x \in M_{2,n}$. $\square$

Corollary 5.5. *The R-modules $M_1, \dots, M_n$ are Noetherian, (respectively Artinian) R-modules if and only if $\bigoplus_{i=1}^{n} M_i$ is Noetherian, (respectively Artinian).*

Proof. Apply induction on n and Proposition 5.4 for the short exact sequence

$$0 \to M_n \to \bigoplus_{i=1}^{n} M_i \to \bigoplus_{i=1}^{n-1} M_i \to 0.$$

$\square$

Definition 5.6. A ring R is Noetherian (respectively Artinian) if it is Noetherian (respectively Artinian) as an R-module. Equivalently, if the set of ideals of R satisfies the ascending chain condition (respectively the descending chain condition).

Examples.   1. A field is both Artinian and Noetherian.

2. Any finite ring is both Artinian and Noetherian. (for instance $\mathbb{Z}/n\mathbb{Z}$).

3. Every principal ideal domain is Noetherian, because every ideal is finitely generated. The ring of integers $\mathbb{Z}$ is thus Noehterian, but it is not Artinian (as we have seen in the previous list of examples).

4. The ring $\mathbb{K}[x_1, x_2, \dots]$ is not Noetherian, but it is a subring of its field of fractions which is Noetherian. Thus subrings of Noetherian rings need not be Noetherian.

5. The ring $\mathcal{C}(X)$ of real-valued continuous functions on a compact infinite Hausdorff space X is not Noetherian: Take a strictly decreasing sequence $F_1 \supsetneq F_2 \supsetneq \dots$ of closed sets in X and define the ideals $I_n := \{f \in \mathcal{C}(X) \mid f(F_n) = 0\}$. These form a non-stationary increasing chain.

Proposition 5.7. *Let R be a Noetherian (respectively Artinian) ring. If M is a finitely generated R-module, then M is Noetherian (respectively Artinian).*

Proof. By finite generation we have a short exact sequence

$$0 \to K \to R^n \to M \to 0.$$

and we conclude by Proposition 5.4 and Corollary 5.5. $\qquad\square$

Remark 5.8. Let I be an ideal of R, and M be an R-module, so M/IM is both an R/I-module and an R-module. Then, M/IM is Noetherian (respectively Artinian) as an R/I-module if and only if it is Noetherian (respectively Artinian) as an R-module. This follows because, a subgroup $N \subseteq M/IM$ is an R/I submodule if and only if $(R/I) \cdot N \subseteq N$ if and only if[1] $R \cdot N \subseteq N$. So the posets of R/I-submodules and R-submodules of M/IM coincide.

Proposition 5.9. *Let I be an ideal of the ring R. Being Noetherian (respectively Artinian) is bequeathed from R to the quotient ring R/I.*

Proof. Applying Proposition 5.4 to $\ 0 \to I \to R \to R/I \to 0$. implies R/I is a Noetherian (resepcitvely Artinian) R-module. Restricting scalars from R/I to R, we have that R/I is Noetherian also as an R/I-module. $\qquad\square$

5.2   Composition Series and Length of a Module

Let M be an R-module. A composition series of M is a finite maximal strictly increasing chain in $\mathcal{P}_{\subseteq}(M)$. That is a sequence of modules

$$0 = M_n \subsetneq M_{n-1} \subsetneq \dots \subsetneq M_1 \subsetneq M_0 = M \tag{5.1}$$

such that no further submodules can be inserted between any two consecutive $M_i \subsetneq M_{i-1}$. This is equivalent to M_{i-1}/M_i being a simple module, i.e. a module with no submodules other than 0 and itself. A composition series (or chain) as in (5.1) is said to have length n.

Denote for any R-module M the least length of a composition series by $\ell(M)$, with the convention that if M has no composition series then $\ell(M) = +\infty$.

Lemma 5.10. *Let M be an R-module. If $N \subsetneq M$, then $\ell(N) < \ell(M)$.*

---
[1] this is simply because $[r][n] = r[n] \in M/IM$.

Proof. Let $0 = M_n \subsetneq M_{n-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 = M$ be a composition series of M of minimum length. Define for every $i = 0 \ldots n$

$$N_i := M_i \cap N.$$

We have the composition of two natural maps: $\quad N_{i-1} \to M_{i-1} \to M_{i-1}/M_i \quad$ (without having a regular sequence!). The kernel of this composition is equal to $N_{i-1} \cap M_i = (M_{i-1} \cap N) \cap M_i = N_i$, so, by the universal property of the quotient module (Theorem 2.10), there is an injection $N_{i-1}/N_i \hookrightarrow M_{i-1}/M_i$. As M_{i-1}/M_i is simple, we have either $N_{i-1}/N_i = 0$ or $N_{i-1}/N_i = M_{i-1}/M_i$. Leaving out those N_i which are equal to N_{i-1} we obtain a composition series of N of length at most $\ell(M)$. We still need to show that it has to be strictly shorter, so assume it is not. That is

$$\frac{N_{i-1}}{N_i} = \frac{M_{i-1}}{M_i}, \quad \forall\, i = 1 \ldots n.$$

So, as $M_n = N_n = 0$, we have $M_{n-1} = N_{n-1}$, and so on until $M = M_0 = N_0 = N$ - a contradition. $\qquad \square$

Proposition 5.11. *Let M be an R-module having at least one composition series.*

(a) *Every strictly increasing chain of submodules of M has length $\leq \ell(M)$.*

(b) *Every composition series of M has length $\ell(M)$.*

(c) *Every strictly increasing chain of submodules can be extended to a composition series.*

Proof. (a) Assume $0 = M_k \subsetneq M_{k-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 = M$ is a chain of submodules of M of length k. By Lemma 5.10 we have $\ell(M) > \ell(M_1) > \cdots > \ell(M_k) = 0$, hence $\ell(M) \geq k$, thus $k = \ell(M)$.

(b) If we have a composition series of length n, then by definition we have $\ell(M) \leq n$ and by the previous point $\ell(M) \geq n$.

(c) Let now $0 = M_k \subsetneq M_{k-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 = M$ be a chain of submodules. By (a) we have $k \leq \ell(M)$. Thus, if $k = \ell(M)$, it must be maximal. If it is not maximal, than we may insert some $M_i \supsetneq M_i' \supsetneq M_{i-1}$ and repeat this procedure until we obtain a chain of length $\ell(M)$.

$\qquad \square$

Proposition 5.12. *An R-module M has a composition series if and only if M is both Artinian and Noetherian.*

Proof. $\boxed{\Rightarrow}$ All the strict chains in M have length at most $\ell(M)$ by Proposition 5.11.
$\boxed{\Leftarrow}$ Set $M_0 = M$. Using Noetherianity and Propostion 5.1, there exists a maximal element in $M_1 \in \mathcal{P}_{\subseteq}(M) \setminus \{M\}$, so $M_0 \supsetneq M_1$. Choose M_2 among the maximal elements of submodules of M strictly contained in M_1, and so on. Using now the Artinian property, we get that this strictly decreasing chain must become stationary (at 0), and we obtain thus a composition series of M. $\qquad \square$

Propositions 5.11 and 5.12 justify the following definition.

Definition 5.13. A module which is both Noetherian and Artinian is called **module of finite length**. In this case, the **length of a module** is the length of any of its composition series and is denoted by $\ell(M)$.

Remark 5.14. The Jordan-Hölder theorem applies to modules of finite length. That is the quotients of consecutive modules in any composition series is independent of the series.

Proposition 5.15. *The length of a module is an additive function (cf. Definition 2.40) on the class of R-modules of finite length.*

Proof. Let $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ be a short exact sequence of modules of finite length. We want to show that $\ell(M_2) = \ell(M_1) + \ell(M_3)$. Let $0 = M_{\ell_i,i} \subsetneq M_{\ell_i-1,i} \subsetneq \cdots \subsetneq M_{1,i} \subsetneq M_{0,i} = M$ be composition series for M_i for each $i = 1, 3$.

We first put together a composition series for M_2 using those of M_1 and M_3. First, as f_1 is injective, we have that

$$0 = f_1(M_{\ell_1,1}) \subsetneq f_1(M_{\ell_1-1,1}) \subsetneq \cdots \subsetneq f_1(M_{0,1}) \subseteq M_2$$

As f_2 is surjective, and $\mathrm{Ker}(f_2) = \Im(f_1)$ we also have

$$f_1(M_{0,1}) = f_1(M_1) = f_2^{-1}(0) = f_2^{-1}(M_{\ell_3,3}) \subsetneq f_2^{-1}(M_{\ell_1-1,3}) \subsetneq \cdots \subsetneq f_2^{-1}(M_{0,3}) \subseteq M_2.$$

Thus $\ell(M_1) + \ell(M_3) \leq \ell(M_2)$ by Propostion 5.11 (a).

If the chain of submodules of M_2 obtained by gluing the two above together would not be maximal, then either that of M_1 or that of M_3 would not have been maximal either and we conclude. $\square$

Proposition 5.16. *If V is a $\mathbb{K}$-vector space, then the following are equivalent:*

(a) *V has finite dimension.*

(b) *V has finite length.*

(c) *V is Noetherian.*

(d) *V is Artinian.*

Furthermore, $\dim_{\mathbb{K}} V = \ell(V)$.

Proof. $\boxed{\text{(a)} \Rightarrow \text{(b)}}$ Choose a basis $\{v_1, \ldots, v_d\}$ and construct the composition series

$$0 \subsetneq \langle v_1 \rangle \subsetneq \langle v_1, v_2 \rangle \subsetneq \cdots \subsetneq \langle v_1, \ldots, v_d \rangle = V.$$

$\boxed{\text{(b)} \Rightarrow \text{(c)}}$ Is given by Propostion 5.12. $\boxed{\text{(b)} \Rightarrow \text{(d)}}$ Is given by Propostion 5.12. $\boxed{\text{(c)} \Rightarrow \text{(a)}}$ Assume V is not finite dimensional. Then there exists an infinite sequence $(v_n)_{n \in \mathbb{N}}$ of linearly independent elements of V. Then the sequence

$$\langle v_0 \rangle \subsetneq \langle v_0, v_1 \rangle \subsetneq \ldots$$

would contradict the ascending chain condition. $\boxed{\text{(d)} \Rightarrow \text{(a)}}$ Works analogously by choosing the sequence

$$\langle v_0, v_1, \ldots \rangle \supsetneq \langle v_1, v_2, \ldots \rangle \subsetneq \ldots$$

$\square$

Corollary 5.17. *Let R be a ring in which the zero ideal is a product of not necessarily distinct maximal ideals: $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_n$. Then R is Noetherian if and only if R is Artinian.*

Proof. Set $V_i := \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1} / \mathfrak{m}_1 \cdots \mathfrak{m}_i$. Notice that V_i is an $R/\mathfrak{m}_i$-vector space (as a special case of M/IM is an R/I-module). In particular, by Proposition 5.16 being Noetherian is equivalent to being Artinian, and it is equivalent to having finite dimension. Furthermore, by Remark 5.8, V_i being Artinian (Noetherian) as a vector

space is equivalent to being Artinian (Noetherian) as an R-module.

Consider the following list of short exact sequences

$$0 \longrightarrow \mathfrak{m}_1 \longrightarrow R \longrightarrow R/\mathfrak{m}_1 \longrightarrow 0$$

$$0 \longrightarrow \mathfrak{m}_1\mathfrak{m}_2 \longrightarrow \mathfrak{m}_1 \longrightarrow \mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2 \longrightarrow 0$$

$$\vdots$$

$$0 \longrightarrow \mathfrak{m}_1 \cdots \mathfrak{m}_n \longrightarrow \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1} \longrightarrow \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_n \longrightarrow 0$$

By Proposition 5.4 on each short exact sequence we have

$$R \text{ is Noetherian} \quad \Leftrightarrow \quad \mathfrak{m}_1 \text{ and } R/\mathfrak{m}_1 \text{ are Noetherian}$$
$$\mathfrak{m}_1 \text{ is Noetherian} \quad \Leftrightarrow \quad \mathfrak{m}_1\mathfrak{m}_2 \text{ and } \mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2 \text{ are Noetherian}$$
$$\vdots$$
$$\mathfrak{m}_1 \ldots \mathfrak{m}_{n-1} \text{ is Noetherian} \quad \Leftrightarrow \quad \mathfrak{m}_1 \ldots \mathfrak{m}_n \text{ and } \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_n \text{ are Noetherian}$$

The same equivalences hold if we replace Noetherian with Artinian. If we start with R Noetherian, we get all the way down through the sequence of equivalences. For the quotients V_i being Noetherian is equivalent to being Artinian. So, to get back up, we only need that both modules on the right hand side in the last equivalence are Artinian. But $\mathfrak{m}_1 \ldots \mathfrak{m}_n = 0$, so Artinian, and we can climb back up through the equivalences and get that R is Artinian. Clearly this works both ways. $\qquad\square$

Recall from Exercise Sheet 6, Problem 1 that an R-module is simple (i.e. the only proper submodule is 0) if and only if there exists $\mathfrak{m} \in \mathrm{MaxSpec}(R)$ such that $M \simeq R/\mathfrak{m}$ as R-modules. From Exercise Sheet 8, Problem 4, recall that the **support** of an R-module M is the set

$$\mathrm{Supp}(M) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid M_\mathfrak{p} \neq 0\}.$$

Theorem 5.18 (Jordan-Hölder). *Let R be a ring and M a module of finite length and let*

$$0 = M_n \subsetneq M_{n-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M_0 = M$$

be a composition series of M. We have

(a) *$\mathfrak{m} \in \mathrm{Supp}(M) \Leftrightarrow \exists\, i \in 1, \ldots, n$ such that $M_{i-1}/M_i \simeq R/\mathfrak{m}$. In particular, all primes in the support are maximal.*

(b) *$\ell(M_\mathfrak{m}) = \sharp\{i \in 1, \ldots, n \mid \mathrm{Ann}(M_{i-1}/M_i) = \mathfrak{m}\}$.*

(c) *There is a canonical isomorphism*

$$M \longrightarrow \prod_{\mathfrak{m} \in \mathrm{Supp}(M)} M_\mathfrak{m}.$$

Proof. The key trick behind the proof comes from the exactness of localization (Proposition 3.10). This gives us for any prime ideal $\mathfrak{p}$ the chain

$$0 = (M_n)_\mathfrak{p} \subseteq (M_{n-1})_\mathfrak{p} \subseteq \cdots \subseteq (M_1)_\mathfrak{p} \subseteq (M_0)_\mathfrak{p} = M_\mathfrak{p}$$

For any maximal ideal $\mathfrak{m}$ we have from Remark 3.25 that

$$(R/\mathfrak{m})_\mathfrak{p} = \begin{cases} R/\mathfrak{m} & \text{if } \mathfrak{p} = \mathfrak{m} \\ 0 & \text{if } \mathfrak{p} \neq \mathfrak{m}. \end{cases}$$

Furthermore, as localization and quotients commute, we have for every i

$$(M_{i-1})_\mathfrak{p}/(M_i)_\mathfrak{p} \simeq (M_{i-1}/M_i)_\mathfrak{p} \simeq (R/\mathfrak{m})_\mathfrak{p}.$$

Combining these two observations we easily obtain points (a) and (b).

For Part (c), we get from the above that for two maximal ideals $\mathfrak{m}$ and $\mathfrak{m}'$ we have

$$(M_\mathfrak{m})_{\mathfrak{m}'} = \begin{cases} M_\mathfrak{m} & \text{if } \mathfrak{m} = \mathfrak{m}' \\ 0 & \text{if } \mathfrak{m} \neq \mathfrak{m}'. \end{cases}$$

Furthermore, by definition we have $M_\mathfrak{m} = 0$ if $\mathfrak{m} \notin \text{Supp}(M)$, so $\bigoplus_{\mathfrak{m} \in \text{MaxSpec}(R)} M_\mathfrak{m} = \bigoplus_{\mathfrak{m} \in \text{Supp}(M)} M_\mathfrak{m}$. Taking now the sum of the localization maps $M \longrightarrow M_\mathfrak{m}$ for all $\mathfrak{m} \in \text{MaxSpec}(M)$ we get

$$M \longrightarrow \bigoplus_{\mathfrak{m} \in \text{Supp}(M)} M_\mathfrak{m}.$$

By Proposition 3.16 it suffices to check that all localizations at maximal ideals are isomorphisms. Localization commutes with direct sums, so all these localizations are identity maps, and we conclude. $\square$

Chapter 6

Noetherian Rings

Recall that combining Definition 5.6 with Propositions 5.1 and 5.3 we have that a ring R is Noetherian if and only if one of the following equivalent conditions hold:

1. Every ascending chain of ideals of R is stationary.

2. Every nonempty set of ideals of R has a maximal element.

3. Every ideal in R is finitely generated.

Proposition 6.1. *Let $f : R \longrightarrow S$ be a surjective ring homomorphism. If R is Noetherian, then S is Noetherian.*

Proof. Since f is surjective, we have $S \cong R/\operatorname{Ker} f$ and we conclude by Proposition 5.9. $\square$

Proposition 6.2. *Let R be a subring of S. If R is Noetherian and S is finitely generated as an R-module, then S is also a Noetherian ring.*

Proof. By Proposition 5.7, S is a Noetherian R-module, hence it is Noetherian as a ring as well. $\square$

Example 6.3. The ring of integers $\mathbb{Z}$ is Noehterian, and the ring of Gaussian integers $\mathbb{Z}[i]$ is finitely generated as a $\mathbb{Z}$-module, hence it is Noetherian. His holds true for the ring of integers of every algebraic number field.

Proposition 6.4. *If R is Noetherian and U is a multiplicatively closed set, then $U^{-1}R$ is also Noetherian.*

Proof. Every ideal of $U^{-1}R$ is an extended ideal, so of the form $U^{-1}I$. Since R is Noetherian, I is finitely generated, say by $x_1, \ldots, x_r$. Then $\frac{x_1}{1}, \ldots, \frac{x_r}{1}$ generate the ideal $U^{-1}I$. $\square$

Corollary 6.5. *If R is a Noetherian ring and $\mathfrak{p}$ is a prime ideal, the the localization $R_{\mathfrak{p}}$ is also Noetherian.*

Theorem 6.6 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring, then the polynomial ring in one variable $R[x]$ is also Noetherian.*

Proof. We will prove that every ideal of $R[x]$ is finitely generated. For a polynomial of degree n the coefficient of x^n is called *leading coefficient* and is denoted by $LC(f)$. The set

$$L := \{LC(f) \mid f \in I\} \subseteq R$$

is obviously an ideal of R. Since R is Noetherian, L is finitely generated. Say $(c_1, \ldots, c_m) = L$. By definition, for each $i = 1, \ldots, m$ there exists $f_i \in R[x]$ such that

$$f_i = c_i x^{d_i} + \sum_{j=0}^{d_i - 1} b_{ij} x^j.$$

Let $d := \max\{d_1, \ldots, d_m\}$, and let $I' := (f_1, \ldots, f_m)$. We will show that

$$I = I' + (I \cap \langle 1, x, \ldots, x^{d-1} \rangle), \tag{6.1}$$

but first we will explain why it will be enough to conclude: The ideal I' is finitely generated by definition. The finitely generated R-module $\langle 1, x, \ldots, x^{d-1} \rangle$ is by Proposition 5.7 Noetherian, thus its R-submodule $I \cap \langle 1, x, \ldots, x^{d-1} \rangle$ is finitely generated. Hence, (6.1) describes I as a sum of two finitely generated R-submodules, which implies that I is finitely generated as an ideal. It thus remains only to prove (6.1), that is, that every $f \in I$ can be written as $f = g + h$ with $g \in I'$ and $h \in I \cap \langle 1, x, \ldots, x^{d-1} \rangle$.

Let $f \in I$ with $r := \deg f$. If $r < d$, then $f \in (I \cap \langle 1, \ldots, x^{d-1} \rangle)$ and we are done. If $r \geq d$, let $c = LC(f)$ and write

$$c = a_1 c_1 + \ldots a_m c_m, \quad \text{with } a_i \in R.$$

Hence, as $\deg f = r \geq d$, we can define

$$f' := f - a_1 f_1 x^{r-d_1} - \cdots - a_m f_m x^{r-d_m}.$$

By construction, the coefficient of x^r vanishes, so $\deg f' < \deg f$. After a finite number of steps we arrive at a degree lower than d, thus at a polynomial in $I \cap \langle 1, x, \ldots, x^{d-1} \rangle$, and we conclude. $\square$

Corollary 6.7. *If R is a Noetherian ring, then $R[x_1, \ldots, x_n]$ is Noetherian for any $n \in \mathbb{N}_{>0}$.*

Corollary 6.8. *If R is Noetherian, then any finitely generated R-algebra is Noetherian.*
In particular, any finitely generated ring and any finitely generated $\mathbb{K}$-algebra (where $\mathbb{K}$ is a field) is Noetherian.

Proof. For the first part, combine Corollary 6.7 with Proposition 6.1. For the second part, use the first part taking into account that $\mathbb{Z}$ and any field $\mathbb{K}$ are Noetherian. $\square$

6.1 Primary Decomposition In Noetherian Rings

An ideal I is called **irreducible** if

$$I = J \cap K \Rightarrow (I = J \text{ or } I = K)$$

Lemma 6.9. *In a Noetherian ring R every ideal is a finite intersection of irreducible ideals.*

Proof. Assume the set $\mathcal{C} = \{I \mid I \text{ ideal of } R \text{ which is not a finite intersection of irreducibles}\}$ is not empty. Then, as R is Noetherian, it has a maximal element: I_0. But then I_0 has to be reducible, thus $I_0 = J_1 \cap J_2$, with $I \subsetneq J_1$ and $I \subsetneq J_2$. So J_1, J_2 are not in $\mathcal{C}$, thus they are finite intersections of irreducible, and so must be I_0 - a contradiction. $\square$

Lemma 6.10. *In a Noetherian ring R every irreducible ideal is primary.*

Proof. By passing to the quotient ring, it is enough to show that if (0) is irreducible, then it is primary. So let $xy = 0$, and assume that $x \neq 0$. Consider the chain of ideal

$$\text{Ann}(y) \subseteq \text{Ann}(y^2) \subseteq \ldots$$

As R is Noetherian, there exists n such that

$$\text{Ann}(y^n) = \text{Ann}(y^{n+1}) = \ldots$$

Let now $a \in (x) \cap (y^n)$. From $a \in (x)$ it follows that $a = a'x$ so

$$ay = a'xy = 0.$$

From $a \in (y^n)$ it follows that $a = by^n$, so

$$0 = ay = by^{n+1}.$$

This means $b \in \mathrm{Ann}(y^{n+1}) = \mathrm{Ann}(y^n)$, so $a = by^n = 0$. Thus

$$(x) \cap (y^n) = (0)$$

Since (0) is irreducible we either have $x = 0$ or $y^n = 0$, thus (0) is primary. $\square$

Theorem 6.11. *In a Noetherian ring every ideal has a primary decomposition.*

The above theorem implies that all the results from Chapter 4 about rings in which a primary decomposition exists apply to Noetherian rings. Here are a few more results in this direction.

Proposition 6.12. *In a Noetherian ring every ideal contains a power of its radical.*

Proof. Let R be the Noetherian ring, and let $I \subseteq R$ be an ideal. We know by Noetheriantiy that $\sqrt{I}$ is finitely generated, and choose $a_1, \ldots, a_r$ generators of $\sqrt{I}$. For each of them, there exists an $n_i \in \mathbb{N}$ such that $a_i^{n_i} \in I$. Define

$$n := \sum_{i=1}^{r} (n_i - 1) + 1.$$

As $(\sqrt{I})^n = (a_1^{k_1} \cdots a_r^{k_r} \mid \text{with } k_1 + \cdots + k_r = n)$, we must have for each generator at least one i for which $k_i > n_i$. So each generator is in I and thus $(\sqrt{I})^n \subseteq I$. $\square$

Corollary 6.13. *In a Noetherian ring the nilradical is nilpotent.*

Corollary 6.14. *Let R be a Noetherian ring, $\mathfrak{m}$ be a maximal ideal of R and $\mathfrak{q}$ be any ideal of R. Then the following are equivalent:*

(a) $\mathfrak{q}$ *is* $\mathfrak{m}$-*primary.*

(b) $\sqrt{\mathfrak{q}} = \mathfrak{m}$.

(c) $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ *for some* $n \in \mathbb{N}_{>0}$.

Proof. The equivalence between (a) and (b) is given by definintion and Proposition 4.4.
(b)$\Rightarrow$ (c) is given by Proposition 6.12
(c)$\Rightarrow$ (b) is obtained by taking radicals in the chain of inclusions:

$$\mathfrak{m} = \sqrt{\mathfrak{m}^n} \subseteq \sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}.$$

$\square$

For Noetherian rings we can improve the First Uniqueness Theorem 4.9 as follows.

Proposition 6.15. *Let $I \subsetneq R$ be an ideal in the Noetherian ring R. We have*

$$\mathrm{Ass}(I) = \{I : x \mid x \in R\} \cap \mathrm{Spec}(R).$$

Proof. By passing to R/I we may assume that $I = 0$, and thus $I : x = 0 : x = \mathrm{Ann}(x)$. Let $\bigcap_{i=1}^{r} \mathfrak{q}_i = 0$ be a minimal primary decomposition, with $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. In the proof of Theorem 4.9 we have seen that

$$\sqrt{\mathrm{Ann}(x)} = \mathfrak{p}_i, \quad \forall \, 0 \neq x \in \bigcap_{\substack{i=1 \\ i \neq j}}^{r} \mathfrak{q}_i =: I_i.$$

$\boxed{\subseteq}$ By the above equality we have $\mathrm{Ann}(x) \subseteq \mathfrak{p}_i$. By Proposition 6.12 there exists $m \in \mathbb{N}$ such that $\mathfrak{p}^m \subseteq \mathfrak{q} \subseteq \mathfrak{p}$. So we have

$$I_i \mathfrak{p}_i^m \subseteq I_i \cap \mathfrak{p}_i^m \subseteq I_i \cap \mathfrak{q}_i = 0.$$

Let $m_0 = \min\{m \in \mathbb{N} \mid I_i \mathfrak{p}_i^m = 0\}$. So $I_i \mathfrak{p}_i^{m_0 - 1} \neq 0$. Choose $0 \neq x \in I_i \mathfrak{p}_i^{m_0 - 1}$. We have for this x that

$$\mathfrak{p}_i \cdot x = 0,$$

so $\mathfrak{p}_i \subseteq \mathrm{Ann}(x)$. As this x also lies in I_i, we have the other inclusion as well, so $\mathrm{Ann}(x) = \mathfrak{p}_i$.

$\boxed{\supseteq}$ If $\mathrm{Ann}(x) \in \mathrm{Spec}(R)$, then $\mathrm{Ann}(x) = \sqrt{\mathrm{Ann}(x)} \in \mathrm{Spec}(R)$, and we conclude by Theorem 4.9. $\qquad\square$

6.2 Noetherianity And Integrality

Warning: This section assumes some knowledge of Chapter 8.

Proposition 6.16. *Let $R \subseteq S \subseteq T$ be three rings. Assume that the following three conditions hold:*

(i) *R is Noetherian.*

(ii) *T is a finitely generated R-algebra.*

(iii) *T is a finitely generated S-module.*

Then S is a finitely generated R-algebra.

Proof. Let $t_1, \ldots, t_m$ be R-algebra generators of T and $y_1, \ldots, y_n$ be S-module generators of T. Then, there exist $s_{ij}, s_{ijk} \in S$ such that

$$t_i \;=\; \sum_{j=1}^{n} s_{ij} y_j \tag{6.2}$$

$$y_i y_j \;=\; \sum_{k=1}^{n} s_{ijk} y_k \tag{6.3}$$

Let S_0 be the R-algebra generated by the s_{ij} and the s_{ijk}. Since R is Noetherian, by Corollary 6.8, S_0 is Noetherian and $R \subseteq S_0 \subseteq S$.

Any element of T is the evaluation of a polynomial in $R[x_1, \ldots, x_m]$ at $(t_1, \ldots, t_m)$. Using (6.2), and then using (6.3) repeatedly we obtain each element of T as a linear combination of y_i with coefficients in S_0. So T is a finitely generated S_0-module. Since S_0 is Noetherian, by Propostion 5.7, T is a Noetherian S_0-module. Since S is an S_0-submodule of T, it is by Proposition 5.3 a finitely generated S_0-module. So, since S_0 is a finitely generated R-algebra, then so is S. $\qquad\square$

Proposition 6.17. *Let $\mathbb{K}$ be a field and E a finitely generated $\mathbb{K}$-algebra. If E is a field, then it is a finite algebraic extension of $\mathbb{K}$.*

Proof. Let $E = \mathbb{K}[a_1, \ldots, a_n]$. Assume that E is not algebraic, then relabel the a_i such that $a_1, \ldots, a_r$ are algebraically independent over $\mathbb{K}$, and for $i > r$ we have that a_i is algebraic over the field $F = \mathbb{K}(a_1, \ldots, a_r)$. Hence E is a finite algebraic extension of F, hence by 8.2 a finitely generated F-module. Then, by Proposition 6.16 for $\mathbb{K} \subseteq F \subseteq E$, we get that F is a finitely generated $\mathbb{K}$-algebra; say

$$F = \mathbb{K}[b_1, \ldots, b_m] \quad \text{with } b_i = \frac{f_i(a_1, \ldots, a_r)}{g_i(a_1, \ldots, a_r)},$$

with f_i, g_i polynomials.

There are infinitely many irreducible polynomials over a field, so we can choose an irreducible polynomial h which is prime to each $g_1, \ldots, g_r$ (take for instance $g_1 \ldots g_r + 1$). But then $\frac{1}{h(a_1, \ldots, a_r)} \in \mathbb{K}[b_1, \ldots, b_m]$, but, as $h(a_1, \ldots, a_r) \in F$ - we have a contradiction. So, our assumption that E was not algebraic was wrong, and we conclude. $\qquad \square$

Corollary 6.18 (The Weak Nullstellensatz)**.** *Let $\mathbb{K}$ be a field, and R be a finitely generated $\mathbb{K}$-algebra, and let $\mathfrak{m} \in \mathrm{MaxSpec}(R)$. Then $R/\mathfrak{m}$ is a finite algebraic extension of $\mathbb{K}$. In particular, if $\mathbb{K}$ is algebraically closed, then $R/\mathfrak{m} \simeq \mathbb{K}$.*

Proof. Take $E = R/\mathfrak{m}$ in Proposition 6.17. $\qquad \square$

6.3 Krull Dimension

The **Krull dimension** of a ring R is

$$\dim_{Krull} R := \sup\{k \in \mathbb{N} \mid \text{there exists prime ideals } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k\} \in \mathbb{N} \cup \{\infty\}.$$

Examples.   1. A field has Krull dimension zero, corresponding to a point being zero dimensional

2. A principal ideal domain, which is not a field, has Krull dimension one. In particular $\mathbb{K}[x]$ and $\mathbb{Z}$ have Krull dimension one.

3. The polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ has Krull dimension n. It is easy to see that $\dim_{Krull} \mathbb{K}[x_1, \ldots, x_n] \geq n$, but it takes some effort for the other direction.

4.

Chapter 7

Artinian Rings

Recall that a ring R is Artinian if its poset of ideals satisfies the descending chain condition, or equivalently the minimal condition. For modules being Artinian and being Noetherian were in way dual. We will see that for rings the Artinian condition is much stronger; in particular, we will see that Artinian rings are a special type of Noetherian rings. While Noetherian rings come with a mild form of finiteness (finite generation of all ideals), Artinian rings have a finite spectrum consisting only of maximal ideals. One may think of Artinian rings a simultaneous generalization of finite rings and of rings which are finite dimensional vector spaces over some field.

Remark 7.1. Every finite dimensional $\mathbb{K}$-algebra is Artinian. This means that R is a finite dimensional vector space, and every ideal is a $\mathbb{K}$-subspace. Thus every chain must terminate.

Proposition 7.2. *In an Artinian ring every prime ideal is maximal.*

Proof. Let R be an Artinian ring and $\mathfrak{p} \in \mathrm{Spec}(R)$. Then $R/\mathfrak{p}$ is an Artinian domain. Our aim is to show that it is a field, so let $0 \neq x \in R/\mathfrak{p}$. Considering the descending chain $(x) \supseteq (x^2) \supseteq \ldots$ we get that $(x^n) = (x^{n+1})$ for some $n \in \mathbb{N}$. So there exists $y \in \mathbb{R}/\mathfrak{p}$ such that $x^n = yx^{n+1}$. So we get $x^n(1 - xy) = 0$, and as $R/\mathfrak{p}$ is a domain, $xy = 1$. $\qquad\square$

Corollary 7.3. *In an Artinian ring the nilradical is equal to the Jacobson radical.*

Proposition 7.4. *An Artinian ring has only a finite number of maximal ideals.*

Proof. Consider the set of all finite intersections of maximal ideals. Then, by the minimal property, this set has a minimal element, say $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. We claim that these are all the maximal ideals: Let $\mathfrak{m}$ be some maximal. By minimality we must have

$$\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n.$$

Combining the above equality with $\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \subseteq \mathfrak{m}$ we get from prime avoidance (Lemma 1.39) that $\mathfrak{m}_i \subseteq \mathfrak{m}$ for some i, so, from the maximality of the ideal, $\mathfrak{m}_i = \mathfrak{m}$. $\qquad\square$

Proposition 7.5. *In an Artinian ring the nilradical is nilpotent.*

Proof. Let R be the Artinian ring. By the d.c.c we have there exists some $n \in \mathbb{N}_{>0}$ such that

$$\left(\sqrt{(0)}\right)^n = \left(\sqrt{(0)}\right)^{n+k}, \quad \forall\, k \in \mathbb{N}.$$

Denote by $I = \left(\sqrt{(0)}\right)^n$ and assume that $I \neq 0$. Notice that $I^2 = \left(\sqrt{(0)}\right)^{2n} = \left(\sqrt{(0)}\right)^n = I$, and define

$$\Sigma := \{J \subseteq R \mid JI \neq 0\}.$$

We have that $I \in \Sigma$, it is thus not empty. So, as R is Artinian, Σ must contain a minimal element. Let $J_0 \in \Sigma$ be one such element. As $J_0 I \neq 0$, there exists $a \in J_0$ such that $aI \neq 0$, equivalently $(a)I \neq 0$. So, as $(a) \subseteq J_0$, by minimality we have $J_0 = (a)$. On the other hand, we also have $(aI)I = aI^2 = aI \neq 0$, so $aI \in \Sigma$. Since $aI \subseteq (a) = J_0$, again by minimality, we have $aI = (a)$. This implies there exists $b \in I$ such that

$$a = ab.$$

Multiplying this equality repeatedly with b we obtain

$$a = ab = ab^2 = \cdots = ab^m = \ldots$$

As $b \in I = \sqrt{(0)}$ we obtain that $a = 0$ - a contradiction. $\qquad\square$

Theorem 7.6. *A ring R is Artinian if and only if it is Noetherian of Krull dimension zero.*

An alternative phrasing would be: R is Artinian iff and only if R is Noetherian and all prime ideals are maximal.

Proof. $\boxed{\Rightarrow}$ By Proposition 7.2 we have $\dim R = 0$. By Proposition 7.4 $\mathrm{Spec}(R) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$ for some r with $\mathfrak{m}_i$ maximal ideals. Then, by Proposition 7.5, there exists some $k \in \mathbb{N}$ such that

$$\prod_{i=1}^{r} \mathfrak{m}_i^k \subseteq \Big(\bigcap_{i=1}^{r} \mathfrak{m}_i \Big)^k = \Big(\sqrt{(0)} \Big)^k = 0.$$

By Corollary 5.17, as R is Artinian it must also be Noetherian.
$\boxed{\Leftarrow}$ Since R is Noetherian, each ideal has a primary decomposition by Theorem 6.11. In particular, the zero ideal has one, and thus R has only finitely many minimal primes. Since $\dim R = 0$, all the minimal primes are maximal ideals. So, this time by Corollary 6.13, we have that the nilradical is nilpotent, and using the same argument as above we can use again Corollary 5.17. $\qquad\square$

Corollary 7.7. *A ring R is Artinian if and only if it has finite length as an R-module.*

Proof. This follows from Theorem 7.6 and Proposition 5.12. $\qquad\square$

Remark 7.8. If $(R, \mathfrak{m})$ is an Artinian local ring, then we have

1. $\mathrm{Spec}(R) = \{\mathfrak{m}\}$.

2. $\sqrt{(0)} = \mathfrak{m}$.

3. $\mathfrak{m}$ is nilpotent.

4. If $x \in A$, then either x is nilpotent or x is a unit.

Examples. $\mathbb{Z}/(p^n)$, $\mathbb{K}[\epsilon]/(\epsilon^n)$, $\mathbb{K}[x,y]/(x^2, xy, y^2)$.

Proposition 7.9. *Let $(R, \mathfrak{m})$ be A Noetherian local ring. Exactly one of the following statements are true:*

(a) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ *for all $n \in \mathbb{N}$.*

(b) $\mathfrak{m}^n = 0$ *for some n, in which case R is Artinian.*

Proof. Suppose $\mathfrak{m}^n = \mathfrak{m}^{n+1} = \mathfrak{m} \cdot \mathfrak{m}^n$. As R is Noetherian, $\mathfrak{m}$ is finitely generated, and as it is local, $\mathfrak{m} = \mathcal{J}_R$ is the Jacobson radical. So we may apply Nakayama's Lemma 2.27 and obtain $\mathfrak{m}^n = 0$. To show it is Artinian, we will use Theorem 7.6, and show that $\dim R = 0$ by showing there are no other primes besides $\mathfrak{m}$: Let $\mathfrak{p} \in \mathrm{Spec}(R)$. Then $\mathfrak{m}^n = 0 \subseteq \mathfrak{p}$, so, taking radicals, we get $\mathfrak{m} \subseteq \mathfrak{p}$, i.e. $\mathfrak{m} = \mathfrak{p}$ (because $\mathfrak{m}$ is maximal). $\qquad\square$

Remember that having just one maximal ideal is not enough to conclude Artinian.

Theorem 7.10 (Structure of Artinian Rings). *A ring R is Artinian if and only if it is a finite direct product of local Artinian rings. Furthermore, if R is Artinian, the decomposition as product of local Artinian rings is unique (up to permutation of factors).*

Proof. If R is a product of Artinian rings, as each ring can be regarded as an R-module via the canonical projection, we get by Corollary 5.5 that R is Artinian as well.

For the other direction, assume R is Artinian. Since R has finite length as a module over itself, by the Jordan-Hölder Theorem we have that

$$R \simeq \bigoplus_{\mathfrak{m} \in \mathrm{Supp}(R)} R_{\mathfrak{m}}$$

as R-modules. Since $\mathrm{Supp}(R) = \mathrm{Spec}(R) = \mathrm{MaxSpec}(R)$ and it is finite by Proposition 7.4, we have that

$$\bigoplus_{\mathfrak{m} \in \mathrm{Supp}(R)} R_{\mathfrak{m}} = \prod_{\mathfrak{m} \in \mathrm{MaxSpec}(R)} R_{\mathfrak{m}}.$$

Furthermore, the isomorphism was given as the sum of the localization maps $R \longrightarrow R_{\mathfrak{m}}$, which are all ring homomorphisms, so we conclude.

Finally, let us prove the uniqueness. Assume $R = \prod_{i=1}^{n} R_i$ with $(R_i, \mathfrak{q}_i)$ Artinian local rings. We have the natural surjection $\phi_i : R \longrightarrow R_i$ for each $i = 1, \ldots, n$ and let us denote by $I_i := \mathrm{Ker}\, \phi_i$. So we have $R_i \simeq R/I_i$ with $\phi : R \longrightarrow \prod_{i=1}^{n} R/I_i$ given by $\phi(x) = (x + I_1, \ldots, x + I_n)$ which puts us in the situation of Proposition 1.37. As ϕ is bijective, we get by this proposition that $I_i + I_j = R$ for any $i \neq j$ (from surjectivity) and $\bigcap_{i=1}^{n} I_i = 0$ from injectivity.

Let $\mathfrak{m}_i := \phi^{-1}(\mathfrak{q}_i)$. As the preimage of a prime is prime, $\mathfrak{m}_i$ is prime, and because R is Artinian it is also maximal.

*C*laim: I_i is $\mathfrak{m}_i$-primary.

For this, as $\mathfrak{m}_i$ is maximal, it is enough to show $\sqrt{I_i} = \mathfrak{m}_i$. Let $x \in \sqrt{I_i}$. So, there exists r such that $x^r \in I_i$, that is, such that $\phi_i(x^r) = (\phi_i(x))^r = 0$. But $\mathfrak{q}_i$ is the nilradical of R_i, so $\phi_i(x) \in \mathfrak{q}_i$, that is $x \in \mathfrak{m}_i$.

Now, since $\bigcap_{i=1}^{n} = (0)$, we have a primary decomposition of the zero ideal in R. Since the I_i are pairwise coprime, so are the $\mathfrak{m}_i$, thus they are exactly the minimal primes or R. Hence, by the second uniqueness theorem of primary decompositions (Theorem 4.16), all the isolated primary components of I_i are uniquely determined by I_i. Hence the rings $R_i = R/I_i$ are uniquely determined by R. $\qquad\square$

In general, for any local ring $(R, \mathfrak{m})$, if $\mathcal{K} = R/\mathfrak{m}$ is the residue field, we have that $\mathfrak{m}/\mathfrak{m}^2$ is a $\mathcal{K}$-vector space. Using the canonical projection $\mathfrak{m} \longrightarrow \mathfrak{m}/\mathfrak{m}^2$, we have that if $\mathfrak{m}$ is finitely generated, then $\dim_{\mathcal{K}} \mathfrak{m}/\mathfrak{m}^2 < \infty$. Recall that the local version of the Nakayama Lemma (Proposition 2.32) says that in the finitely generated case the dimension is equal to the cardinality of (any) minimal set of generators of $\mathfrak{m}$.

Proposition 7.11. *Let $(R, \mathfrak{m})$ be an Artinian local ring. The following are equivalent:*

(a) *Every ideal in R is principal.*

(b) *The maximal ideal $\mathfrak{m}$ is principal.*

(c) $\dim_{\mathcal{K}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

Proof. $\boxed{(a) \Rightarrow (b)}$ is trivial.

$\boxed{(b) \Leftrightarrow (c)}$ is given by Nakayama for local rings.

$\boxed{(b) \Rightarrow (a)}$ Say $\mathfrak{m} = (x)$, and let $I \subseteq R$ be an ideal different from (0) or (1). Since $(R, \mathfrak{m})$ is an Artinian local

ring, we have by Remark 7.8 $\mathfrak{m} = \sqrt{(0)}$, so there exists some $n \in \mathbb{N}$ such that $\mathfrak{m}^n = (0) \subsetneq I$. As $I \subseteq \mathfrak{m}$, there must exist some $k \in \mathbb{N}$ such that

$$I \subseteq \mathfrak{m}^k = (x^k) \text{ and } I \not\subseteq \mathfrak{m}^{k+1} = (x^{k+1}).$$

So there exists $y \in I$ and $r \in R$ such that $y = r \cdot x^k$, with $r \notin (x) = \mathfrak{m}$. So r is a unit (by Remark 7.8) and thus $x^k = r^{-1}y \in I$. So $\mathfrak{m}^k = (x^k) \subseteq I \subseteq \mathfrak{m}^k$, thus $I = (x^k)$ is principal. $\qquad \square$

Chapter 8

Integral Dependence

8.1 Basics

Let R be a subring of S (recall that subrings must contain 1.)

Definition 8.1. An element $s \in S$ is **integral** over R if it is the root of a monic polynomial with coefficients in R, that is if there exists $n \in \mathbb{N}_{>0}$ and $r_0, \ldots, r_{n-1} \in R$ such that

$$s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0. \tag{8.1}$$

In this case (8.1) is called an **equation of integral dependence** of an **integral equation** of s over R.

Examples. 1. Every element of R is integral over R.

2. Let $a/b \in \mathbb{Q}$, with $\gcd(a,b) = 1$, is integral over $\mathbb{Z}$ then there exist $c_0, \ldots, c_{n-1} \in \mathbb{Z}$ such that

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0,$$

so b divides a, thus it can only be 1 or -1. So the only integral rational numbers over $\mathbb{Z}$ are the integers themselves.

3. The elements of $\mathbb{Q}[i]$ integral over $\mathbb{Z}$ are the Gaussian integers.

4. The complex numbers integral over $\mathbb{Z}$ are called algebraic integers.

5.

Proposition 8.2. *Let R be a subring of S, and $s \in S$. The following are equivalent:*

(a) *The element s is integral over R.*

(b) *The R-algebra $R[s]$ generated by s is a finitely generated R-module.*

(c) *There exists a subring S' of S such that $R[s] \subseteq S' \subseteq S$, and S' is a finitely generated R-module.*

(d) *There exists a faithful $R[s]$-module M which is finitely generated as an R-module.*

Proof. $\boxed{\text{(a)}\Rightarrow\text{(b)}}$ Assume that $s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0$. So for every $k \geq 0$ we get s^{n+k} as an R-linear combination of the first n powers of s. Thus $R[s] = \mathrm{Span}_R(1, \ldots, s^{n-1})$.
$\boxed{\text{(b)}\Rightarrow\text{(c)}}$ Take $S' = R[s]$.
$\boxed{\text{(c)}\Rightarrow\text{(d)}}$ Take $M = S'$. This is faithful, as $1 \in S'$.

$\boxed{(d) \Rightarrow (a)}$ This follows from Cayley-Hamilton (more exactly from Corollary 2.25): Take the finitely generated R-module M, multiplication by s as the endomorphism $\varphi \in \mathrm{End}_R(M)$, and $I = R$ as the ideal for which $\varphi(M) \subseteq IM$. The latter holds, since M is an $R[s]$-module, so $sM \subseteq M$. So we have by Corollary 2.25 that there exist $r_0, \ldots, r_{n-1} \in R$ such that $\varphi^n + r_{n-1}\varphi^{n-1} + \cdots + r_1\varphi + r_0 \, \mathrm{id}_M = 0$. Since M is faithful, we conclude that the same must hold for s. $\qquad \square$

Corollary 8.3. *Let R be a subring of S, and $s_1, \ldots, s_n \in S$ be integral over R. Then the ring $R[s_1, \ldots, s_n]$ is a finitely generated R-module.*

Proof. Induction on n. $\qquad \square$

Corollary 8.4. *Let R be a subring of S. The set*

$$C = \{s \in S \mid s \text{ is integral over } R\} \tag{8.2}$$

forms a subring of S which contains R.

Proof. Let $s_1, s_2 \in S$ be integral over R. It is enough to show that $s_1 \pm s_2$ and $s_1 s_2$ are also integral. By Corollary 8.3 the R-algebra $R[s_1, s_2]$ is a finitely generated R-modules. As it contains $s_1 \pm s_2$ and $s_1 s_2$, we conclude by Proposition 8.2 (c). $\qquad \square$

Definition 8.5. Let R be a subring of S.

1. The ring C from (8.2) is the **integral closure** of R in S.

2. If $C = R$, then R is called **integrally closed** in S.

3. If $C = S$, then S is called **integral** over R.

4. A domain R is simply called *integrally closed* (without mentioning where) if it is integrally closed in its field of fractions.

More generally, if $f : R \longrightarrow S$ is a ring homomorphism, so S is an R-algebra, we have:

4. if S is integral over $f(R)$, then the morphism f is said to be **integral**, and S is called an integral R-algebra.

Remark 8.6. Recall that an R-algebra S is *finite* if it is finitely generated as an R-module, and of *finite type* if it is finitely generated as an algebra. So, essentially we have proved that for algebras we have:

$$\text{finite type} + \text{integral} \; \Rightarrow \; \text{finite}.$$

Corollary 8.7. *If $R \subseteq S \subseteq T$ are three rings, and S is integral over R and T is integral over S, then T is integral over R.*

Proof. Let $t \in T$. Since T is integral over S, we have $s_1, \ldots, s_n \in S$ such that

$$t^n + s_1 t^{n-1} + \cdots + s_n = 0.$$

Let $S' = R[s_1, \ldots, s_n]$. Then, t is integral over S', so $S'[t]$ is a finitely generated S'-module. By Corollary 8.3, S' is a finitely generated R-module. By Proposition 2.48 we have that $S'[t]$ is a finitely generated R-module, so we conclude by Proposition 8.2. $\qquad \square$

Corollary 8.8. *Let $R \subseteq S$ be rings, and C be the integral closure of R in S. Then C is integrally closed in S.*

Proof. If $s \in S$, is integral over C, then by Corollary 8.7 s is integral over R, so $s \in C$. $\qquad \square$

The next result shows that integral dependence is preserved by quotients and localizations.

Proposition 8.9. *Let $R \subseteq S$ be rings. Let $J \subseteq S$ be an ideal and $I = I^c = J \cap R$ its contraction. Let also U^{-1} be a multiplicatively closed set of R.*

(a) *If S is integral over R, then S/J is integral over R/I and $U^{-1}S$ is integral over $U^{-1}R$.*

(b) *If C is the integral closure of R in S, then $U^{-1}C$ is the integral closure of $U^{-1}R$ in $U^{-1}S$.*

Proof. (a) Take $s \in S$, with the equation $s^n + r_1 s^{n-1} + \cdots + r_n = 0$. Then moding out I solves the first part, and taking r_i/u^i gives the equation for s/u.

(b) By the first part $U^{-1}C$ is integral over $U^{-1}R$. So let $s/u \in U{-}1S$ be integral over $U^{-1}R$. That is we have

$$\frac{s^n}{u} + \frac{r_1}{u_1}\frac{s^{n-1}}{u} + \cdots + \frac{r_n}{u_n} = 0.$$

Multiplying the above equation with $(u \cdot u_1 \cdots u_n)^n$ gives an integral equation of $su_1 \ldots u_n$ over R, so $su_1 \ldots u_n \in C$, and hence $\frac{s}{u} = \frac{su_1\ldots u_n}{uu_1\ldots u_n} \in U^{-1}C$. $\square$

8.2 The Going Up Theorem

Proposition 8.10. *Let $R \subseteq S$ be domains, with S integral over R. Then S is a field if and only if R is a field.*

Proof. $\boxed{\Rightarrow}$ Let $r \in R \setminus \{0\}$, which has an inverse $r^{-1} \in S$, which is a field. As S is integral over R, we have

$$(r^{-1})^m + a_1(r^{-1})^{m-1} + \cdots + a_m = 0,$$

with $a_i \in R$. Multiplying the above by r^{m-1} one gets

$$r^{-1} = -a_1 - a_2 r - \cdots - a_m r^{m-1} \in R.$$

$\boxed{\Leftarrow}$ Let $s \in S \setminus \{0\}$, and consider an integral relation of minimal degree:

$$s^n + r_1 s^{n-1} + \cdots + r_n = 0$$

As S is a domain, $r_n \neq 0$ (otherwise, we have s a common nonzero factor, and then use that R is a field to obtain an integral dependence relation of smaller degree). Then we get

$$s \cdot \left(r_n^{-1}(r_1 s^{n-1} + \cdots + r_{n-1})\right) = 1.$$

So s is invertible. $\square$

Corollary 8.11. *Let $R \subseteq S$ be rings with S integral over R. Let $\mathfrak{q} \in \mathrm{Spec}(S)$ and $\mathfrak{p} = R \cap \mathfrak{q}$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. By Proposition 8.9 we have the domain $S/\mathfrak{q}$ integral over the domain $R/\mathfrak{p}$, and we conclude by Proposition 8.10. $\square$

Corollary 8.12. *Let $R \subseteq S$ be rings with S integral over R. If $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec}(S)$ with $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q} \cap R = \mathfrak{q}' \cap R$. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Denote by $\mathfrak{p} := \mathfrak{q} \cap R$. By Proposition 8.9 $S_{\mathfrak{p}}$ is integral over $R_{\mathfrak{p}}$. Now $\mathfrak{p}^e \in R_{\mathfrak{p}}$ is maximal, and it is $\mathfrak{p}^e = \mathfrak{q}^e \cap R_{\mathfrak{p}} = \mathfrak{q}'^e \cap R_{\mathfrak{p}}$. We conclude by the description of ideals in the localization and Corollary 8.11. $\square$

Theorem 8.13. *Let $R \subseteq S$ be rings with S integral over R, and let $\mathfrak{p} \in \mathrm{Spec}\, R$. Then there exists $\mathfrak{q} \in \mathrm{Spec}\, S$ such that $\mathfrak{p} = \mathfrak{q} \cap R$.*

Proof. Consider the commutative diagram with injective horizontal arrows (because R is a subring).

$$\begin{array}{ccc} R & \longhookrightarrow & S \\ \downarrow & & \downarrow \\ R_{\mathfrak{p}} & \longhookrightarrow & S_{\mathfrak{p}} \end{array}$$

Let $\mathfrak{n}$ be some maximal ideal of $S_{\mathfrak{p}}$. By Corollary 8.11 $\mathfrak{n} \cap R_{\mathfrak{p}}$ is also maximal, so it must be $\mathfrak{p}^e$ - the unique maximal ideal of $R_{\mathfrak{p}}$. Taking the vertical contraction of $\mathfrak{n}$ in S we get a prime ideal $\mathfrak{q} \subseteq S$, whose contraction (by commutativity of the diagram) is the contraction of $\mathfrak{p}^e$, which is $\mathfrak{p}$. $\square$

Theorem 8.14 (Going Up)**.** *Let $R \subseteq S$ be rings with S integral over R, and let $\mathfrak{p} \in \operatorname{Spec} R$. Let $0 \leq m < n \in \mathbb{N}$, $\mathfrak{p}_i \in \operatorname{Spec} R$ for $i = 1, \ldots, n$ and $\mathfrak{q}_j \in \operatorname{Spec} S$ for $j = 1, \ldots, m$ with the property that*

$$\mathfrak{p}_j = \mathfrak{q}_j \cap R, \quad \forall\, j = 1, \ldots, m,$$

and with the chains of primes:

$$\begin{array}{ccccccccc} \mathfrak{p}_1 & \subseteq & \ldots & \subseteq & \mathfrak{p}_m & \subseteq & \ldots & \subseteq & \mathfrak{p}_n \\ \mathfrak{q}_1 & \subseteq & \ldots & \subseteq & \mathfrak{q}_m & & & & \end{array}.$$

Then, there exist $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n \in \operatorname{Spec} S$ with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all $i = m+1, \ldots, n$ and

$$\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m \subseteq \mathfrak{q}_{m+1} \subseteq \ldots \subseteq \mathfrak{q}_n.$$

Proof. Using induction, the whole theorem can be deduced from the case $m = 1$ and $n = 2$. Using Proposition 8.9 we reduce the statement to a statement about $R/\mathfrak{p}_1$ and $S/\mathfrak{q}_1$. Then we use Theorem 8.13 to deduce the existence of $\mathfrak{q}_2' \subseteq S/\mathfrak{q}_1$, and then the correspondence between $\operatorname{Spec} S$ and $\operatorname{Spec} S/\mathfrak{q}_1$ to conclude. $\square$

8.3   The Going Down Theorem

In this part we focus on integral domains, for which being integrally closed (in their field of fractions cf. Definition 8.5) is a local property.

Proposition 8.15. *Let R be an integral domain. The following are equivalent.*

(a) *R is integrally closed.*

(b) *$R_{\mathfrak{p}}$ is integrally closed for every $\mathfrak{p} \in \operatorname{Spec} R$.*

(c) *$R_{\mathfrak{m}}$ is integrally closed for every $\mathfrak{m} \in \operatorname{MaxSpec} R$.*

Proof. Let C be the integral closure of R in $(R \setminus \{0\})^{-1})R$. Thus we have an injective map $R \hookrightarrow C$. Thus being integrally closed is equivalent to the map being surjective. Combining now Proposition 8.9 part (ii) with surjectivity being a local property (Proposition 3.16) we conclude. $\square$

Definition 8.16. Let $R \subseteq S$ be rings and $I \subseteq R$ be an ideal. An element $s \in S$ is called **integral over I** if it satisfies an equation of integral dependence

$$s^n + a_1 s^{n-1} + \cdots + a_n = 0, \quad \text{with } a_i \in I \; \forall\, i = 1, \ldots, n.$$

The integral closure of I in S is the set

$$\overline{I} := \{s \in S \mid s \text{ is integral over } I\}.$$

Notice that one has to be careful when using this notation, as the closure depends on S. If no S is mentioned, then we understand that $S = R$.

Lemma 8.17. *Let $R \subseteq S$ be rings, $I \subseteq R$ be an ideal of R and let C be the integral closure of R in S. Denote by I^e the extension of I in C and by $\overline{I}$ the integral closure of I in S. We have*

$$\overline{I} = \sqrt{I^e}.$$

Proof. $\boxed{\subseteq}$ If $s \in C$ is integral over I, then we have $a_1, \dots, a_n \in I$ such that

$$s^n + a_1 s^{n-1} + \cdots + a_n = 0,$$

so $s^n \in I^e$.

$\boxed{\supseteq}$ Let $s \in \sqrt{I^e}$, so there exists $n \in \mathbb{N}$ such that $s^n \in I^e$, that is $s^n = \sum_{i=1}^r a_i s_i$ with $a_i \in I$ and $s_i \in C$. Since all the s_i are integral over R, we have by Corollary 8.3 that $M = R[s_1, \dots, s_r]$ is a finitely generated R-module. So we have $x^n M \subseteq IM$, so byCayley-Hamilton (Corollary 2.25 (a)) we have that s^n is integral over I, thus also s is integral over I. $\qquad\square$

Proposition 8.18. *Let $R \subseteq S$ be domains, with $\mathcal{K} =$ the field of fractions of R, and let $I \subseteq R$ be an ideal. Assume that R is integrally closed, and that $s \in S$ is integral over I. Then s is algebraic over $\mathcal{K}$, and if its minimal polynomial over $\mathcal{K}$ is*

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

, then $a_i \in \sqrt{I}$ for $i = 1, \dots, n$.

Proof. Clearly s is algebraic over $\mathcal{K}$. Let's now consider an extension field $\mathcal{K} \subseteq \mathcal{L}$, with the property that all the conjugates of s (i.e. the other roots of the minimal polynomial), say $s = s_1, \dots, s_n$ belong to $\mathcal{L}$. So, as all these conjugates satisfy the same equation, they are all integral over I. The coefficients of the minimal polynomial can be expressed as sums of products of the s_i (actually as the elementary symmetric polynomials evaluated at the s_i). So, by Lemma 8.17 they all belong to $\sqrt{I^e}$. But since R is integrally closed, $I = I^e$. $\qquad\square$

Theorem 8.19 (Going Down). *Let $R \subseteq S$ be integral domains, with R integrally closed (in its field of fractions) and S integral over R. Let $0 \le m < n \in \mathbb{N}$, $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ be a chain of prime ideals of R, and $\mathfrak{q}_1 \supseteq \mathfrak{q}_m$ be a chain of prime ideals of S such that*

$$\mathfrak{q}_i \cap R = \mathfrak{p}_i, \quad \forall \, i = 1, \dots, m.$$

The chain $\mathfrak{q}_1 \supseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \supseteq \mathfrak{q}_m \supseteq \cdots \supseteq \mathfrak{q}_n$ of primes of S such that $\mathfrak{q}_j \cap R = \mathfrak{p}_j$ for all $j = m+1, \dots, n$.

Proof. By induction, we reduce (again) the proof to the case $m = 1$ and $n = 2$. We want to show that $\mathfrak{p}_2$ is the contraction of a prime of $S_{\mathfrak{q}_1}$. By Proposition 3.28 it is equivalent to proving that $\mathfrak{p}_2^{ec} = (\mathfrak{p}_2^e)^c = (S_{\mathfrak{q}_1} \cdot \mathfrak{p}_2) \cap R = \mathfrak{p}_2$, which by Proposition 1.44 boils down to the inclusion from left to right. So choose one element $\frac{s}{u} \in \S_{\mathfrak{q}_1} \cdot \mathfrak{p}_2$. We have

$$S_{\mathfrak{q}_1} \cdot \mathfrak{p}_2 = \{ \frac{s}{u} \mid a \in S \cdot \mathfrak{p}_2 \text{ and } u \in S \setminus \mathfrak{q}_1 \}.$$

So s is integral over $\mathfrak{p}_2$ by Lemma 8.17. By Proposition 8.18, we have that s is algebraic over $\mathcal{K}$ - the field of fractions of R - with minimal polynomial

$$s^r + a_1 s^{r-1} + \cdots + a_r = 0, \text{ with } a_i \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2. \tag{8.3}$$

Assume furthermore, that $x = \frac{s}{u} \in S_{\mathfrak{q}_1} \mathfrak{p}_2 \cap R$. Then, computing in $\mathcal{K}$, we have $u = sx^{-1}$. So, we obtain a minimal algebraic expression of u over $\mathcal{K}$ by multiplying (8.3) by x^{-r}:

$$(sx^{-1})^r + a_1 x^{-1}(sx^{-1})^{r-1} + \cdots + a_r x^{-r} = 0 \tag{8.4}$$
$$u^r + b_1 u^{r-1} + \cdots + b_r = 0 \tag{8.5}$$

where $b_i := a_i x^{-i} \in \mathcal{K}$, thus

$$b_i x^i = a_i \in \mathfrak{p}_2, \quad \forall \, i = 1, \dots, r. \tag{8.6}$$

But $u \in S$ is integral over R, and applying Proposition 8.18 with $I = (1)$ we get that each of the b_i must actually belong to R.

Assume now that $x \notin \mathfrak{p}_2$. Then by (??) we have $b_i \in \mathfrak{p}_2$ for all $i = 1, \ldots, r$. So by (8.5) we have that

$$u^r \in S \cdot \mathfrak{p}_2 \subseteq S \cdot \mathfrak{p}_1 \subseteq \mathfrak{q}_1$$

thus $u \in \mathfrak{q}_1$ - a contradiction to $u \in S \setminus \mathfrak{q}_1$.

Hence $x \in \mathfrak{p}_2$ and we conclude. $\qquad\qquad\square$

8.4 Noether Nomralization

Let $\mathbb{K}$ be a field and A be a $\mathbb{K}$-algebra. A set of elements $y_1, \ldots, y_m \in A$ are **algebraically independent**, if they do not satisfy any polynomial equation with coefficients in $\mathbb{K}$. In other words, if

$$\forall\ f \in \mathbb{K}[x_1, \ldots, x_m], f \neq 0 \Rightarrow f(y_1, \ldots, y_m) \neq 0.$$

This is equivalent to the evaluation map $\mathrm{ev}_{y_1, \ldots, y_m} : \mathbb{K}[x_1, \ldots, x_m] \longrightarrow \mathbb{K}[y_1, \ldots, y_m]$ being an isomorphism.

Throughout the literature, there are different formulations of Noether Normalization to be found. You are strongly encouraged to check them out and understand how they connect ([AM69, Chapter V, Exercise 16, p.69], [Eis95, Theorem 4.14, p.127], [AK17, Lemma 15.1, p.108]. We will present here the version we find to be most friendly, which can be found in [Hul03, Theorem 1.24, p.30]:

Theorem 8.20 (Noether normalization)**.** *Let $\mathbb{K}$ be an infinite field and $A = \mathbb{K}[a_1, \ldots, a_n]$ be a finitely generated $\mathbb{K}$-algebra. Then there exist $y_1, \ldots, y_m \in A$, with $m \leq n$ such that*

(a) *$y_1, \ldots, y_m$ are algebraically independent over $\mathbb{K}$, and*

(b) *A is a finite $\mathbb{K}[y_1, \ldots, y_m]$-algebra.*

We consider the following lemma, the proof of which we refer to [Hul03, Lemma 1.23].

Lemma 8.21. *Let $0 \neq f \in \mathbb{K}[x_1, \ldots, x_n]$ be a polynomial of degree d. There exist $\alpha_1, \ldots, \alpha_{n-1} \in \mathbb{K}$ giving a change of variables*
$$x_i' := x_i - \alpha_i x_n, \quad \forall\ i = 1, \ldots, n-1,$$
such that the polynomial $f(x_1' + \alpha_1 x_n, \ldots, x_{n-1}' + \alpha_{n-1} x_n, x_n) \in \mathbb{K}[x_1', \ldots, x_{n-1}', x_n]$ as a term of the form $c x_n^d$ with $c \in \mathbb{K} \setminus \{0\}$.

We give only an example instead of a proof: Let $f = x_1 x_2 - x_2 x_3 + x_1 + x_2 + x_3 \in \mathbb{K}[x_1, x_2, x_3]$, so $n = 3$ and $d = 2$. We can choose for instance $\alpha_1 = -1$, $\alpha_2 = 1$ and obtain:

$$
\begin{aligned}
f(x_1' - x_3, x_2' + x_3, x_3) &= (x_1' - x_3)(x_2' + x_3) - (x_2' + x_3)x_3 + x_1' - x_3 + x_2' + x_3 + x_3 \\
&= \mathbf{-2x_3^2} + x_1' x_3 - 2x_2' x_3 + x_1' x_2' + x_1' + x_2' + x_2' + x_3'
\end{aligned}
$$

Notice that any choice with $\alpha_1 \neq 1$ would have worked. The point is, that "most" of the changes of variables give us the result we want.

Proof. Consider the ring homomorphism from the polynomial ring in n variables to A:

$$\mathrm{ev}_{\mathbf{a}} : \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}[a_1, \ldots, a_n] = A,$$

and define $I := \mathrm{Ker}(\mathrm{ev}_{\mathbf{a}})$. If $I = 0$, then $m = n$ and $y_i = a_i$ and we are done. For the nontrivial case, let $0 \neq f \in I$ and use induction on n.

$\boxed{\text{If } n = 1}$ we have $f(a_1) = 0$ and we conclude by Proposition 8.2 taking $m = 0$.

$\boxed{\text{If } n > 1}$ and the result holds for $n - 1$. By Lemma 8.21 there exist $\alpha_1, \ldots, \alpha_{n-1} \in \mathbb{K}$, such that setting $a_i' := a_i - \alpha_i a_n$ and $A' := \mathbb{K}[a_1', \ldots, a_{n-1}'] \subseteq A$, we have some $c \in \mathbb{K} \setminus \{0\}$ and the monic polynomial

$$F(x_n) := \frac{1}{c} f(a_1' + \alpha_1 x_n, \ldots, a_{n-1}' + \alpha_{n-1} x_n, x_n) \in A'[x_n]$$

As F is monic, and $F(a_n) = 0$ by construction (because $f \in \operatorname{Ker} \operatorname{ev}_{\mathbf{a}}$), we have that a_n is integral over A'. Now, by the inductive hypothesis for A' we get there exist $y_1, \ldots, y_m \in A'$ with

(a) $y_1, \ldots, y_m$ are algebraically independent over $\mathbb{K}$,

(b) A' is a finite $\mathbb{K}[y_1, \ldots, y_m]$-algebra.

So we have $\mathbb{K}[y_1, \ldots, y_m] \subseteq A' \subseteq A = A'[a_n]$ and we conclude by Proposition 2.48 (or by Proposition 8.7) we have that A is a finite $\mathbb{K}[y_1, \ldots, y_m]$-algebra. $\qquad\square$

We will see later on how this concept relates to dimension.

Chapter 9

Graded Rings and Modules

Definition 9.1. A **graded ring** is a ring R together with a family $(R_n)_{n \geq 0}$ of *subgroups* of the additive group of R, such that

$$R = \bigoplus_{i \in \mathbb{N}} R_i \quad \text{and} \quad R_i \cdot R_j \subseteq R_{i+j} \quad \forall\, i, j \in \mathbb{N}.$$

The direct sum is thus of *Abelian groups*, but, by the grading of the multiplication, A_0 is a subring of A and each A_i is an A_0-module. An important class of such objects will have $A_0 = \mathbb{K}$, thus all the graded components will be vector spaces.

The subgroups R_i are called the **graded components** of R. A **homogeneous element** of R is simply an element of one of the graded components R_i. In this case we call $i := \deg(f)$ the degree of the homogeneous element. (We will not talk about degree for nonhomogeneous elements in this setting). A **homogeneous ideal** (or **graded ideal**) is an ideal of R which can be generated by homogeneous elements. Note that homogeneous ideal contain many nonhomogeneous elements! They may also have nonhomogeneous sets of minimal generators.

So, for every element $f \in R$, there exist unique $f_i \in R_i$, with only finitely many $f_i \neq 0$, such that

$$f = \sum_{i \in \mathbb{N}} f_i.$$

The f_i are called the **homogeneous components** of f.

There is a special homogeneous ideal of R, called the **irrelevant ideal** of R:

$$R_+ := \bigoplus_{i > 0} R_i.$$

(It plays actually an important role, but it will be "irrelevant" when looking at the corresponding locus in projective geometry).

Remark 9.2. One can easily replace $\mathbb{N}$ with any semigroup with identity and still have a similar theory. In particular, gradings over $\mathbb{Z}$, and $\mathbb{Z}^n$ are interesting.

Example 9.3. The prototype of graded rings is the polynomial ring with coefficients in a field $S = \mathbb{K}[x_1, \ldots, x_n]$, with the standard grading by degree:

$$S = S_0 \oplus S_1 \oplus \ldots$$

where S_d is the $\mathbb{K}$-vector space of homogeneous polynomials of degree d. This ring also accepts "finer" gradings, the finest being the one over $\mathbb{N}^n$ (or $\mathbb{Z}^n$ with components with negative entries 0) with

$$S_{\mathbf{a}} = \mathrm{Span}_{\mathbb{K}}(\mathbf{x}^{\mathbf{a}}), \quad \forall\, \mathbf{a} \in \mathbb{N}.$$

What are in the $\mathbb{Z}^n$-graded setting the homogeneous ideals?

Remark 9.4. Let $I \subseteq R$ be a graded ideal with homogeneous generators $f_1, \ldots, f_s$. If $f \in I$ is homogeneous, then we can write

$$f = \sum g_i f_i \quad \text{with } g_i \text{ homogeneous and } \deg g_i = \deg f - \deg f_i.$$

Indeed with you can use nonhomogeneous G_i to get the linear combination, it is enough to take the components of the G_i of the right degree. The others have to cancel out anyway.

Definition 9.5. Let R be a graded ring. A **graded R-module** is an R-module M together with a family of subgroups M_i such that

$$M = \bigoplus_{i \in \mathbb{N}} M_i \quad \text{and} \quad R_j \cdot M_i \subseteq M_{j+i} \quad \forall\, i, j \in \mathbb{N}.$$

Thus, each M_i is also an A_0-module. Just as before, we have homogeneous elements, graded components, degree, etc.

Definition 9.6. For M, N are graded R-modules, a **homomorphism of graded R-modules** (or a **graded R-linear map**) (of degree zero) is an R-linear map $f : M \longrightarrow N$ such that

$$f(M_i) \longrightarrow N_i, \quad \forall\, i \in \mathbb{N}.$$

Proposition 9.7. *Let R be a graded ring. The following are equivalent:*

(a) *R is a Noetherian ring.*

(b) *R_0 is Noetherian and R is a finitely generated R_0-algebra.*

Proof. $\boxed{(a) \Rightarrow (b)}$ $R_0 = R/R_+$, hence Noetherian by 6.1.
Since R is Noetherian, then R_+ is finitely generated. Let $(f_1, \ldots, f_r) = R_+$. We may assume all the f_i are homogeneous, of degrees $d_1, \ldots, d_r$ respectively. Clearly we can choose them such that $d_i > 0$ for all i. Let $R' := R_0[f_1, \ldots, f_r]$. We prove by induction on $n \in \mathbb{N}$ that $R_n \subseteq R'$.
$n = 0$ holds trivially.
$n > 0$ and assume $R_i \subseteq R'$ for $i < n$. Let $f \in R_n$, so $f \in R_+$, thus it is a linear combination

$$f = \sum_{i=1}^{r} a_i f_i, \quad \text{with } \deg(a_i) = \deg f - \deg f_i.$$

So, by the inductive hypothesis, all the a_i are polynomial expressions in $f_1, \ldots, f_r$ with coefficients in R_0. Thus so is f.
$\boxed{(b) \Rightarrow (a)}$ Is a consequence of the Hilbert Basis Theorem 6.6. $\qquad \square$

9.1 Filtrations

Definition 9.8. Let M be and R-module. An (infinite) chain of submodules of M

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \ldots$$

is called a **filtration** of M. We will write it compactly as $(M_n)_{n \in \mathbb{N}}$. Let $I \subseteq R$ be an ideal. A filtration is called **I-filtration** if $IM_n \subseteq M_{n+1}$ for all n. A filtration is a **stable I-filtration** if there exists $n_0 \in \mathbb{N}$ such that

$$IM_n = M_{n+1} \quad \forall\, n \geq n_0.$$

Example 9.9. $(I^n M)_{n \in \mathbb{N}}$ is a stable I-filtration.

For any (not necessary graded) ring R and any ideal $I \subseteq R$ we can form the following graded ring called the **blowup algebra of I in R**

$$R^* := \bigoplus_{n \in \mathbb{N}} I^n.$$

For any R-module M and any I-filtration $(M_n)_{n \in \mathbb{N}}$ of M, then

$$M^* = \bigoplus_{n \in \mathbb{N}} M_n$$

is a graded R^*-module, since $I^m M_n \subseteq M_{m+n}$. If R is Noetherian and $I = (a_1, \ldots, a_r)$, then $R^* = R[a_1, \ldots, a_r]$ and is thus also Noetherian (as a consequence of the Hilbert Basis Theorem).

Lemma 9.10. *Let R be a Noetherian ring with an ideal $I \subseteq R$, and let M be a finitely generated R-module with an I-filtration $(M_n)_{n \in \mathbb{N}}$. The following are equivalent:*

(a) *M^* is a finitely generated R^*-module.*

(b) *The filtration $(M_n)_{n \in \mathbb{N}}$ is stable.*

Proof. Each M_n is finitely generated (as a submodule of the Notherian module M). So is then

$$Q_n = \bigoplus_{i=0}^{r} M_i.$$

This is a subgroup of M^*, but not necessarily an R^*-submodule. We have

$$M_n^* := \operatorname{Span}_{R^*} Q_n = M_0 \oplus \cdots \oplus M_n \oplus I M_n \oplus I^2 M_n \oplus \cdots \oplus a^r M_n \oplus \ldots$$

Since Q_n is a f.g. R-module, M_n^* is a f.g. R^*-module. So we get an ascending chain $\mathcal{C}^*$:

$$M_0^* \subseteq M_1^* \ldots$$

The union of this chain is M^*, so if it becomes stationary, it becomes stationary at M^*.
Since R^* is Noetherian we have the following equivalences

$$
\begin{aligned}
M^* \text{ is a f.g. } R^*\text{-module} \quad &\Leftrightarrow \quad \mathcal{C}^* \text{ is stationary} \\
&\Leftrightarrow \quad \exists n_0 \in \mathbb{N} \ \text{ such that } M^* = M_{n_0}^* \\
&\Leftrightarrow \quad \exists n_0 \in \mathbb{N} \ \text{ such that } M_{n_0+r} = I^r M_{n_0} \ \ \forall \, r \geq 0 \\
&\Leftrightarrow \quad \text{the filtration is stable.}
\end{aligned}
$$

$\square$

Lemma 9.11 (Artin-Rees)**.** *Let R be a Noetherain ring, $I \subseteq R$ and ideal, M a finitely generated R-module, and $(M_n)_{n \in \mathbb{N}}$ a stable I-filtration of M. If $M' \subseteq M$ is a submodule of M, then $(M' \cap M_n)$ is a stable I-filtration of M'.*

Proof. We have $I(M' \cap M_n) \subseteq I M' \cap I M_n \subseteq M' \cap M_{n+1}$, so we have an I-filtration of M'. So we have $(M')^*$ is an R^*-submodule of M^*. Since R^* is Noetherian and the filtration is stable, by Lemma 9.10 M^* is finitely generated, thus Noetherian, thus $(M')^*$ is also finitely generated, and we apply Lemma 9.10 again to conclude. $\square$

9.2 The Associated Graded Ring

Let R be a ring and $I \subseteq R$ an ideal. We set

$$\mathfrak{gr}_I R := R/I \oplus I/I^2 \oplus \dots$$

The multiplication in $\mathfrak{gr}_I R$ is given as follows:

$$[a] \in I^m/I^{m+1}, [b] \in I^n/I^{n+1} \text{ define } [a] \cdot [b] := [ab] \in I^{m+n}/I^{m+n+1}.$$

More generally, for an R-module M we can do the same for an I-filtration $\mathcal{I} := (M_n)_{n\in\mathbb{N}}$ and define

$$\mathfrak{gr}_\mathcal{I} M := \bigoplus_{n\in\mathbb{N}} M_n/M_{n+1}.$$

This is a graded $\mathfrak{gr}_I R$-module in a natural way:

$$[a][y] = [ay] \in M_{m+n}/M_{m+n+1}, \quad \forall\, [a] \in I^m/I^{m+1}, [y] \in M_n/M_{n+1}.$$

This works because we have an I-filtrarion.

Proposition 9.12. *Let R be a Noetherian ring and I and ideal of R. We have*

(a) $\mathfrak{gr}_I R$ *is Noetherian.*

(b) *If M is a finitely generated R-module, and $\mathcal{I} = (M_n)$ is a stable I-filtration of M, then $\mathfrak{gr}_\mathcal{I} M$ is a finitely generated $\mathfrak{gr}_I R$-module.*

Proof. (a) Since R is Noetherian, then I is finitely generated $I = (a_1, \dots, a_r)$. Denote by $\bar{a}_i$ the equivalence classes of the a_i in I/I_2. Then we have

$$\mathfrak{gr}_I R = (R/I)[\bar{a}_1, \dots, \bar{a}_r].$$

Since R/I is Noetherian (by Proposition 5.9) we conclude by Corollary 6.8 of the Hilbert Basis Theorem.

(b) Let $n_0 \in \mathbb{N}$ be such that $M_{n_0+k} = I^k M_{n_0}$ for all $k \geq 0$, hence $\mathfrak{gr}_\mathcal{I} M$ is generated by $\bigoplus_{n\leq n_0} M_n/M_{n+1}$. Each M_n/M_{n+1} is Noetherian and annihilated by I, hence a finitely generated R/I-module. So the whole sum $\bigoplus_{n\leq n_0} M_n/M_{n+1}$ is finitely generated as an R/I module, so the whole $\mathfrak{gr}_\mathcal{I} M$ is a finitely generated $\mathfrak{gr}_I R$-module.

$\square$

In the particular case in which $I = \mathfrak{m}$ is maximal, we obtain that the associated graded ring is an algebra over a field (finitely generated if I is).

9.3 Krull Intersection Theorem

We get the next result actually as a corollary of the Artin-Rees Lemma.

Theorem 9.13 (Krull Intersection Theorem). *Let $I \subseteq R$ be an ideal in a Noetherian ring R. If M is a finitely generated R-module, then there exists an element $r \in I$ such that*

$$(1 - r)\big(\bigcap_{j\geq 1} I^j M\big) = 0.$$

In particular, if R is a domain or a local ring, and if I is aproper ideal, then

$$\bigcap_{j\geq 1} I^j = 0.$$

Proof. By the Artin-Rees Lemma applied to the submodule $M' = \bigcap_{j \geq 1} I^j M \subseteq M$, and the I-adic filtration $(I^n M)_{n \in \mathbb{N}}$, there exists an integer n_0 such that

$$
\begin{aligned}
\bigcap_{j \geq 1} I^j M &= \left(\bigcap_{j \geq 1} I^j M \right) \cap I^{n_0+1} M \\
&= I \left(\left(\bigcap_{j \geq 1} I^j M \right) \cap I^{n_0+1} \right) \\
&= I \left(\bigcap_{j \geq 1} I^j M \right)
\end{aligned}
$$

So the first statement follows by Corollary 2.25 (b) of the Cayley-Hamilton Theorem.

For the second part, take $M = R$, and it will be enough to show that $1 - r$ is a nonzerodivisor. Since I is proper, we have $1 - r \neq 0$, so we are done if it is a domain. If $(R, \mathfrak{m})$ is local, then, $I \subseteq \mathfrak{m}$, so $r \in \mathfrak{m}$, and thus $1 - r$ is a unit. $\qquad \square$

Corollary 9.14. *Let R be a Noetherian local ring, and let I be a proper ideal of R. If $\mathfrak{gr}_I R$ is a domain, then R is a domain.*

Proof. Hard exercise. (Check [Eis95, Corollary 5.5]). $\qquad \square$

The whole point of these constructions is that graded rings are "easier" to study, because they have more structure. The theory of Hilbert functions is one such example.

9.4 Hilbert Functions

Let $R = \bigoplus_{i \in \mathbb{N}} R_i$ be a Noetherian graded ring. We have thus that R_0 is also Noetherian, and $R = R_0[a_1, \ldots, a_s]$, with a_i homogeneous of degrees $d_i > 0$.

Let $M = \bigoplus_{i \in \mathbb{N}} M_i$ be a finitely generated graded R-module. Then we can generate M also by a finite number of *homogeneous* elements: $m_1, \ldots, m_t$, with $\deg m_j = r_j$.

We will introduce Hilbert functions of graded modules over the polynomial ring (thus in particular for graded quotients over the polynomial ring). In [AM69] there is a more general treatment, but I find this introduction friendlier. So let from now on $\mathbb{K}$ be a fixed field, $n \in \mathbb{N}_{>0}$ and S be the polynomial ring:

$$
S := \mathbb{K}[x_1, \ldots, x_n].
$$

Definition 9.15. Let $M = \bigoplus_{i \in \mathbb{N}}$ be a finitely generated graded S-module. The numerical function $\mathrm{HF}_M : \mathbb{N} \longrightarrow \mathbb{N}$ given by

$$
\mathrm{HF}_M(i) := \dim_{\mathbb{K}} M_i
$$

is called the **Hilbert function of M**.

Note that all these dimensions are finite: if M_s were not finitely generated over $\mathbb{K}$ as we would get $\bigoplus_{i \geq s} M_i$ would not be a finitely generated S-module of M, and thus M would not be Noetherian - a contradiction.

Hilbert's insight was that this infinite series of information can be encoded in a finite way:

Theorem 9.16 (Hilbert)**.** *If M is a finitely generated graded S module, then there exists a polynomial $\mathrm{HP}_M(t) \in \mathbb{Z}[t]$, with $\deg HP_M \leq n - 1$, and a natural number $i_0 \in \mathbb{N}$, such that*

$$
\mathrm{HF}_M(i) = \mathrm{HP}_M(i), \quad \forall \, i \geq i_0.
$$

Definition 9.17. The polynomial HP_M from Theorem 9.16 is called the **Hilbert polynomial of** M.

Definition 9.18. For a graded R-module $M = \bigoplus_{i\in\mathbb{N}} M_i$ and a $d \in \mathbb{Z}$ we define the **d-th twist of** M as the R-module $M(d)$, which is isomorphic to M as R-modules, but has a different grading, with graded components shifted by d:

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

The reason for doing this is mainly to keep track of graded components. One can formally imagine that we are now working in a new category, in which the objects come with a grading, and the only maps allowed now are homogeneous and map degree component to same degree component. For instance, multiplication by a linear form would not be a homogenous homomorphism of degree 0, unless we shift the grading of M by -1.

Definition 9.19. A numerical function $F : \mathbb{Z} \longrightarrow \mathbb{Z}$ is called of **polynomial type** (of degree d) it there exists a polynomial $P \in \mathbb{Q}[t]$ (of degree d) such that $F(i) = P(i)$ for all $n \gg 0$. (Convention: the degree of the zero polynomial is -1)

The **difference operator** Δ on the set of numerical functions is given by

$$(\Delta F(i) = F(i+1) - F(i), \quad \forall\, i \in \mathbb{Z}$$

The d-times differential operator is defined recursively, and denoted by as $\Delta^d F$. (with the convention that $\Delta^0 F = F$).

Lemma 9.20. *Let $H : \mathbb{N} \longrightarrow \mathbb{Z}$ be a numerical function and $d \in \mathbb{N}$. The following are equivalent:*

(a) $\Delta^d F(i) = c, c \neq 0$, *for all $i \gg 0$.*

(b) F *is of polynomial type of degree d.*

Proof. $\boxed{(a) \Rightarrow (b)}$ We use induction on d. If $d = 0$, it is trivial. Assume $d > 0$. We have

$$\Delta^d F(i) = \Delta^{d-1}(F(i+1) - F(i)) = c, c \neq 0, \quad \forall i \gg 0,$$

so by induction there exists a polynomial $p \in \mathbb{Q}[t]$, of degree $d - 1$, and an $i_0 \in \mathbb{N}$ such that

$$F(i+1) - F(i) = P(i), \quad \forall\, i \geq i_0.$$

But then

$$F(i+1) = F(i_0) + \sum_{k=i_0}^{i} P(k),$$

and the last sum is a polynomial function of degree d.

$\boxed{(b) \Rightarrow (a)}$ - clear. $\qquad\square$

Of Theorem 9.16. We will use induction on n, the number of variables in S.

If $n = 0$, then we just have a finite dimensional $\mathbb{K}$-vectors space. So $\mathrm{HP}_M(t) = 0$.

Let J be the kernel of multiplication by x_n. So we get an exact sequence of graded vectors spaces with maps of degree zero:

$$0 \longrightarrow J(-1) \longrightarrow M(-1) \xrightarrow{\cdot x_n} M \longrightarrow M/x_n M \longrightarrow 0.$$

Taking the component of degree i in each term, and using 2.41 for the additive function $\dim_{\mathbb{K}}$ we have

$$\mathrm{HF}_M(i) - \mathrm{HF}_M(i-1) = \mathrm{HF}_{M/x_n M}(i) - \mathrm{HF}_J(i-1).$$

Now both J and $M/x_n M$ are finitely generated $\mathbb{K}[x_1, \ldots, x_{n-1}]$-modules. By induction, the terms on the right-hand side are thus of polynomial type of degree at most $n - 2$. We conclude by Lemma 9.20. $\qquad\square$

The trick is, that we may replace $\dim_{\mathbb{K}}$ with other additive functions, so that we may generalize Hilbert functions to more abstract settings, where a field is not at hand. Let λ be an additive function on the category of finitely generated R_0-modules (cf. Definition 2.40). The **Poincaré series** with respect to λ of a finitely generated graded R-modle M is the generating function of $n \longmapsto \lambda(M_n)$, that is

$$\mathrm{HS}_\lambda(M,t) := \sum_{n \in \mathbb{N}} \lambda(M_n) t^n \in \mathbb{Z}[[t]].$$

Theorem 9.21 (Hilbert-Serre). *Let $R = \bigoplus_{i \in \mathbb{N}} R_i$ be a Noetherian graded ring, generated as an R_0-algebra by the s elements of degrees $d_1, \ldots, d_s \in \mathbb{N}_{>0}$, and let $M = \bigoplus_{i \in \mathbb{N}} M_i$ be a finitely generated graded R-module. Then the Poincaré series of M is a rational function in t. To be more precise: there exists a polynomial $h(t) \in \mathbb{Z}[t]$ such that*

$$\mathrm{HS}_\lambda(M,t) = \frac{f(t)}{\prod_{i=1}^{s}(1 - t^{d_i})}.$$

Proof. We prove this by induction on s, the number of generators of R as an R_0-algebra.

$\boxed{s = 0}$ This means $R = R_0$, so M is a finitely generated R_0-module, so $M_n = 0$ for $n \gg 0$. Thus $\mathrm{HS}_\lambda(M,t)$ is already a polynomial.

$\boxed{s > 0}$ Assume the statement is true for $s - 1$. For every $n \in \mathbb{N}$, multiplication by x_s

$$\cdot x_s : M_n \longrightarrow M_{n+d_s}$$

is R_0-linear. So, by taking kernel and cokernel we obtain an exact sequence

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{\cdot x_s} M_{n+d_s} \longrightarrow L_{n+d_s} \longrightarrow 0. \tag{9.1}$$

Now take the graded modules $\bigoplus_{n \in \mathbb{N}} K_n$ and $\bigoplus_{n \in \mathbb{N}} L_n$. They are both finitely generated R-modules, because they are a submodule, respectively a quotient module of M. We also have by definition $x_s \in \mathrm{Ann}_R K$ and $x_s \in \mathrm{Ann}_R L$. So we can view both as modules over $R' = R_0[x_1, \ldots, x_{s-1}]$. Applying the additive function λ to (9.1) we get

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+d_s}) - \lambda(L_{n+d_s}) = 0$$

Multiplying now with t^{n+d_s} and summing up with respect to n we get

$$-t^{d_s} \Big(\sum_{n=0}^{\infty} \lambda(M_n) \Big) + \sum_{n=0}^{\infty} \lambda(M_{n+d_s}) t^{n+d_s} = \sum_{n=0}^{\infty} \lambda(L_n + d_s) t^{n+d_s} - \sum_{n=0}^{\infty} \lambda(K_n) t^{n+d_s}.$$

Adjusting for the right parameters, and adding and subtracting the first d_s summands of the Poincaré series where necessary, we get

$$(1 - t^{d_s}) \mathrm{HS}_\lambda(M,t) = \mathrm{HS}_\lambda(L,t) - t^{d_s} \mathrm{HS}_\lambda(H,t) + g(t)$$

and we conclude by induction. $\qquad\square$

Chapter 10

Dimension Theory

We will only briefly mention a few things here. Let us start with what we expect from a dimension function. As opposed to other mathematical invariants, dimension is deeply rooted in our intuition of the "real" world. So it is appropriate to start with a list of requirements, which we will call here *Axioms of Dimension*. We refer the reader to [**?**, Chapter 8] for a much better overview.

(D 1) Dimension is a local property.

(D 2) Dimension is immune to nilpotent elements.

(D 3) Dimension is preserved by maps with finite fibers.

(D 4) The dimension around a point in n-space is n.

Let us now be a bit more precise, and translate this wish-list into (slightly) more precise statements.

1 *Dimension is a local property.* Think of a union of some planes and some lines and a few points not contained in either. View this object as one object. Clearly, dimension is not the same everywhere on it, but, as it contains planes, it should say it is 2-dimensional. The point of this first axiom is, that dimension is not everywhere the same. It should be defined locally, and the global dimension should be the supremum of the local ones. In other words,

$$\dim R = \sup_{\mathfrak{p} \in \operatorname{Spec} R} \dim R_{\mathfrak{p}}$$

and as completion is even more local than localization, we should also have

$$\dim R = \dim \widehat{R}.$$

2 *Dimension is immune to nilpotent elements.* The point here is that nilpotents in geometry may be though of as elements which describe some infinitesimal behaviour. (Infinitesimals are these tiny "numbers". So tiny, that if you multiply them with themselves a few times there is nothing left). So nilpotents, while they do have a meaning, they should not contribute to dimension. More precisely:

$$\text{If } I \text{ is nilpotent, then } \dim R = \dim R/I.$$

3 *Dimension is preserved by maps with finite fibers.* In a general geometric context, the fibers of a geometric map are also geometric objects. If the map is well-behaved, then the dimension of the source should be the dimension of the image + the dimension of the fibre. As points should be zero-dimensional, if the

fibre is finite (thus a finite union of points), then the dimensions of image and source should be equal. In algebraic terms, we phrase this as follows:

If $\varphi : R \hookrightarrow S$ turns S into an integral R-module, then $\dim R = \dim S$.

This requirement brings in the connection between Noether normalization and dimension.

4 *The dimension around a point in n-space is n.* This is pretty straight forward. It just means

$$\dim \mathbb{K}[x_1, \ldots, x_n] = \dim \mathbb{K}[[x_1, \ldots, x_n]] = n.$$

With a guideline in place, we can say now what the "right" definition of dimension for commutative rings is: Krull dimension (cf. Section 6.3):

$$\dim_{Krull} R := \sup\{k \in \mathbb{N} \mid \text{there exists prime ideals } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k\} \in \mathbb{N} \cup \{\infty\}.$$

Theorem 10.1 (Dimension Theorem)**.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring. The following three integers are equal*

(a) *The maximum length of a chain of prime ideals in R.*

(b) *The degree of the Hilbert Polynomial of $\mathfrak{gr}_{\mathfrak{m}} R$.*

(c) *The least number of generators of an $\mathfrak{m}$-primary ideal of R.*

The above integer is the dimension of the Noetherian local ring. One useful application of dimension is the algebraic definition of smoothness. To this aim we have the following.

Theorem 10.2. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, with $\mathbb{K} = R/\mathfrak{m}$. Assume that the Krull dimension of R is d. Then the following are equivalent:*

(a) $\mathfrak{gr}_{\mathfrak{m}} R \simeq \mathbb{K}[t_1, \ldots, t_n].$

(b) $\dim_{\mathbb{K}} \mathfrak{m}/\mathfrak{m}^2 = d.$

(c) $\mathfrak{m}$ *can be generated by d elements.*

Chapter 11

Completions

A **topological Abelian group** is a topological space with a compatible commutative group structure, i.e. the maps

$$G \times G \longrightarrow G \quad (x, y) \mapsto x + y$$
$$G \longrightarrow G \quad x \mapsto -x$$

are continuous.

In general, such a group is not necessarily Hausdorff. As we have that Hausdorff is equivalent to $\{(x, x) \; : \; x \in G\}$ being closed in $G \times G$, we get that a topological Abelian group is Hausdorff if $\{0\}$ is closed in G. (This makes its preimage closed in $G \times G$ under $(x, y) \mapsto x - y$.

For a fixed element $g \in G$, the translation $T_g : G \longrightarrow G$ with $T_g(x) := x + g$, is a homeomorphism with inverse T_{-g}. Hence if U is a neighborhood of 0 in G, then $U + g$ is a neighborhood of g in G, and every neighborhood of g appears this way. So the topology of G is uniquely determined by the neighborhoods of 0.

Lemma 11.1. *Let H be the intersection of all neighborhoods of 0 in G. Then:*

(a) *H is a subgroup of G.*

(b) *H is the closure of $\{0\}$.*

(c) *G/H is Hausdorff.*

(d) *G is Hausdorff if and only if $H = 0$.*

Proof. (a) First, note that $0 \in H$.
Second, as $x \mapsto -x$ is continuous and self-inverse, we get that

$$U \text{ is a neighborhood of } 0 \Leftrightarrow -U \text{ is a neighborhood of } 0$$

So if x is in all, then $-x$ is in all.
Third, let $x, y \in H$, and let U be an arbitrary neighborhood of 0. Since $(x, y) \mapsto x + y$ is continuous, there exists a neighborhood $U_1 \times U_2$ in $G \times G$ of $(0, 0)$ such that $+(U_1 \times U_2) \subseteq U$. In the product topology, $U_1 \times U_2$ is a neighborhood (of (0,0)), if and only if U_1, U_2 are neighborhoods (of 0). So, as $x, y \in H$, we have $x, y \in U_1, U_2$, so $(x, y) \in U_1 \times U_2$ maps to $x + y \in U$.

(b) We have $x \in \overline{\{0\}} \Leftrightarrow \{0\} \cap V \neq \emptyset, \; \forall \text{ neighborhood } V \ni x. \Leftrightarrow 0 \in x - U, \; \forall \text{ neighborhood } U \ni 0 \Leftrightarrow x \in H.$

(c) We still have a topological Abelian group G/H, so, as all points (i.e. all cosets) are closed we have a Hausdorff space. (Notice that for arbitrary topological spaces, closed points just implies T_1, but not T_2. E.g. $\mathbb{N}$ with the cofinite topology.)

(d) $\Leftarrow$ follows from the previous point. $\Rightarrow$ Hausdorff implies T_1 which is equivalent to all points are closed, so $\{0\} = \overline{\{0\}} = H$.

$\square$

Definition 11.2. A **Cauchy sequence** in a topological group G is a sequence $(x_n)_{n \in \mathbb{N}}$ of elements of G, such that for every neighborhood U of 0, there exists an integer n_U such that

$$x_i - x_j \in U \ \forall \ i, j \geq n_U.$$

Two Cauchy sequences are said to be *equivalent* if their difference converges to zero, that is

$$(x_n) \sim (y_n) \Leftrightarrow \forall 0 \in \ U \text{ neighborhood } \exists n_U \text{ such that } x_n - y_n \in U.$$

The **completion** of G is

$$\widehat{G} := \{\text{Cauchy sequences in } G\}/ \sim .$$

Remark 11.3.   1. If $(x_n), (y_n)$ are Cauchy sequences, then $(x_n + y_n)$ is also a Cauchy sequence, and if $(x_n) \sim (x'_n)$ and $(y_n) \sim (y'_n)$, then $(x_n + y_n) \sim (x'_n + y'_n)$. It is an easy check that $\widehat{G}$ obtains an Abelian group structure this way.

2. For each $x \in G$, the constant sequence $(x)_{n \in \mathbb{N}}$ is a Cauchy sequence. This defines a group homomorphism

$$\Phi : G \longrightarrow \widehat{G}$$

$$x \longrightarrow (x)_{n \in \mathbb{N}}$$

Two elements are mapped to the same equivalence class, if $x - y \in U$ for all neighborhoods of U. So

$$\ker \Phi = H = \overline{\{0\}}.$$

Thus, by Lemma 11.1, Φ is injective if and only if G is Hausdorff.

3. If G_1, G_2 are topological Abelian groups, and $f : G_1 \longrightarrow G_2$ is a continuous group homomorphism, then it maps Cauchy sequences to Cauchy sequences and induces this way a continuous group homomorphism

$$\widehat{f} : \widehat{G}_1 \longrightarrow \widehat{G}_2.$$

Clearly, if we have three groups and $G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3$, then $\widehat{f_2 \circ f_1} = \widehat{f}_2 \circ \widehat{f}_1$.

Example 11.4. The prototype of this construction is the completion of the rational numbers: $\widehat{\mathbb{Q}} = \mathbb{R}$. Another important example are the p-adic integers: the group is $\mathbb{Z}$ and a fundamental set of neighborhoods of 0 is given by the ideals (p^n). So two numbers are "close" (i.e. their difference is in a smaller neighborhood of 0) if their difference is divisible by a high power of p. Let us stretch an analogy and take $p = 10$ (even if it is not prime). When completing $\mathbb{Q}$, we add successive approximations, that is infinitely many decimal positions:

$$0.1, 0.12, 0.123, \ldots$$

That is, $0.12 - 0.1 = 0.02 = 2 \cdot 10^{-2}$, and $0.123 - 0.12 = 0.003 = 3 \cdot 10^{-3}$, so the last two are closer to each other than the first two. For the 10-adic topology, we have

$$10, 210, 3210, \ldots$$

and again, $210 - 10 = 200 = 2 \cdot 10^2$ and $3210 - 210 = 3000 = 3 \cdot 10^3$, so 3210 is closer to 210 than 210 is to 10. This way, while the regular completion corresponds to adding infinitely many decimals to the right, the p-adic completion corresponds to adding infinitely many "figures" (symbols representing 0 to $p - 1$) to the left.

From now on we will concentrate more on completions arising from these special topologies, which mimic the p-adic topology over $\mathbb{Z}$. So assume that the topology on our group G is has a fundamental system of neighborhoods of 0 consisting of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots$$

So U is a neighborhood of 0 if $\exists\, n \in \mathbb{N}$ such that $U \supseteq G_n$.

Remark 11.5. In a topology as above, the sets G_n are both open and closed.

Proof. $\boxed{\text{Open.}}$ If $x \in G_n$, then $x + G_n$ is a neighborhood of x, and since G_n is a subgroup $x + G_n \subseteq G_n$.
$\boxed{\text{Closed.}}$ For any $x \in G$, the set $x + G$ is open, so $G \setminus G_n = \bigcup_{x \notin G}(x + G_n)$ is also open. $\qquad\square$

For such topologies, there is a way to define the completion which is purely abstract and algebraic, and does not mention Cauchy sequences or the topology. I find it important though to keep in mind what the original idea was. This is why we had the above discussion. We give the following definition in our special setting. This could be extended to more general abstract setups.

Definition 11.6. Let $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots$ be subgroups of an Abelian group G. The **inverse limit** of the factor groups G/G_i is

$$\varprojlim G/G_i := \big\{ g = (g_1, g_2, \dots) \in \textstyle\prod_{i \in \mathbb{N}} G/G_i \mid g_j \equiv g_i \bmod G_i,\ \forall j > i \geq 0. \big\}$$

In general, one needs an inverse system (see the Appendix), similar to the one we needed for directed systems on Exercise Sheet 5. The point is, that in such a system we also have a family of maps, for $j > i$, which in our case are the canonical projections

$$\pi_{ji} : G/G_j \longrightarrow G/G_i$$

Remark 11.7. For a topological group, with filtration-induced topology as above we have

$$\widehat{G} = \varprojlim G/G_i.$$

Indeed, for every Cauchy sequence $(x_k)_{k \in \mathbb{N}}$ we have that $\lim_k \pi_{ki}(x_k) =: \xi_i \in G/G_i$ is ultimately constant for every k. We clearly have $\pi_{ji}\xi_j = \xi_i$, so the Cauchy sequence defines an element in the inverse limit. Furthermore, equivalent Cauchy series clearly define the same element, thus we have a well defined map from $\widehat{G}$ to $\varprojlim G/G_i$. Conversely, for every element (g_i) in the inverse limit we can construct a Cauchy series by choosing $x_i \in g_i + G_i$, and keeping track that $x_{i+1} - x_i \in \mathbb{G}_i$.

The disadvantage of the inverse limit definition, is that we may have different inverse systems giving rise to the same topology, but a priori to different inverse limits. So one needs to introduce an equivalence of inverse limits. We will not do that here. A big advantage of inverse limits is exactness. Notice that the maps π_{ji} are all surjective if we start with a filtration by subgroups as we did[1].

Let $\{A_i\}_{i \in \mathbb{N}}$, $\{B_i\}_{i \in \mathbb{N}}$, and $\{C_i\}_{i \in \mathbb{N}}$ be three inverse systems with the property that for every $i \in \mathbb{N}$ we have

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A_{i+1} & \longrightarrow & B_{i+1} & \longrightarrow & C_{i+1} & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_i & \longrightarrow & B_i & \longrightarrow & C_i & \longrightarrow & 0
\end{array}
$$

all such diagrams commute. In this case we say that we have an **exact sequence of inverse systems**. Then we have automatically a (not necessarily exact) sequence

$$0 \longrightarrow \varprojlim A_i \longrightarrow \varprojlim B_i \longrightarrow \varprojlim C_i \longrightarrow 0$$

---

[1] such inverse systems are called surjective in a more abstract setting.

Proposition 11.8. *For every exact sequence of inverse systems as above we have the exact sequence:*

$$0 \longrightarrow \varprojlim A_i \longrightarrow \varprojlim B_i \longrightarrow \varprojlim C_i.$$

Moreover, if the inverse system $\{A_i\}_{i\in\mathbb{N}}$ is surjective, then even

$$0 \longrightarrow \varprojlim A_i \longrightarrow \varprojlim B_i \longrightarrow \varprojlim C_i \longrightarrow 0$$

is exact.

Proof. This is a consequence of the Snake Lemma 2.39. First, define $A = \prod_{i\in\mathcal{I}} A_i$ and similarly B and C. Then define $d^A : A \longrightarrow A$ by setting

$$d^A(a_n) := (a_n - \pi_{n+1,n}(a_{n+1})),$$

and similarly d^B and d^C. Notice that $\ker d^A = \varprojlim A_i$, and similarly for d^B and d^C. So we get the diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle d^A} & & \downarrow{\scriptstyle d^B} & & \downarrow{\scriptstyle d^C} & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0
\end{array}
$$

Now we apply the Snake Lemma 2.39, and use that the kernels are the respective projective limits, to get

$$0 \longrightarrow \varprojlim A_i \longrightarrow \varprojlim B_i \longrightarrow \varprojlim C_i \longrightarrow \operatorname{Coker} d^A \longrightarrow \operatorname{Coker} d^B \longrightarrow \operatorname{Coker} d^C \longrightarrow 0$$

Now, whenever $(A_i)_{i\in\mathbb{N}}$ is surjective, we also have d^A surjective, and we conclude. $\qquad\square$

Corollary 11.9. *Let $0 \to G' \to G \xrightarrow{p} G'' \to 0$ be an exact sequence of groups. Let G have the topology induced by a filtration of subgroups $(G_i)_{i\in\mathbb{N}}$, and give G' and G'' the induced topologies by the filtrations $(G' \cap G_i)_{i\in\mathbb{N}}$, respectively $(p(G_i))_{i\in\mathbb{N}}$. Then the following sequence is exact:*

$$0 \to \widehat{G'} \to \widehat{G} \to \widehat{G''} \to 0.$$

Proof. Apply Proposition 11.8 to the family of short exact sequences:

$$0 \longrightarrow \frac{G'}{G' \cap G_i} \longrightarrow \frac{G}{G_i} \longrightarrow \frac{G''}{p(G_i)} \longrightarrow 0.$$

$\qquad\square$

Corollary 11.10. *In the hypothesis of Corollary 11.9, taking $G'' = G_n$ we obtain that*

(a) $\widehat{G_n}$ *is a subgroup of $\widehat{G}$.*

(b) $\widehat{G}/\widehat{G_n} \simeq G/G_n$.

(c) $\widehat{\widehat{G}} = \widehat{G}$.

Proof. Take in Corollary 11.9 $G' = G_n$ and $G'' = G/G_n$, we obtain (a). The filtration thus becomes constant and equal to (0) from n on, thus G'' has the discrete topology. In the discrete topology, the Cauchy sequences are the (eventually) constant sequences, so $\widehat{G''} = G''$. For (c) just take inverse limits in (b):

$$\varprojlim \frac{\widehat{G}}{\widehat{G_n}} = \varprojlim \frac{G}{G_n}.$$

$\qquad\square$

We will apply the above theory mainly in two settings

1. $G = R$ is a ring and $(G_n)_{n \in \mathbb{N}} = (I^n)_{n \in \mathbb{N}}$, where I is an ideal.

2. $G = M$ is an R-module, and $(G_n)_{n \in \mathbb{N}} = (I^n M)_{n \in \mathbb{N}}$, where I is an ideal of R.

In both settings, we will call the induced topology *I*-**adic topology**, and in both settings the extra structure is compatible with this topology. That is, multiplication (in R and with scalars from R, respectively) is continuous. The I-adic completion of R, and the I-adic completion of M are denoted by $\widehat{R}$ (or $\widehat{R_I}$) and $\widehat{M}$ (or $\widehat{M_I}$) respectively, and is also a topological ring, respectively $\widehat{R}$-module. A ring or module is **complete** if it is equal to its completion.

If M, N are topological R-modules with respect to the I-adic topology, and if $f : M \longrightarrow N$ is R-linear, then f is continuous. Indeed we have

$$f(I^n M) = I^n(f(M)) \subseteq I^n N$$

so, the fundamental set of neighborhoods is compatible. This means, that every f induces and $\widehat{R}$-linear map $\widehat{f} : \widehat{M} \longrightarrow \widehat{N}$.

Examples. 1. The most important example is the completion of the polynomial ring $S = \mathbb{K}[x_1, \ldots, x_n]$ with respect to the irrelevant maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n)$. In this case, we have

$$\widehat{S_\mathfrak{m}} = \mathbb{K}[[x_1, \ldots, x_n]].$$

2. More generally, if $R = \mathbb{K}[x_1, \ldots, x_n]/I$, then the completion with respect to $\mathfrak{m} = (x_1, \ldots, x_n)$ is

$$\widehat{R_\mathfrak{m}} = \frac{\mathbb{K}[[x_1, \ldots, x_n]]}{I\mathbb{K}[[x_1, \ldots, x_n]]}.$$

The usefulness of (and motivation for) completions consists in their ability to mimic analytic methods in algebraic geometry. While localizations correspond to taking a look in all Zariski open sets around a point, this topology is too coarse. Taking a completion allows one to take a look in the (much smaller) "classical" neighborhoods around a point. The punch line is: localization allows us to invert polynomials with respect to multiplication, completion allows us to extract radicals as well: for instance, $\sqrt{x+1}$ is not algebraic, (i.e. it cannot be expressed as a polynomial, but it is analytic, that is you may use its development as a formal power series:

$$\sqrt{1+x} = 1 + \frac{x}{2} - \frac{x^2}{8} + \sum_{n \geq 3} (-1)^{n-1} \frac{1 \cdot 3 \cdots (2n-3)}{n! 2^n} x^n$$

You are strongly encouraged to read about completions in Eisenbud's book [Eis95, Chapter 7]. We recall from there just the Cohen structure theorem, without proof.

Theorem 11.11 (Cohen Structure Theorem). *Let R be a complete local Noetherian ring with maximal ideal $\mathfrak{m}$ and residue class field $\mathbb{K}$. If R contains a field, then*

$$R \simeq \mathbb{K}[[x_1, \ldots, x_n]]/I$$

for some $n \in \mathbb{N}$ and some ideal I.

The point of introducing I-stable filtrations in Section 9.1 was that any two such filtrations define the same I-adica topology on M. Furthermore, as a corollary of the Artin-Rees lemma one gets that:

Corollary 11.12. *Let $M' \subseteq M$ be two R-modules, and I an ideal of R. The I-adic topology on M' coincides with the one induced by the I-adic topology on M.*

Corollary 11.13. *Let R be a Noetherian ring, $I \subseteq R$ be an ideal and $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be a short exact sequence of finitely generated R-modules. Then the short exact sequence of completions is exact:*

$$0 \longrightarrow \widehat{M'} \longrightarrow \widehat{M} \longrightarrow \widehat{M''} \longrightarrow 0$$

We are now interested in comparing $\widehat{R} \otimes_R M$ and $\widehat{M}$. We have the completion morphisms $\Phi_R : R \longrightarrow \widehat{R}$ and $\Phi_M : M \longrightarrow \widehat{M}$, so we can form the chain of maps $\widehat{R} \otimes_R M \longrightarrow \widehat{R} \otimes_R \widehat{M} \longrightarrow \widehat{R} \otimes_{\widehat{R}} \widehat{M} \simeq \widehat{M}$ We call this map $\Phi : \widehat{R} \otimes_R M \longrightarrow \widehat{M}$.

Proposition 11.14. *In the above notation we have:*

1. *if M is finitely generated, then Φ is surjective (for any R).*

2. *if R is Notherian and M finitely generated, then Φ is an isomorphism.*

So, when R is Notherian, the functor $M \mapsto \widehat{R} \otimes_R M$ is exact on the category of finitely generated R-modules. By 2.52 we thus have:

Corollary 11.15. *If R is a Noetherian ring and $I \subseteq R$ an ideal, then the I-completion $\widehat{R}$ is a flat R-algebra.*

(In general the functor $M \mapsto \widehat{M}$ is not exact).

Proposition 11.16. *Let R be Noetherian and $\widehat{R}$ it I-adic completion.*

(a) $\widehat{I} = \widehat{R}I \simeq \widehat{R} \otimes_R I$.

(b) $\widehat{I^n} = (\widehat{I})^n$.

(c) $\widehat{I^n}/\widehat{I^{n+1}} \simeq I^n/I^{n+1}$, *and in particular* $\mathfrak{gr}_{\widehat{I}}\widehat{R} \simeq \mathfrak{gr}_I R$.

(d) $\widehat{I}$ *is contained in the Jacobson radical of* $\widehat{A}$.

(e) *If $(R, \mathfrak{m})$ is a local ring, then the $\mathfrak{m}$-adic completion of R is a local ring with maximal ideal $\widehat{\mathfrak{m}}$.*

By Krull's Theorem, if we take $U = 1 + I$, then we have an inclusion $U^{-1}A \hookrightarrow \widehat{A}$. We state one more result without proving it.

Theorem 11.17. *If R is Noetherian, then $\widehat{R}$ is Noetherian.*

Corollary 11.18. *If $\mathbb{K}$ is a field, then $\mathbb{K}[[x_1, \ldots, x_n]]$ is Noetherian.*

Appendix A

Topology

Definition A.1. A **topology** on a set X is a collection of subsetes $\mathcal{T} \subseteq 2^X$, called **open** sets, satisfying the axioms

(T1) The subsets $\emptyset$ and X are open.

(T2) The intersection of finitely many (equivalently of any two) open sets is again open.

(T3) The union of arbitrarily many open sets is again open.

The pair $(X, \mathcal{T})$, where $\mathcal{T}$ is a topology on X is called **topological space**. The complements in X of open sets are called closed sets. By DeMorgan's rules:

$$X \setminus (\cup_i U_i) = \bigcap_i (X \setminus U_i)$$
$$X \setminus (\cap_i U_i) = \bigcup_i (X \setminus U_i)$$

we get equivalent axioms for the collection of closed sets of a topology:

($\mathrm{T}_c 1$) The subsets $\emptyset$ and X are closed.

($\mathrm{T}_c 2$) The union of finitely many (equivalently of any two) closed sets is again closed.

($\mathrm{T}_c 3$) The intersection of arbitrarily many closed sets is again closed.

A **basis of the topology** $\mathcal{T}$ on X is a collection $\mathcal{B} \subseteq \mathcal{T}$ of open sets such that for every $x \in X$ and every open set $U \in \mathcal{T}$ with $x \in U$ there exists a $B \in \mathcal{B}$ with

$$x \in B \subseteq U.$$

This can be easily show to be equivalent to each open set is an arbitrary union of basis elements. That is to

$$\forall \, U \in \mathcal{T}, \; \exists \, \mathcal{B}' \subseteq \mathcal{B}, \text{ such that } U = \bigcup_{B \in \mathcal{B}'} B.$$

Not every collection $\mathcal{B}$ of subsets can be used to define the open sets of topology by taking all unions of subcollections from $\mathcal{B}$. For instance, take $X = \{1, 2, 3\}$, $B_1 = \{1, 2\}$ and $B_2 = \{2, 3\}$. Taking all unions of sets from $\mathcal{B} = \{B_1, B_2\}$ one gets as candidates for open sets

$$\emptyset, B_1, B_2, X.$$

This collection however does not define a topology, because $B_1 \cap B_2$ is not an open set.

The general definition of basis for <u>a</u> topology (not for <u>the</u> topology $\mathcal{T}$) is the following:
A **basis for a topology** on a set X is a collection $\mathcal{B}$ of subsets of X such that

(a) For each $x \in X$, there exists $B \in \mathcal{B}$ such that $x \in B$.

(b) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \cap B_2$, then there exists $B_3 \in \mathcal{B}$ such that $x \in B_3$ and $B_3 \subseteq B_1 \cap B_2$.

Check [Mun00, Section 13] for more details.

Let $(X_1, \mathcal{T}_1), (X_2, \mathcal{T}_2)$ be two topological spaces. The **product topology** on $X_1 \times X_2$ is the topology having as basis the collection

$$\mathcal{B}_{\mathcal{T}_1 \times \mathcal{T}_2} = \{U_1 \times U_2 \; : \; \text{with } U_i \in \mathcal{T}_i\}.$$

It is very easy to check that $\mathcal{B}_{\mathcal{T}_1 \times \mathcal{T}_2}$ is a basis. It is also easy to find an example which shows that $\mathcal{B}_{\mathcal{T}_1 \times \mathcal{T}_2}$ is not a topology. The following theorem may also be useful.

Theorem A.2. *If $\mathcal{B}_1$ is a basis for $\mathcal{T}_1$ and $\mathcal{B}_2$ is a basis for $\mathcal{T}_2$, then the collection*

$$\mathcal{B}_{\mathcal{B}_1 \times \mathcal{B}_2} = \{B_1 \times B_2 \mid B_i \in \mathcal{B}_i\}$$

is a basis for the product topology on $X_1 \times X_2$.

Let $(X, \mathcal{T})$ be a topological space and $Y \subseteq X$ a subset. The collection

$$\mathcal{T}_Y := \{Y \cap U \; : \; U \in \mathcal{T}\}$$

is a topology on Y called the **subspace topology**. If $\mathcal{B}$ is a basis for $\mathcal{T}$, then $\mathcal{B}_Y := \{B \cap Y \; : \; B \in \mathcal{B}\}$ is a basis for $\mathcal{T}_Y$.

Let $A \subseteq X$ be subset of a topological space. The **interior** of A is the union of all open sets contained in A and the **closure** of A is the intersection of all closed sets containing A. So

$$\begin{aligned}
\operatorname{Int}(A) &= \bigcup_{U \subseteq A} U \quad \text{all } U \text{ are open} \\
\overline{A} &= \bigcap_{Z \supseteq A} Z \quad \text{all } Z \text{ are closed}
\end{aligned}$$

Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be topological spaces. A map $f : X \longrightarrow Y$ is **continuous** if

$$\forall \, V \in \mathcal{T}_Y \Rightarrow f^{-1}(V) \in \mathcal{T}_X.$$

If $\mathcal{B}_Y$ is a basis of the topology $\mathcal{T}_Y$ on Y, then to prove continuity, it is enough to show that

$$\forall \, V \in \mathcal{B}_Y \Rightarrow f^{-1}(V) \in \mathcal{T}_X.$$

Theorem A.3. *Let $f : X \longrightarrow Y$ be a map between topological spaces. The following are equivalent.*

(a) *f is continuous.*

(b) *For every subset A of X, one has $f(\overline{A}) \subseteq \overline{f(A)}$.*

(c) *For every closed set $B \in Y$, the set $f^{-1}(B)$ is closed in X.*

(d) *For each $x \in C$ and each neighborhood V of $f(x)$, there is a neighborhood U of x such that $f(U) \subseteq V$.*

A **homeomorphism** is a bijective map $f : X \longrightarrow Y$ between topological spaces, such that both f and its inverse f^{-1} are continuous. In other words, it is a bijective map, such that

$$U \text{ is open in } X \iff f(U) \text{ is open in } Y.$$

A topological space X is a **T_0 space**[1] if it fulfills the first of the following axioms

(T_0 separation) For any $x, y \in X$ there exists an open set U such that

$$(x \in U \text{ and } y \notin U) \quad \text{or} \quad (x \notin U \text{ and } y \in U).$$

(T_1 separation) For any $x, y \in X$ there exist open sets U and V such that

$$(x \in U \text{ and } y \notin U) \quad \text{and} \quad (x \notin V \text{ and } y \in V).$$

A topological space is **quasi-compact** if and only if each open covering of X has a finite subcovering. A subset $A \subseteq X$ is quasi-com if it is a quasi-compact space with the subspace topology. A map $f : X \longrightarrow Y$ is quasi-compact if $f^{-1}(V)$ is quasi-compact for every quasi-compact open set $V \subseteq Y$.

A topological space X is an **irreducible topological space** if $X \neq \emptyset$ and if every pair of non-empty open sets in X intersect. Equivalently, if $X \neq \emptyset$ and whenever $X = Z_1 \cup Z_2$ with Z_1, Z_2 closed, then $X = Z_1$ or $X = Z_2$. An **irreducible component** of X is a maximal irreducible subset of X.

---

[1] also called Kolmogorov space

Appendix B

Homological and Categorical Aspects

A **directed set** is a partially ordered set $\mathcal{I}$ such that for each pair $i, j \in \mathcal{I}$, there exists $k \in \mathcal{I}$ such that $i \leq k$ and $j \leq k$. Let R be a ring and $(M_i)_{i \in \mathcal{I}}$ be a family of R-modules indexed by a directed set $\mathcal{I}$. For each pair $i, j \in \mathcal{I}$ with $i \leq j$, let $\mu_{ij} : M_i \longrightarrow M_j$ be an R-linear map, such that the following axioms are satisfied:

(DSys 1) $\mu_{ii} = \mathrm{id}_{M_i}$ for all $i \in \mathcal{I}$.

(DSys 2) $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ whenever $i \leq j \leq k$.

The modules M_i together with the homomorphisms μ_{ij} are said to form a **direct system** $\mathcal{M} = (M_i, \mu_{ij})$ over the directed set I.

Let $C = \oplus_{i \in \mathcal{I}} M_i$. We identify M_i with its canonical image under the canonical injection $j_i : M_i \longrightarrow C$, and define the R-submodule of C:
$$D := \langle x_i - \mu_{ij}(x_i) \mid \forall\ x_i \in M_i,\ \ \forall\ j \geq i \rangle .$$

Denote by $M := C/D$ the quotient module, by $\mu : C \longrightarrow M$ the canonical projection, and for each $i \in \mathcal{I}$ by $\mu_i := \mu|_{M_i}$ the restriction to M_i. The homomorphisms μ_i are part of the data, and the **direct limit** of the direct system $\mathcal{M} = (M_i, \mu_{ij})$ is the pair

$$\varinjlim M_i := (M, (\mu_i)_{i \in \mathcal{I}}) .$$

An **inverse system** is a family $(M_i)_{i \in \mathcal{I}}$ (of R-modules but it may be in any category) together with homomorphisms $\pi_{ji} : M_j \longrightarrow M_i$ for any $i \leq j$ (so they go this time from the higher indexed one to the smaller indexed one – they mimic projections $G/G_j \longrightarrow G/G_i$ with $G_j \subseteq G_i$) such that

(ISys 1) $\pi_{ii} = \mathrm{id}_{M_i}$ for all $i \in \mathcal{I}$.

(ISys 2) $\pi_{ki} = \mu_{ji} \circ \mu_{kj}$ whenever $i \leq j \leq k$.

The **inverse limit** of the inverse system is a submodule of the direct product of the family:

$$\varprojlim M_i := \big\{ (m_i) \in \prod_{i \in \mathcal{I}} M_i \mid \pi_{ji}(m_j) = m_i\ \forall j \geq i \big\}.$$

So the inverse limit comes equipped with the canonical projections

$$p_j : \varprojlim M_i \longrightarrow M_j,$$

which are just the restrictions of the canonical projections from the direct product. Note that

$$\pi_{ji} \circ p_j = p_i,\ \forall\ i \leq j.$$

The inverse limit is universal among all other objects Y equipped with such maps $q_j : Y \longrightarrow M_i$. That is, for any R-module Y and family of morphisms q_j with $\pi_{ji} \circ q_j = q_i$ for all $i \leq j$, there exists a unique map $u : Y \longrightarrow \varprojlim M_i$ such that $q_j = p_j \circ u$ for all j, i.e. such that the following diagram commutes

$$
\begin{array}{ccc}
 & Y & \\
q_j \swarrow & \downarrow u & \searrow q_i \\
 & \varprojlim M_i & \\
p_j \swarrow & & \searrow p_i \\
M_j & \xrightarrow{\pi_{ji}} & M_i
\end{array}
$$

B.1 Valuation rings

Are important for studying curves. They give a criterion for separatedness of schemes [Harshorne, II.4, Theorem 4.3].

Index