MAGIC073: Commutative Algebra

Fall 2024/25
Lecturer: Nadia Mazza (Lancaster University)
contact email: n.mazza@lancaster.ac.uk

Contents

Preface

The first two sections review some fundamental concepts of commutative algebra, while the remaining sections present topics which may not have been seen in an undergraduate introductory course on commutative algebra. The content of the notes, which has been selected from the material in the references at the end, is intended to prepare the learner to explore the applications of commutative algebra to a broad range of research areas.

Within the lecture notes, there are several exercises at the end of each section. Every student is encouraged to attempt as many of these as they wish, and more from the selected bibliography. Your lecturer will recommend some exercises periodically. These are taken from the notes, and sketches of solutions will be made available on the MAGIC website by the end of the course. Student are assumed to understand the relevance of engaging with the practical aspects of a course.

The entire material covered in lectures is examinable, including the exercises. More details about examination will follow in due time.

For the computer-algebra enthusiasts, the resource [GP] may be of interest, and also the numerous possibilities offered by MAGMA: `http://magma.maths.usyd.edu.au/magma/`. No assessment component will require any knowledge of software, but some may state whether solutions obtained using computer algebra are accepted or not.

1 Commutative algebra - the essentials

1.1 Conventions

$\mathbb{N} = \{1, 2, 3, \dots\}$ is the set of natural numbers, $\mathbb{Z}$ the ring of integers, $\mathbb{Q}$ the field of rational numbers, $\mathbb{R}$ the field of real numbers and $\mathbb{C}$ the field of complex numbers. As sets:

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C},$$

where the symbol $\subsetneq$ means proper inclusion, in contrast to $\subseteq$ or $\subset$ which denote any inclusions; and similarly for the use of $\supsetneq, \supseteq, \supset$. We may also use $<$ and $>$ instead of $\subset, \supset$, respectively; mainly when the structures compared are groups, rings, ideals or modules. If $n \in \mathbb{N}$, we write $\mathbb{Z}/n$ for the quotient ring $\mathbb{Z}/n\mathbb{Z}$, whose elements are written $0, 1, \dots, n-1$, meaning $i = \{i + kn \mid k \in \mathbb{Z}\}$.

Composition of maps $f : X \to Y$ and $g : Y \to Z$ is written $g \circ f : X \to Z$ (or simply gf).

If $A \subseteq B$ are sets, we write $B \setminus A$ for the set of all the elements of B which do not lie in A.

Any additional piece of notation will be introduced when needed.

1.2 Revisions on rings

A *ring* is always meant to be a *unital ring*, that is, a ring is an abelian group $(R, +)$, whose additive identity element is 0, and R is equipped with a multiplication, denoted by juxtaposition, such that there exists a multiplicative identity $1 \in R$, that is, $1a = a = a1$ for all $a \in R$. We require the multiplication to be associative and to satisfy the distributivity rules

$$a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc, \ \forall\ a, b, c \in R.$$

If the multiplication is commutative, i.e. $ab = ba$ for all $a, b \in R$, then we call R *commutative*. Most of the rings we will study in this course are commutative rings.

If $1 = 0$, then $R = \{0\}$ is the *trivial ring*. In general, we will consider rings where $1 \neq 0$, and it is common to assume that this holds by 'default'.

A *subring* of a ring R is a subset $S \subseteq R$ such that S is an additive subgroup of R, $1 \in S$, and $ab \in S$ for all $a, b \in S$. Alternatively, we say that R is a ring *extension* of S. The extension is *trivial* if $R = S$. If both R and S are fields, then we call R a *field extension* of S, and S a *subfield* of R. For instance, $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subfield of $\mathbb{C}$, and $\mathbb{C}$ is an extension field of $\mathbb{R}$. An *ideal* of R is a subgroup I of $(R, +)$, such that $ab, ba \in I$ for any $a \in R$ and $b \in I$. These are often called *two-sided ideals* because I is multiplication-closed on both sides, which leads to the notions of one-sided ideals in non-commutative rings. In commutative rings, all ideals are necessarily two-sided, and simply called ideals. In particular, given $a \in R$, then the set $aR = Ra = \{ar \mid r \in R\}$ is an ideal.

A *ring homomorphism* is a function $f : R \to S$ between two rings such that

$$f(ab) = f(a)f(b), \quad f(a + b) = f(a) + f(b) \quad \text{and} \quad f(1) = 1, \quad \text{for all } a, b \in R.$$

Note that the second equality implies that $f(0) = 0$.

If $R = S$, we call f an *endomorphism*. We call f a ring *isomorphism* if f is bijective, and we write $R \cong S$. An *automorphism* is an isomorphism with $R = S$.

Remark 1.1. A group homomorphism $f : R \to S$ between two rings need not be a ring homomorphism. For instance, the constant function $f : R \to S$ between two nontrivial rings, defined by $f(a) = 0$ for all $a \in R$, is a group homomorphism, but not a ring homomorphism.

The *characteristic* of a commutative ring R is the nonnegative integer n defined by

$$\ker(\rho : \mathbb{Z} \to R) = n\mathbb{Z},$$

where ρ is the unique ring homomorphism $\mathbb{Z} \to R$ mapping $1_\mathbb{Z} \mapsto 1_R$. Equivalently, the characteristic of R is the least positive integer n such that $n1 = 0$, or 0 if no such integer exists. For instance, $\mathbb{Z}$, $\mathbb{Z}/n$, $\{0\}$ have characteristic $0, n$ and 1, respectively.

Several of the following concepts generalise to noncommutative rings. We concentrate our attention to commutative rings, which makes the statements easier. The noncommutative versions are left as an exercise for the interested reader.

Definition 1.2. Let R be a nontrivial commutative ring.

i. A *zero divisor* in R is a nonzero element $a \in R$ such that there exists a nonzero element $b \in R$ with $ab = 0$.

ii. R is an *integral domain*, or simply an *ID* if R has no zero divisors.

iii. A *unit* or an *invertible element* of R is a nonzero element $u \in R$ such that there exists $b \in R$ with $bu = 1$.

iv. The *unit group* of R is the set $R^\times$ of units of R. This is an abelian group.

v. A *field* is an ID R with $R^\times = R - \{0\}$.

Observe that if R and S are IDs, then their cartesian product $R \times S$ is not an ID.

Some rings have additional properties relating to the factorisation, such as:

- A *unique factorisation domain*, or UFD, is an integral domain in which every nonzero noninvertible element has a unique factorisation into a product of irreducible elements (see Definition 1.13) up to the ordering of the factors and the choice of associate irreducible factors. Recall that $a, b \in R$ are *associated*, usually written $a \sim b$, if $a \mid b$ and $b \mid a$, i.e. there exist $c, d \in R$ such that $ac = b$ and $bd = a$. If R is an ID, then $a \sim b$ is equivalent to the existence of $u \in R^\times$ such that $b = ua$. We refer to [Jac, Exercise 7, Section 2.14, Vol I] for an example of ID which is not a UFD.
- A *principal ideal domain*, or PID, is an ID in which every ideal is principal, see Section 1.4 below.
- A *Euclidean domain*, or ED, is an ID with a Euclidean function, i.e. a function $v : R \to \mathbb{N} \cup \{0\}$ such that for all $a, b \in R - \{0\}$, there exists $q, r \in R$ with $a = qb + r$ and $v(r) < v(b)$.

Let R be a commutative ring. An element $a \in R$ is *nilpotent* if there exists $n \in \mathbb{N}$ such that $a^n = 0$ in R. For instance, 2 is nilpotent in $\mathbb{Z}/4$. In particular, if $a \in R$ is a nonzero nilpotent element, then a is a zero divisor in R. If R has no nonzero nilpotent elements, then we say that R is *reduced*. The set of nilpotent elements of R is denoted $\mathrm{Nil}(R)$.

An element $e \in R$ is an *idempotent* if $e^2 = e$. We say that e is a *nontrivial* idempotent if $e \neq 0, 1$. For instance, $0, 1, 3$ and 4 are all the idempotents in $\mathbb{Z}/6$, and an ID has no nontrivial idempotents.

To summarise the relationships between the above classes of commutative rings, we have proper inclusions:

$\{$ fields $\} \subsetneq \{$EDs $\} \subsetneq \{$PIDs $\} \subsetneq \{$UFDs $\} \subsetneq \{$ IDs $\} \subsetneq \{$ reduced rings $\} \subsetneq \{$commutative rings $\}$

In addition to the above types of rings, we record the following class of rings. Recall that a *maximal ideal* of R is a proper ideal I of R such that, if an ideal J of R satisfies $I \subseteq J \subseteq R$, then either $I = J$ or $J = R$ (but not both, of course).

Definition 1.3. A ring is local if it has a unique maximal ideal.

The definition of *local* does not require the ring to be commutative, but many 'interesting' local rings are commutative. Later we will see a process to construct a local ring given a commutative ring, including that of constructing the field of fraction of an ID.

Here are elementary examples of local rings:

- A field.
- $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid \gcd(p, b) = 1\}$ for a prime p.
- $k[x]/(x^2)$, where k is a field.
- $k[[x]]$.
- Discrete valuation rings (cf. [Jac, Section 9, Vol II]).

There are many other classes of rings that we will not cover in this course. The textbooks listed in the bibliography at the end of the notes contain a lot more information.

1.3 Polynomial rings

Let R be a ring. The *(univariate) polynomial ring over* R is the set $R[x]$ of all the *polynomials* in the variable (or indeterminate) x with coefficients in R. That is, all the formal expressions $f = a_n x^n + \cdots + a_1 x + a_0$ for some $n \in \mathbb{N} \cup \{0\}$ and some $a_0, \ldots, a_n \in R$. Addition and multiplication use associativity and distributivity:

$$\Big(\sum_{0\le i\le m} a_i x^i\Big) + \Big(\sum_{0\le i\le n} b_i x^i\Big) = \sum_{0\le i\le \max(m,n)} (a_i + b_i) x^i$$

$$\Big(\sum_{0\le i\le m} a_i x^i\Big)\Big(\sum_{0\le i\le n} b_i x^i\Big) = \sum_{0\le k\le m+n} \Big(\sum_{0\le i\le k} (a_i b_{k-i}) x^k\Big)$$

where we set $a_i = b_j = 0$ whenever $i > m$ or $j > n$. Note that R is commutative if and only if $R[x]$ is commutative too. In fact, R is a UFD if and only if $R[x]$ is a UFD. A *multivariate* polynomial ring can be obtained inductively as a ring extension $R[x_1, \ldots, x_d] = \big(R[x_1, \ldots, x_{d-1}]\big)[x_d]$ in d variables $x_1, \ldots, x_d$. This is a UFD if and only if R is a UFD.

The *power series ring* over R is the ring $R[[x]]$ whose elements are *power series*, that is, formal expressions of the form $\sum_{i\ge 0} a_i x^i$. The construction can be extended to multivariate power series rings. We leave the proof of the following result as an exercise, and we refer to [Jac, Vol II, Section 7.10] for more details about the properties of power series rings.

Lemma 1.4. *Let R be a commutative ring.*

i. R is reduced if and only if $R[[x]]$ is reduced.

ii. R is an ID if and only if $R[[x]]$ is an ID.

1.4 Ideals

Let R be a commutative ring and let I be an ideal of R. A *generating set* of I is a subset X of I, such that I is the set of all the R-linear combinations of the elements of X:

$$I = \{a_1 x_1 + \cdots + a_n x_n \ : \ x_i \in X,\ a_i \in R\}.$$

If $X = \{x_1, \ldots, x_n\}$ is finite, we write $I = x_1 R + \cdots + x_n R$ or $I = (x_1, \ldots, x_n)$ for the ideal of R generated by X. An ideal I is *principal* if I can be generated by a single element, i.e. $I = (a) = aR$

for some $a \in R$. An ID in which every ideal is principal is a *principal ideal domain*, or simply a *PID*. For instance $\mathbb{Z}$ is a PID, but $\mathbb{Z}[x]$ is not a PID.

Given two ideals I, J in a commutative ring R, we can construct new ideals from them: their *intersection*

$$I \cap J = \{a \in R \ : \ a \in I \text{ and } a \in J\},$$

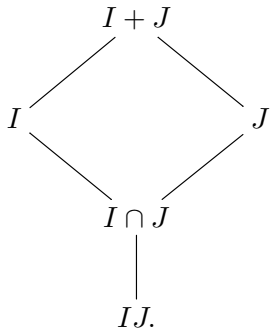
their *product*

$$IJ = \{ \sum_{\text{finite}} ab \ : \ a \in I \text{ and } b \in J\},$$

and their *sum*

$$I + J = \{a + b \ : \ a \in I \text{ and } b \in J\}.$$

They relate in the following diagram, where an edge means that the ideal in the bottom vertex is contained in (or equal to) the ideal in the upper vertex:



If $I = J$, then $I + I = I \cap I = I$, and in general the containment $I \supset I^2$ is proper.

Given $a, b \in R$, recall $a \in bR$ if and only if b *divides* a, i.e. there exists $c \in R$ such that $a = bc$. The *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

- d is a common divisor of a and b, i.e. there exist $a', b' \in R$ such that $a = da'$ and $b = db'$.
- Any common divisor $d' \in R$ of a and b divides d.

Greatest common divisors need not exist, but if they do, then they are uniquely determined up to associates, and we write $\gcd(a, b)$ for *a* greatest common divisor. For instance, if $R = \mathbb{Z}$, then $\gcd(6, 15) = 3$ or -3. Iteratively, we define $\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)$.

Definition 1.5. Let R be a commutative ring, and let I, J be ideals of R. Then I and J are *coprime* if $I + J = R$, or equivalently if there exist $x \in I$ and $y \in J$ such that $1 = x + y$.

If R is a UFD, then we say that $x_1, \ldots, x_n \in R$ are *coprime* if $\gcd(x_1, \ldots, x_n) \in R^\times$, respectively *pairwise coprime* if $\gcd(x_i, x_j) = 1$ for all $i \neq j$.

Lemma 1.6. *Let R be a commutative ring, and let I, J be ideals of R. Suppose that I is maximal and that $J \not\subseteq I$. Then I and J are coprime. Furthermore, $I \cap J = IJ$.*

Proof. By assumption, $I + J$ is an ideal of R containing I properly. The first statement follows from the maximality of I.

It remains to show that $I \cap J \subseteq IJ$. Let $x \in I \cap J$, and let $a \in I, b \in J$ such that $1 = a + b \in I + J = R$. We have $x = x1 = xa + xb \in IJ$, as required.

□

There are two subtly distinct notions:

Definition 1.7. Let R be a commutative ring.

i. An ideal I is *nilpotent* if there exists $n \in \mathbb{N}$ such that $I^n = \{0\}$. That is, the product of any n elements of I is zero.

ii. An ideal I is *nil* if every element of I is nilpotent.

Observe that a nilpotent ideal is nil, but a nil ideal need not be nilpotent, e.g. consider the ring $R = \bigoplus_{n\geq 2} \mathbb{Z}/(2^n)$. (Loosely, the distinction between direct sum and product is that the elements in a direct sum have finitely many nonzero coordinates, which is not required for the elements in a direct product.)

Let I be an ideal I of a commutative ring R. The *quotient ring*, denoted R/I, is the commutative ring whose elements are the cosets $a + I = \{a + x \mid x \in I\}$ of the abelian group R/I, with the multiplication induced by that of R. That is, $(a+I)(b+I) = ab+I$. (It is an exercise to check that this is well-defined.) Let us recall the following two types of ideals.

Definition 1.8. Let R be a commutative ring and let I be an ideal of R.

i. I is a *prime ideal* of R if $I \neq R$ and whenever $ab \in I$ for $a, b \in R$, then $a \in I$ or $b \in I$ or both. The set of prime ideals of R is the *prime ideal spectrum* of R, denoted $\mathrm{Spec}(R)$.

ii. I is a *maximal ideal* of R if $I \neq R$ and whenever $I \subseteq J \subseteq R$ for any ideal J in R, then $J = I$ or $J = R$. (That is, I is not properly contained in any proper ideal of R.) The set of maximal ideals of R is the *maximal ideal spectrum* of R, denoted $\mathrm{MaxSpec}(R)$.

In many rings, prime and maximal ideal provide useful information on the ring structure.

Example 1.9.

i. If $R = \mathbb{Z}$, the maximal and nonzero prime ideals coincide, and they are all of the form $p\mathbb{Z}$, where p is a prime. Hence $\mathrm{Spec}(\mathbb{Z}) = \mathrm{MaxSpec}(\mathbb{Z}) \cup \{(0)\} = \{(p) \mid p \text{ prime or } 0\}$.

ii. Let k be a field.

- $\mathrm{Spec}(k) = \mathrm{MaxSpec}(k) = \{(0)\}$.
- $\mathrm{Spec}(k[x]) = \mathrm{MaxSpec}(k[x]) \cup \{(0)\}$, with $\mathrm{MaxSpec}(k[x]) = \{(f) \mid f \in k[x] \text{ irreducible }\}$.
- $\mathrm{Spec}\left(k[x]/(x^2)\right) = \mathrm{MaxSpec}\left(k[x]/(x^2)\right) = \{(\overline{x})\}$, where $\overline{x} = x + (x^2)$ is the image of x via the natural projection map $k[x] \to k[x]/(x^2)$.
- $\mathrm{Spec}(k[[x]]) = \mathrm{MaxSpec}(k[[x]]) \cup \{(0)\}$, with $\mathrm{MaxSpec}(k[[x]]) = \{(x)\}$.
- $\mathrm{Spec}(k \times k) = \mathrm{MaxSpec}(k \times k) = \{k \times \{0\}, \{0\} \times k\}$

We leave the proof of Theorem 1.10, usually seen in undergraduate algebra, as an exercise. The proof of the last part requires *Zorn's lemma*: *In any nonempty partially ordered set S, if every totally ordered subset has an upper bound in S, then S has some maximal element.*

Theorem 1.10. *Let R be a commutative ring, and let I be a proper ideal of R.*

i. I is prime if and only if the quotient ring R/I is an ID.

ii. I is maximal if and only if the quotient ring R/I is a field. Consequently, every maximal ideal is prime.

iii. I is contained in a maximal ideal. (Every proper ideal is contained in a maximal ideal.)

Here is a nontrivial example.

Example 1.11. Let k be a field and consider the polynomial ring $k[x, y, w, z]$. The ideal

$$(xz - yw, xw - y^2, yz - w^2)$$

is prime, whilst

$$(x - 1, y^2 - x^3)$$

is not prime. (To prove the first claim, it may be useful to observe that every generator is a homogeneous polynomial of degree 2. To prove the second claim, use Theorem 1.10(i).)

Later, we will use the properties of prime ideals to introduce a topology on any commutative ring. For now, we review some useful properties of prime ideals.

Lemma 1.12. *Let R be a commutative ring and let I, J, K be ideals of R. Suppose that $K \supseteq I \cap J$ with K prime. Then at least one of I or J is contained in K.*

Proof. Suppose that $I \not\subseteq K$. Let $a \in I \setminus K$. Then, for any $b \in J$, we have $ab \in I \cap J \subseteq K$, which implies that $b \in K$ for all $b \in J$, since K is prime. Therefore $J \subseteq K$ □

Let us consider some relationships between the properties of elements in a commutative ring R and those of the principal ideals they generate. For instance, $a \in R^\times$ if and only if $aR = R$, whereas $a \in R$ is nilpotent if and only if aR is nil. Given that prime and maximal ideals are relevant in describing the structure of R (see Section 4), we introduce the following notions.

Definition 1.13. Let R be a commutative ring.

i. An element $p \in R$ is *prime* if p is nonzero and not invertible, and if whenever p divides a product ab with $a, b \in R$, then p divides at least one of a or b.

ii. An element $x \in R$ is *irreducible* if x is nonzero and not invertible, and if whenever we can write x as a product $x = ab$ with $a, b \in R$, then $x \sim a$ or $x \sim b$.

Theorem 1.14. *Let R be an ID.*

i. An element $p \in R$ is prime if and only if the principal ideal pR is nonzero and prime.

*ii. An element $p \in R$ is irreducible if and only if the principal ideal pR is nonzero and maximal amongst the set of proper principal ideals of R. (*Maximal *in the following sense: $pR \subseteq aR \subseteq R$ implies $aR = pR$ or $aR = R$ but not both. Though pR need not be a maximal ideal of R.)*

The proof is straighforward from the definitions. For UFDs, we have a stronger statement.

Lemma 1.15. *Let R be a UFD.*

i. Prime and irreducible elements coincide.

ii. If R is a PID, then R is a UFD and the nonzero prime ideals coincide with the maximal ideals. They are of the form pR, for some prime element $p \in R$.

iii. $R[x]$ is a UFD. Moreover, $R[x]$ is a PID if and only if $R[x]$ is an Euclidean domain if and only if R is a field.

1.5 Ring homomorphisms

The morphisms in the category of rings are ring homomorphisms. They are useful to compare rings, or to construct new rings from 'old', for instance.

Given a ring homomorphism $f : R \to S$ between two rings, we define:

- $\ker(f) = \{a \in R \mid f(a) = 0\}$, the *kernel* of f, and
- $\mathrm{im}(f) = \{f(a) \mid a \in R\}$, the *image* (or *range*) of f.

In particular, $\ker(f)$ is an ideal of R and $\mathrm{im}(f)$ is a subring of S, since we require $f(1) = 1$ by definition. A ring homomorphism f is injective if and only if $\ker(f) = \{0\}$ and f is surjective if and only if $\mathrm{im}(f) = S$.

Example 1.16. Let R be a ring.

i. If S is a subring of R, then the inclusion $\iota : S \to R$ is an injective ring homomorphism.

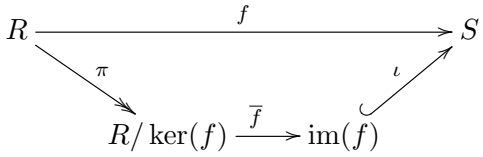
ii. If I is an ideal of R, then the quotient map $\pi : R \to R/I$, given by $\pi(a) = a + I$ is a surjective ring homomorphism.

The key result is the following theorem, from which all the rest of this section can (in some sense) be obtained.

Theorem 1.17 (First isomorphism theorem)**.** *Let $f : R \to S$ be a ring homomorphism. Then f induces a ring isomorphism*

$$\overline{f} : R/\ker(f) \longrightarrow \mathrm{im}(f), \quad \overline{f}(a + \ker(f)) = f(a).$$

The statement of Theorem 1.17 can be represented in the diagram:



That is, $a, b \in R$ have the same image via f if and only if $b - a \in \ker(f)$, which implies that the map f *factors* through the quotient ring $R/\ker(f)$. The induced map $R/\ker(f) \to S$ is necessarily injective. Restricting the codomain to $\mathrm{im}(f)$ yields an isomorphism $\overline{f} : R/\ker(f) \longrightarrow \mathrm{im}(f)$, since every function is surjective on its image. (We indicate surjections with $\twoheadrightarrow$ and injections with $\hookrightarrow$.)

From Theorem 1.17, we deduce the following. The proof is left as exercise.

Corollary 1.18. *Let $f : R \to S$ be a ring homomorphism, and let $\overline{f} : R/\ker(f) \to \mathrm{im}(f)$ be the induced ring isomorphism.*

i. Every ideal I of R is the kernel of some ring homomorphism with domain R.

ii. $\overline{f}$ induces an inclusion-preserving bijection between the sets of ideals of R containing $\ker(f)$ and the ideals of $R/\ker(f)$. Moreover, under this correspondence, the sets of prime (resp. maximal) ideals of R containing $\ker(f)$ map to the prime (resp. maximal) ideals of $R/\ker(f)$.

iii. If I is an ideal of R containing $\ker(f)$, then the quotient map $\pi : R \to R/I$ induces a ring isomorphism $R/I \xrightarrow{\cong} (R/\ker(f))/(I/\ker(f))$.

We end this section with a nontrivial example, showing that there may be more (maximal) ideals than we may think at first. Let $R = k^{\mathbb{N}}$ be the cartesian product of countably many copies of a field k (i.e. the sequences in k). Endow R with the coordinatewise addition and multiplication, so that R is a commutative ring (not finitely generated).

- For every $i \in \mathbb{N}$, let $I_i = \{(a_j)_{j\in\mathbb{N}} \in R \mid a_i = 0\}$. Then I_i is a maximal ideal of R, since $R/I_i \cong k$ (and I_i is an ideal). Thus, we obtain countably many distinct maximal ideals of R, and $\cap_{i\in\mathbb{N}} I_i = \{0\}$.
- Let $J = \{(a_j)_{j\in\mathbb{N}} \in R \mid \exists$ a finite set $F \subset \mathbb{N}$ with $a_j = 0, \forall\, j \notin F\}$. Note that J is an ideal of R, and J is not contained in any of the I_i. We claim that J is not a prime ideal of R. Consider the quotient R/J. The nonzero elements are the cosets $a + J$, where $a = (a_i)_{i\in\mathbb{N}} \in R$, such that each such coset representative has infinitely many nonzero coordinates a_i. Let $a = (a_i)_{i\in\mathbb{N}}$ and $b = (b_i)_{i\in\mathbb{N}}$ with $a_{2d} = b_{2d+1} = 1$ and $a_{2d+1} = b_{2d} = 0$ for all $d \in \mathbb{N}$. Then $a, b \notin J$, and so $a + J, b + J \neq 0_{R/J}$. But $ab = 0_R$, and so $(a + J)(b + J) = 0_{R/J}$. Therefore R/J is not an ID.

1.6 Contraction and expansion of ideals

In this section, we consider ring homomorphisms to compare the ideals in two commutative rings. Given a ring homomorphism $\varphi : R \to S$, the preimage

$$\varphi^{-1}(J) = \{a \in R \mid \varphi(a) \in J\} \quad \text{of an ideal } J \text{ of } S$$

is an ideal of R (cf. Exercises below). Moreover, if $J \in \mathrm{Spec}(S)$, then $\varphi^{-1}(J) \in \mathrm{Spec}(R)$, but this does not hold in general for the maximal ideals.

Definition 1.19. Let $\varphi : R \to S$ be a ring homomorphism, let I be an ideal of R and let J be an ideal of S.

i. The *contraction* of J to R is the ideal $J^c = \varphi^{-1}(J)$ of R.

ii. The *expansion* of I to S is the ideal $I^e = \varphi(I)S$ of S. That is, I^e is the smallest ideal of S containing $\varphi(I)$.

The contraction of prime ideals of S to R along φ induces a function

$$\varphi^* : \mathrm{Spec}(S) \longrightarrow \mathrm{Spec}(R), \quad J \longmapsto \varphi^{-1}(J).$$

We will study the properties of φ^* in Section 4. We call φ^* the *induced morphism*.

A special case is that of a quotient map $\pi : R \to R/I$, where I is an ideal of R. Then $\pi^* : \mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ is an inclusion, since the prime ideals of R/I are in 1-1 correspondence with those of R containing I. In such a situation, we call the induced morphism π^* a *closed immersion*.

Example 1.20.

i. Let k be a field of positive characteristic p, and let $\rho : \mathbb{Z} \to k$ be the characteristic homomorphism. Then $\rho^*((0)) = (p)$. Note in this case that ρ^* is a closed immersion if and only if $k = \mathbb{F}_p$.

ii. Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring with coefficients in a field k. Let $\epsilon : R \to k$ be the evaluation map at $(a_1, \ldots, a_n) \in k^n$. So ϵ is a surjective ring homomorphism, with $\ker(\epsilon) = (x - a_1, \ldots, x - a_n) \in \mathrm{MaxSpec}(R)$. That is, $\epsilon^*((0)) = (x - a_1, \ldots, x - a_n)$, and ϵ^* is a closed immersion.

1.7 Nilpotent elements and radical ideals

In this section we briefly discuss the notion of *radical* of an ideal.

Definition 1.21. Let R be a commutative ring.

i. Let I be an ideal of R. The *radical of* I is the ideal

$$\sqrt{I} = \{a \in R \mid \exists\, n \in \mathbb{N} \text{ such that } a^n \in I\}.$$

We call I a *radical ideal* of R if $I = \sqrt{I}$.

ii. The *nilradical of* R is the ideal

$$\mathrm{Nil}(R) = \bigcap_{P \in \mathrm{Spec}(R)} P.$$

iii. The *Jacobson radical of* R is the ideal

$$\mathrm{Rad}(R) = \bigcap_{P \in \mathrm{MaxSpec}(R)} P.$$

Example 1.22.

- $\mathrm{Nil}(\mathbb{Z}) = \mathrm{Rad}(\mathbb{Z}) = \{0\}$, and the same holds for any PID.
- If R is an ID, then $\mathrm{Nil}(R) = \{0\}$. But $\mathrm{Rad}(R)$ can be strictly larger. For instance, if R is a local ID, e.g. $R = k[[x]]$ with k a field, or $R = \mathbb{Z}_{(p)}$, then $\mathrm{Rad}(R) \neq (0)$ is the unique maximal ideal.
- Let $R = \mathbb{C}[x]$ and let $I = (x^3 - 1)$. Then $I = \sqrt{I} \notin \mathrm{Spec}(R)$.

Given a commutative ring R, we can detect the nilpotent elements as follows.

Theorem 1.23. *Let R be a commutative ring, and let $a \in R$. Then a is nilpotent if and only if $a \in P$ for all $P \in \mathrm{Spec}(R)$. That is, $\mathrm{Nil}(R)$ is the set of nilpotent elements of R.*

Proof. Suppose that $a^n = 0$ for some $n \geq 1$. Since $0 \in I$ for any ideal, then $a \in P$ for any prime ideal P. Indeed, this is obvious if $n = 1$. If $n > 1$, write $a^n = a \cdot a^{n-1}$ and argue by induction to obtain the desired conclusion.

Conversely, suppose that a is not nilpotent. Let $A = \{a^n,\ n \in \mathbb{N}\}$, and let $X = \{I \text{ ideal of } R \mid I \cap A = \emptyset\}$. Note that $X \neq \emptyset$ since $(0) \in X$. Moreover, X is a poset (=partially ordered set) for the inclusion of ideals, and each totally ordered subset of X has an upper bound in X. Namely, if $I_1 \subseteq I_2 \subseteq \ldots$ is a chain in X, then $I = \cup_i I_i \in X$, since $I \cap A = \emptyset$, and I is an upper bound of the chain. Hence by Zorn's lemma, X has a maximal element.

Pick a maximal element I of X. Let $x, y \in R$ such that $x, y \notin I$. Then the ideals (x, I) and (y, I) contain I properly, and so their intersections with A are nonempty. That is, there exist $m, n \in \mathbb{N}$ such that $a^m \in (x, I)$ and $a^n \in (y, I)$. It follows that $a^{m+n} \in (xy, I)$, which shows that $xy \notin I$. Hence I is prime and does not contain a. The result follows.

□

Here is a useful property of radicals of ideals in general. Note that if two ideals I, J of R are coprime, then $R = I + J \subseteq \sqrt{I} + \sqrt{J}$ shows that $\sqrt{I}, \sqrt{J}$ are coprime too.

Lemma 1.24. *Let R be a commutative ring, and let I, J be ideals of R. Suppose that $\sqrt{I}$ and $\sqrt{J}$ are coprime. Then I and J are coprime.*

Proof. It suffices to show that $\sqrt{I+J} = R$. The inclusions $I, J \subseteq I+J$ imply that $\sqrt{I}, \sqrt{J} \subseteq \sqrt{I+J}$, and since $\sqrt{I+J}$ is an ideal, $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I+J}$. The result follows. □

The next result does not require the ring to be commutative, but since our definition of the Jacobson radical has been specialised to commutative rings, we state the result for commutative rings only. See [Isa, Section 13B] and [Jac, Vol II, Section 4.2] for a detailed discussion and analysis in the general case.

Proposition 1.25. *Let R be a commutative ring.*

i. If $a \in \mathrm{Rad}(R)$, then $1 - a \in R^\times$.

ii. If $a \in R$ is nilpotent, then $1 - a \in R^\times$.

Proof. i. Let $a \in \mathrm{Rad}(R)$. Then, $1-a$ is not invertible if and only if the principal ideal $(1-a)R \neq R$. Thus, if $1 - a \notin R^\times$, then $(1-a)R \subseteq I$ for some maximal ideal I. But then $1 = (1-a) + a \in \mathrm{Rad}(R) + I = I$, a contradiction. Therefore, $(1-a)R = R$, i.e. $1-a$ is invertible.

ii. Suppose that $a^n = 0$ for some integer $n \geq 2$. (The assertion is trivial if $n = 1$.) Then $1 = 1 - a^n = (1-a)\big(\sum_{i=0}^{n-1} a^i\big)$, as required.

□

Note that the first statement is not an if and only if. For instance, if $R = \mathbb{Z}/6$, then $\mathrm{Rad}(R) = (2) \cap (3) = (0)$. Let $a = 4$. Since $a^2 = a$, we have $1 - 2a = 5 \in R^\times$, but $2a = 2 \notin J(R)$.

Let us observe some elementary facts.

Proposition 1.26. *Let R be a commutative ring and let I be an ideal of R. Let $\pi : R \to R/I$ be the quotient map. Then $\sqrt{I} = \pi^{-1}(\mathrm{Nil}(R/I))$. In particular, $I = \sqrt{I}$ if and only if R/I is reduced (i.e. $\mathrm{Nil}(R/I) = (0)$).*

Proof. Let $a \in \pi^{-1}(\mathrm{Nil}(R/I))$. That is, $a \in R$ and $\pi(a) \in \mathrm{Nil}(R/I)$. By Theorem 1.23, $\pi(a)$ is nilpotent in R/I. That is, there exists $n \in \mathbb{N}$ such that $\pi(a)^n = 0_{R/I}$, In other words, $a^n \in I$, and so $a \in \sqrt{I}$.

We leave the proof of converse as an exercise, since it is very similar. □

Corollary 1.27. *Let R be a commutative ring and let I be an ideal of R. Then,*

$$\sqrt{I} = \bigcap_P P \quad \textit{where } P \textit{ runs through the prime ideals of } R \textit{ containing } I.$$

Hence, the prime ideals containing I are precisely those containing $\sqrt{I}$. That is $\mathrm{Spec}(R/I)$ is in bijection with $\mathrm{Spec}(R/\sqrt{I})$. (This is in fact a homeomorphism, as will prove in Section 4.)

Proof. Let $\pi : R \to R/I$ be the quotient map. By Proposition 1.26, $\sqrt{I} = \pi^{-1}(\mathrm{Nil}(R/I))$, and by Theorem 1.23, $\mathrm{Nil}(R/I) = \cap_{P \in \mathrm{Spec}(R/I)} P$. The result follows since π induces a bijection between the sets of prime ideals of R containing I and the prime ideals of R/I. Indeed, $\pi^{-1}(P) \in \mathrm{Spec}(R)$ for all $P \in \mathrm{Spec}(R/I)$, and such ideals contain I. Conversely, if $P \in \mathrm{Spec}(R)$ contains I, then $(R/I)/(P/I) \cong R/P$ is an ID, and so $P/I = \pi(P) \in \mathrm{Spec}(R/I)$. □

1.8 Localisation of a commutative ring

Recall that given an ID R, the *field of fractions* of R, also called the *quotient field* of R, is the set

$$\{\frac{a}{b} \mid a, b \in R,\ b \neq 0\}, \quad \text{with} \quad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b}\,\frac{c}{d} = \frac{ac}{bd}.$$

In this section, we generalise the construction in the category of commutative rings.

Definition 1.28. Let R be a commutative ring. A *multiplicative set (of R)* is a subset U of R such that the following conditions hold:

- $1 \in U$,
- $0 \notin U$, and
- U is closed under multiplication, i.e. $st \in U$ for all $s, t \in U$.

For instance, if R is an ID, then $R \setminus \{0\}$ is a multiplicative set in any ID. If $R = \mathbb{Z}/6$, then $\{1, 2, 4\}$ is a multiplicative set which contains zero divisors.

Lemma 1.29. *Let R be a commutative ring and let I be a prime ideal of R. Then $U = R \setminus I$ is a multiplicative set.*

Proof. Since I is a proper ideal, $1 \notin I$ and $0 \in I$. Moreover, since I is prime, if $a, b \in R \setminus I$, then $ab \in R \setminus I$, as required. □

Another example of multiplicative set of a commutative ring R is the set of nonzero elements of R that are not zero divisors of R:

$$U = R \setminus \mathcal{Z}, \quad \text{where} \quad \mathcal{Z} = \{a \in R \mid \exists\ b \in R \setminus \{0\} \text{ such that } 0 = ab\}.$$

We have:

- $1 \in U$ and $0 \notin U$.
- For any $a, b \in U$, then $ab \in U$. Indeed, if there is $c \in R$ with $c \neq 0 = (ab)c$, then $0 = a(bc) = b(ac)$ shows that $a, b \in \mathcal{Z}$.

Theorem 1.30. *Let R be a commutative ring and let U be a multiplicative set of R. Define*

$$R_U = R \times U/\sim, \quad \textit{where} \quad (a, s) \sim (b, t) \iff \exists\ d \in U \textit{ such that } d(at - bs) = 0.$$

Write $[a, s]$ for the equivalence class of (a, s). Then R_U is a commutative ring with $0 = [0, 1]$, with $1 = [1, 1]$ and with

$$[a, s] + [b, t] = [at + bs, st] \quad \textit{and} \quad [a, s][b, t] = [ab, st].$$

The function $\theta : R \to R_U$ (the canonical map*), given by $\theta(r) = [r, 1]$ is a ring homomorphism and $\theta(U) \subseteq (R_U)^\times$. Moreover, θ is injective if U has no zero divisors. In this case, $\operatorname{char} R = \operatorname{char} R_U$.*

Definition 1.31. Let R be a commutative ring and let U be a multiplicative set of R. The ring R_U constructed in Theorem 1.30 is the *localisation of R at U*. The elements of R_U are often denoted by fractions $\frac{a}{s}$ instead of $[a, s]$, to emphasise the fact that we formally *invert* the elements of U in R_U.

Remark 1.32. The above definition of the localisation R_U is simpler if U contains no zero divisors. Indeed, the condition $\exists\ d \in U$ such that $d(at - bs) = 0$ is equivalent to $at = bs$, since our assumption on U imples that $dr = 0$ if and only if $r = 0$. The reason for the extra condition in the general case lies in the proof of the transitivity of $\sim$ below.

Proof. Explicitly, for $a \in R$ and $s \in U$, we have

$$[a, s] = \{(b, t) \in R \times U \mid at = bs\}.$$

It is routine to check that $\sim$ is an equivalence relation, and that R_U is a commutative ring with the given operations. Indeed, $\sim$ is

- reflexive since $(a, s) \sim (a, s) \iff as = as$,
- symmetric since $(a, s) \sim (b, t) \iff at = bs \iff bs = at \iff (b, t) \sim (a, s)$, and
- transitive since if $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$, i.e. $d(at - bs) = 0 = e(bu - ct)$ for some $d, e \in U$, then by multiplying $d(at - bs) = 0$ by eu and $e(bu - ct) = 0$ by ds, and adding both together, that $det(au - cd) = 0$, with $det \in U$. Hence $(a, s) \sim (c, u)$.

We now need to prove that addition and multiplications are well defined. That is, suppose that $(a, s) \sim (a', s')$ and $(b, t) \sim (b', t') \in R \times U$, in other words, we assume that $d(as' - a's) = 0 = e(bt' - b't)$ for some $d, e \in U$. We want to show that $[a, s] + [b, t] = [a', s'] + [b', t']$ and that $[a, s][b, t] = [a', s'][b', t']$. By definition, $[a, s] + [b, t] = [at + bs, st]$, $[a', s'] + [b', t'] = [a't' + b's', s't']$, and we need to check that $(at + bs, st) \sim (a't' + b's', s't')$. We calculate

$$\begin{aligned} de(at + bs)(s't') &= deats't' + bss't' = d(as')tt'e + e(bt')ss'd = d(a's)tt'e + e(b't)ss'd \\ &= de(a't')(st) + de(b's')(st) = de(a't' + b's')(st) \end{aligned}$$

as required. Similarly for the multiplication, which we leave as an exercise, together with the proof of the associativity and commutativity of these operations. Observe that $1 = [1, 1] = \{(s, s) \mid s \in U\}$ and $0 = [0, 1] = \{(0, s) \mid s \in U\}$.

It remains to show that θ is a ring homomorphism and that θ is injective if U has no zero divisors. Let $a, b \in R$. Then $\theta(1) = 1$,

$$\theta(a) + \theta(b) = [a, 1] + [b, 1] = [a1 + b1, 1] = [a + b, 1] = \theta(a + b)$$

and

$$\theta(a)\theta(b) = [a, 1][b, 1] = [ab, 1] = \theta(ab).$$

If U has no zero divisors, then $[0, 1] = \theta(a) = [a, 1]$ if and only if $0 = d(a1 - a)$ for some $d \in U$, which implies that θ is injective.

Finally, the last claim is clear since a subring of a commutative ring has the same characteristic. □

Example 1.33. Let $R = \mathbb{Z}$ and $U = \mathbb{Z} \setminus p\mathbb{Z} = \{a \in \mathbb{Z} \mid p \nmid a\}$, where p is a given prime. Then

$$R_U \cong \left\{ \frac{a}{s} \in \mathbb{Q} \mid p \nmid s \right\} \subsetneq \mathbb{Q},$$

often denoted $\mathbb{Z}_{(p)}$ in the literature.

By contrast, if $U = \{p^n \mid n \geq 0\}$, then

$$R_U = \mathbb{Z}\left[\frac{1}{p}\right] = \left\{ \frac{a}{p^n} \mid a \in \mathbb{Z},\ n \geq 0 \right\} \subsetneq \mathbb{Q}.$$

Example 1.34. Let $R = \mathbb{Z}[x]$, and take $p = x^2 - 2$. Then p is irreducible in R, hence prime since R is a UFD, and so (p) is a prime ideal. Let $U = R \setminus (p)$. Then U is a multiplicative set with no zero divisors. The localisation R_U is isomorphic to the subring

$$R_U = \left\{ \frac{f}{g} \in \mathbb{Q}(x) \mid (x^2 - 2) \nmid g \right\} \quad \text{of the field of rational functions } \mathbb{Q}(x).$$

In other words, we have extended $\mathbb{Z}[x]$ by adjoining multiplicative inverses of the polynomials not divisible by $x^2 - 2$.

For $R = \mathbb{Z}$, we have considered two different localisations: $\mathbb{Q}$ and $\mathbb{Z}_{(p)}$, respectively the localisations of $\mathbb{Z}$ at the prime ideals (0) and (p), for a prime p. Observe that

$$\mathbb{Z}_{(p)} \subseteq \mathbb{Q} \quad \text{and} \quad (p) \supseteq (0), \quad \text{with} \quad (0), (p) \in \operatorname{Spec}(\mathbb{Z}_{(p)}).$$

The localisation of $\mathbb{Z}_{(p)}$ at (0), i.e. the field of fractions of $\mathbb{Z}_{(p)}$, is isomorphic to $\mathbb{Q}$, as follows from the next result.

Proposition 1.35. *Let R be a commutative ring and U, U' two multiplicative sets with no zero divisors. Suppose that $U' \subseteq U$. Then, there is a ring isomorphism*

$$R_U \cong \big(R_{U'}\big)_{U/U'}, \quad \textit{where} \quad U/U' = \{\frac{s}{s'} \in R_{U'} \mid s \in U,\ s' \in U'\}.$$

In particular, there exists an injective ring homomorphism $R_{U'} \longrightarrow R_U$.

Proof (Sketch). The assertion about the existence of an injective ring homomorphism is a direct application of Theorem 1.30, once we have proved that R_U is the localisation $\big(R_{U'}\big)_{U/U'}$.

First, note that U/U' is a multiplicative set of $R_{U'}$ with no zero divisors. The elements of $\big(R_{U'}\big)_{U/U'}$ are equivalence classes $\big[[a,t'],[s,s']\big] = \frac{\frac{a}{t'}}{\frac{s}{s'}}$, and $\frac{\frac{a}{t'}}{\frac{s}{s'}} = \frac{\frac{b}{u'}}{\frac{v}{v'}}$ if and only if

$$\frac{a}{t'}\frac{v}{v'} = \frac{b}{u'}\frac{s}{s'} \iff \frac{av}{t'v'} = \frac{bs}{u's'} \iff avu's' = bst'v',$$

where $a, b \in R,\ s, v \in U$ and $s', t', u', v' \in U'$.

Define a function $\sigma : R_U \longrightarrow \big(R_{U'}\big)_{U/U'}$ by $\sigma(\frac{a}{s}) = \frac{\frac{a}{1}}{\frac{s}{1}}$. We can check (exercise) that σ is a ring homomorphism. Moreover, we observe that $\frac{\frac{a}{1}}{\frac{s}{1}} = \frac{\frac{a}{s'}}{\frac{s}{s'}}$, for all $s' \in U'$, which proves that every element of $U/U' \subseteq \big(R_{U'}\big)_{U/U'}$ is invertible. The result follows. (for a more conceptual proof, see [Jac, Vol II, Proposition 7.4]). □

The localisation of a commutative ring is a construction which satisfies a universal property.

Proposition 1.36. *Let $f : R \to S$ be a ring homomorphism, where R and S are commutative rings. Let $U \subseteq R$ be a multiplicative set, and suppose that $f(U) \subseteq S^\times$. Then, there exists a unique ring homomorphism $\tilde{f} : R_U \to S$ such that $\tilde{f}\theta = f$, i.e we have a commutative diagram*

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\theta}\downarrow & \nearrow_{\exists!\tilde{f}} & \\ R_U & & \end{array}$$

Proof. Define $\tilde{f}\big(\frac{a}{s}\big) = f(a)f(s)^{-1}$ for all $\frac{a}{s} \in R_U$, which makes sense since $f(s) \in S^\times$ by assumption. A routine computation shows that $\tilde{f}$ is independent of the choice of representative in the class $\frac{a}{s}$. Indeed, if $(a,s) \sim (a',s')$, say $d(as' - a's) = 0$, then

$$0 = f(d(as' - a's)) = f(d)\big(f(a)f(s') - f(a')f(s)\big) = f(a)f(s') - f(a')f(s), \quad \text{since } f(d) \in S^\times.$$

To show the uniqueness of $\tilde{f}$, note that for all $s \in U$, any ring homomorphism $\dot{f} : R_U \to S$ extending f must satisfy $\dot{f}\big(\frac{1}{s}\big) = f(s)^{-1}$, since $1 = \dot{f}\big(\frac{1}{1}\big) = \dot{f}\big(\frac{s}{1}\ \frac{1}{s}\big) = f(s)\dot{f}\big(\frac{1}{s}\big)$.

The result follows. □

The examples mentioned in Example 1.33 are the main examples of localisation of rings.

- The *localisation of R at a prime ideal I* is the ring usually written R_I (instead of $R_{R\setminus I}$), is the localisation with respect to the multiplicative set $R \setminus I$. Since we invert every element of R that does not belong to I, the ring R_I is local, with unique maximal ideal $\theta(I)R_I$, see Corollary 1.40 below. For instance $\mathbb{Z}_{(p)}$ for p a prime, or the field of fractions of an ID.
- The *localisation of R with respect to an element $a \in R$*, usually written $R[a^{-1}]$ is the localisation of R with respect to the multiplicative set $\{1, a, a^2, a^3, \dots\}$. For instance, the ring of Laurent polynomials $k[t, t^{-1}]$ is the localisation of the polynomial ring $k[t]$ with respect to the multiplicative set $\{1, t, t^2, \dots\}$.
- An example showing that θ need not be injective (and so R not isomorphic to a subring of R_U) is the localisation of $\mathbb{Z}/6$ with respect to $\{1, 3\}$. Then $2 \mapsto \theta(2) = \frac{2}{1} = \frac{2}{1}\,\frac{3}{3} = \frac{0}{1}$.

Example 1.37. Let $n \in \mathbb{Z}$ with distinct prime divisors $p_1, \dots, p_d$. The ring $\mathbb{Z}[n^{-1}]$ is isomorphic to the subring of $\mathbb{Q}$ formed by all the elements whose denominators are non-negative powers of n. The canonical map $\theta : \mathbb{Z} \to \mathbb{Z}[n^{-1}]$ and the induced function $\theta^* : \mathrm{Spec}(\mathbb{Z}[n^{-1}]) \to \mathrm{Spec}(\mathbb{Z})$, as defined in Section 1.6, are injective. We have $\mathrm{Spec}(\mathbb{Z}[n^{-1}]) = \mathrm{Spec}(\mathbb{Z}) \setminus \{(p_i),\ 1 \le i \le d\}$.

Consider the localisation R_U of a commutative ring R with respect to a multiplicative set U, and let $\theta : R \to R_U$ be the canonical map. Let I be an ideal of R, and let J be an ideal of R_U. The expansion $\theta(I)R_U = \{[a, s] \in R_U \mid \exists\, b \in R \text{ such that } a = bs\}$ of I, and the contraction $\theta^{-1}(J) = \{a \in R \mid \exists\, s \in U \text{ such that } [a, s] \in J\} = \{a \in R \mid [a, 1] \in J\}$ of J satisfy the following. (Note that $\theta(as) = \frac{as}{1}$, and that $\frac{a}{1} = \frac{1}{s}\frac{as}{1}$ for all $a \in R$ and all $s \in U$.)

- If $J \neq R_U$, then $\theta^{-1}(J) \cap U = \emptyset$.
- If $I \cap U = \emptyset$, then $\theta(I)R_U = \{\frac{a}{s} \in R_U \mid a \in I,\ s \in U\} \neq R_U$.

Theorem 1.38. *Let R_U be the localisation of a commutative ring R with respect to a multiplicative set U, and let $\theta : R \to R_U$ be the canonical homomorphism.*

i. The expansion: $I \mapsto \theta(I)R_U$ yields an order-preserving bijection between the prime ideals of R which do not meet U and the prime ideals of R_U. Its inverse is given by the contraction of ideals.

ii. Every ideal J of R_U is the expansion of its contraction, i.e. $J = J^{ce} = \theta\big(\theta^{-1}(J)\big)R_U$.

iii. Every ideal I of R is contained in the contraction of its expansion, i.e. $I \subseteq I^{ec} = \theta^{-1}\big(\theta(I)R_U\big)$.

Definition 1.39. In the notation of Theorem 1.38, the ideal

$$I^{ec} = \theta^{-1}\big(\theta(I)R_U\big) = \{a \in R \mid \exists\, s \in U \text{ such that } as \in I\}$$

of Part (iii) is the *saturation of I with respect to U*. An ideal I of R is *saturated*, if $I = \theta^{-1}\big(\theta(I)R_U\big)$

Proof of Theorem 1.38. The third part holds, as observed above. For the second part, we also have noted that $J \subseteq J^{ce}$ for any ideal J of R. Conversely, let $\frac{a}{s} \in J$. Then

$$\theta(a) = \frac{a}{1} = \frac{a}{s}\frac{s}{1} = \frac{a}{s}\theta(s) \in \theta(R) \cap J.$$

Identifying R with its image $\theta(R)$, the equality shows that $a \in J^c$. So $\frac{a}{s} \in aR_U \subseteq J^cR_U = J^{ce}$, as required.

For the first part, since $\theta(U) \subseteq (R_U)^\times$, the expansion $\theta(I)R_U$ of an ideal I of R is a proper ideal of R_U if and only if $I \cap U = \emptyset$. Clearly, the expansion-contraction maps are order preserving between the

ideals of R and those of R_U. We also know that if $J \in \mathrm{Spec}(R_U)$, then $\theta^{-1}(J) \in \mathrm{Spec}(R)$. It remains to prove that $\theta(I)R_U \in \mathrm{Spec}(R_U)$ for $I \in \mathrm{Spec}(R)$. If I is prime and $a \in \theta^{-1}(\theta(I)R_U)$, then there exist $b \in I$ and $s, t \in U$ such that $\frac{a}{s}\frac{b}{t} \in \theta(I)R_U$. Thus, there exists $u \in U$ such that $u(at - bs) = 0 \in I$, and since $ut \in U$ and I is prime, our assumption $I \cap U = \emptyset$ forces $a \in I$. Therefore $\theta^{-1}(\theta(I)R_U) \subseteq I$, and hence $I = I^{ec} = \theta^{-1}(\theta(I)R_U)$.

□

The saturation of an ideal is generally bigger than the ideal. For instance, let p be a prime and consider the localisation $\mathbb{Z}[p^{-1}]$ of $\mathbb{Z}$. Then, the saturation $(n\mathbb{Z})^{ec}$ of $n\mathbb{Z}$, with $n = p^d m$ where $\gcd(p, m) = 1$ is the ideal $m\mathbb{Z}$.

We conclude this section with the following consequence of Theorem 1.38.

Corollary 1.40. *Let R be a commutative ring and let I be a prime ideal of R. The localisation R_I of R at I is a local ring.*

Proof. Recall that U is a multiplicative set and that , for any ideal J of R which is not contained in I, then $J^e = R_I$, since the image in R_I of any element of J not contained in I is invertible. By Theorem 1.38, $\mathrm{MaxSpec}(R_I) \subseteq \mathrm{Spec}(R_I) = \{J^e \mid J \in \mathrm{Spec}(R),\ I \subseteq J\}$. Hence, any proper ideal of R_I is contained in I^e.

□

1.9 Exercises

Exercise 1.1. Prove that the cartesian product of two IDs is not an ID.

Exercise 1.2. Let R be the ring of continuous real-valued functions on $[0, 1]$. Show that $\{f \in R \mid f(0) = 0\}$ is a maximal ideal of R.

Exercise 1.3. Let R, S be two commutative rings, and let $\mathrm{Hom}(R, S)$ be the set of ring homomorphisms $R \to S$. Can $\mathrm{Hom}(R, S)$ be made into a group? What if we consider the set $\mathrm{Hom}_{\mathbf{AbGr}}(R, S)$ of (abelian) group homomorphisms $R \to S$?

Exercise 1.4. Let R be a ring, and let $e \in R$. Assume that e is a nontrivial idempotent.

i. Prove that e is a zero divisor, and that $1 - 2e \in R^\times$.

ii. Prove that eR is a ring with multiplicative identity e. Hence, find a ring S and a ring isomorphism $R \cong eR \times S$.

iii. Let S be a ring. Describe $\mathrm{Nil}(R \times S)$. Deduce that if R and S are reduced rings, then $R \times S$ is reduced too.

iv. Prove that an ID is reduced, but there are reduced rings which are not IDs, and find an example of such a reduced commutative ring.

Exercise 1.5. Find the maximal ideals in the local rings $\mathbb{Z}_{(p)}$, $k[x]/(x^2)$ and $k[[x]]$, where p is a prime and k is a field.

Exercise 1.6. Let k be field and let $M_n(k)$ be the ring of $n \times n$ matrices for some integer $n \geq 2$. Describe the two-sided ideals of $M_n(k)$.

Exercise 1.7. Let $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$. Prove that $\mathbb{Z}[i\sqrt{5}]$ is not a UFD.

Exercise 1.8. Let K be an extension field of k. Hence K is a k-vector space and a commutative ring (i.e. a k-*algebra* as we shall see). Prove that

i. The set of k-linear transformations $\varphi : k[x_1, \ldots, x_n] \to K$ such that $\varphi(fg) = \varphi(f)\varphi(g)$ for all $f, g \in k[x_1, \ldots, x_n]$ is in bijection with K^n.

ii. If $I = (f_1, \ldots, f_m)$ is an ideal of $k[x_1, \ldots, x_n]$ then the set of k-linear transformations $\varphi : \big(k[x_1, \ldots, x_n]\big)/I \to K$ such that $\varphi(fg) = \varphi(f)\varphi(g)$ is in bijection with the set of n-tuples $a = (a_1, \ldots, a_n) \in K^n$ such that $f_1(a) = \cdots = f_m(a) = 0$.

iii. Suppose that $k = K = \mathbb{C}$ and let $I = (x_1 - a_1, \ldots, x_n - a_n)$. Prove that I is a maximal ideal of $\mathbb{C}[x_1, \ldots, x_n]$

Exercise 1.9. Let R be a commutative ring.

i. Prove that an ideal I of R is proper if and only if $I \cap R^\times = \emptyset$. In particular, a field has no nontrivial proper ideals.

ii. Prove that $R[x]$ is a PID if and only if R is a field.

iii. Prove that the union of two ideals is an ideal if and only if one contains the other.

iv. Let $e \in R$ be an idempotent. Prove that eR is an ideal.

v. Let $a \in \mathrm{Nil}(R)$. Prove that $aR \subseteq \mathrm{Nil}(R)$.

Exercise 1.10. Let k be a field, let $R = k[x, y]$ and let $I = xR + yR$. Describe the powers $I^n = \underbrace{I \cdots I}_{n \text{ times}}$ for $n \in \mathbb{N}$.

Exercise 1.11. [Jac, Proposition 7.2, Vol II] Let R be a commutative ring and let U be a multiplicative subset of R. Let I be an ideal of R such that I is maximal in the poset

$$\{J \text{ ideal of } R \mid J \cap U = \emptyset\},$$

where the order relation is given by the inclusion of ideals. Prove that I is prime.

Exercise 1.12. Let R be a ring and let I be an ideal of R. Prove that the following statements are equivalent:

i. I is prime.

ii. If J, K are ideals of R such that $JK \subseteq I$, then at least one of J or K must be contained in I.

iii. There do not exist ideals J, K of R with $J \not\subseteq I$ and $K \not\subseteq I$, and such that $JK \subseteq I$.

Exercise 1.13. Describe $\mathrm{Spec}(\mathbb{Z}[x])$ and $\mathrm{MaxSpec}(\mathbb{Z}[x])$. Same question with $\mathbb{R}$ and with $\mathbb{C}$ instead of $\mathbb{Z}$. (Hint: Theorem 1.14 may be useful.)

Exercise 1.14. Let $f : R \to S$ be a ring homomorphism.

i. Prove that the preimage $f^{-1}(J)$ is an ideal of R for every ideal J of S. If the image $f(I)$ an ideal of S for an ideal I of R?

ii. If I is a prime ideal of S, is $f^{-1}(I)$ a prime ideal of R? Same question for maximal ideals.

Exercise 1.15. Let R be a commutative ring, let I be an ideal in R and let X be a nonempty subset of R. Define

$$(I \ : \ X) = \{a \in R \ : \ aX \subseteq I\}, \quad \text{where} \quad aX = \{ax \ : \ x \in X\}.$$

i. Prove that $(I \ : \ X)$ is an ideal of R.

ii. Let J be the ideal in R generated by the subset X of R. Prove that $(I \ : \ X) = (I \ : \ J)$, for any ideal I.

iii. Let I, J be two ideals in R. Prove the following.

(a) $I \subseteq (I \ : \ J)$.

(b) $J(I \ : \ J) \subseteq I$.

(c) if $I = I_1 \cap I_2$, then $(I \ : \ J) = (I_1 \ : \ J) \cap (I_2 \ : \ J)$.

(d) if $J = J_1 + J_2$, then $(I \ : \ J) = (I \ : \ J_1) \cap (I \ : \ J_2)$.

Exercise 1.16. Use the Chinese remainder theorem with $R = \mathbb{Q}[x],\ I = (x^3 - 8)R$ and $J = (x^2 + 1)R$, and find a polynomial $f \in R$ such that $f \equiv x \bmod I$ and $f \equiv (x + 1) \bmod J$.

Exercise 1.17. Let $f = 2x^3 + 3x^2 + 5x + a \in \mathbb{Z}/7[x]$.

i. Find all $a \in \mathbb{Z}/7$ such that f is irreducible.

ii. Let $a = 1$.

(a) Prove that the principal ideal $I = f\mathbb{Z}/7[x]$ is maximal. Let $\pi : \mathbb{Z}/7[x] \longrightarrow (\mathbb{Z}/7[x])/I$ be the projection map.

(b) Prove that $\pi(g) \neq 0$, for $g = 3x^2 + 4x + 5 \in \mathbb{Z}/7[x]$.

(c) Find $\big(\pi(g)\big)^{-1}$ in $(\mathbb{Z}/7[x])/I$.

Exercise 1.18. Let R be a commutative ring.

i. Prove that $\mathrm{Nil}(R)$ and $\mathrm{Rad}(R)$ are ideals of R and that $\mathrm{Nil}(R) \subseteq \mathrm{Rad}(R)$.

ii. Prove that if $I \in \mathrm{Spec}(R)$, then $\sqrt{I} = I$.

iii. Find a commutative ring R and a radical ideal $I = \sqrt{I}$ such that $I \notin \mathrm{Spec}(R)$. (Hint: consider $\mathbb{Z}$ and an ideal $n\mathbb{Z}$ with n a product of distinct primes.)

iv. Prove that $\mathrm{Nil}(R/\mathrm{Nil}(R)) = \{0\}$.

Exercise 1.19. Let p be a prime number. Prove that the saturated ideals of $\mathbb{Z}$ with respect to $\mathbb{Z} \setminus (p)$ are those generated by the powers of p, i.e. of the form $(p^n) = p^n\mathbb{Z}$ for some $n \in \mathbb{N}$. (Note that there is a unique prime ideal of $\mathbb{Z}$ which does not meet $\mathbb{Z} \setminus (p)$, and that $\mathbb{Z}_{(p)}$ has a unique nonzero prime - hence maximal - ideal.)

Exercise 1.20. Let k be a field, let $R = k[x, y]$ and let $\lambda \in k$. Consider the ideal $I = (x - \lambda y)$ of R.

i. Prove that the quotient ring R/I is isomorphic to $k[y]$.

ii. Deduce from the above that the ideal $I = (x - \lambda y)$ is prime.

2 Modules

Definition 2.1. Let R be a ring (not necessarily commutative). A *left R-module* is an abelian group $M = (M, +)$ together with an action $\rho : R \times M \to M$ of R, written $\rho(a, x) = ax$ subject to the following axioms:

- $a(x + y) = ax + ay$ for all $a \in R$ and all $x, y \in M$;
- $(a + b)x = ax + bx$ for all $a, b \in R$ and all $x \in M$;
- $(ab)x = a(bx)$ for all $a, b \in R$ and all $x \in M$;
- $1x = x$ for all $x \in M$.

There is an analogue notion of right R-modules, and the results are exactly the same. Since we only consider left R-modules, we will henceforth drop the word *left*, and call them simply R-modules.

An *R-submodule* of M is an abelian subgroup N of M such that $ax \in N$ for all $a \in R$ and all $x \in N$. If N is an R-submodule of M, the *quotient R-module* is the quotient abelian group M/N with the induced R-action: $a(x + N) = ax + N$ for all $a \in R$ and all $x + N \in M/N$.

The *zero submodule* of an R-module is the trivial subgroup $\{0\}$, which we write 0 if there is no confusion. An R-module is *simple* if it has no proper nonzero submodules.

The *regular representation* of R is the R-module R with the action of R given by the left multiplication in R.

From the definition, we see that $0x = 0$ for all $x \in M$ (or pedandically, $0_R x = 0_M$).

Example 2.2.

i. $\mathbb{Z}$-modules are precisely the abelian groups. Hence any R-module is a $\mathbb{Z}$-module, for any ring R.

ii. If R is a field, $\mathbb{R}$-modules are precisely the R-vector spaces.

iii. 0 and R are R-modules for any ring R. More generally, if I is a two-sided ideal of R, then I and R/I are R-modules for the action induced by left multiplication by R.

iv. If G is a group and R a commutative ring, the modules over the group algebra $A = RG$ are the *representations* of G over R.

v. If I is an ideal of R and M an R-module, then the set $IM = \{\sum_{j=1}^{n} a_j x_j \mid a_j \in I,\ x_j \in M\}$ is an R-submodule of M.

Let M be an R-module. Regarding M as a $\mathbb{Z}$-module, the torsion subgroup $M_{\mathbb{Z}-tor}$ of M is the subgroup of M formed by the elements of finite order. Note that $M_{\mathbb{Z}-tor}$ is an R-module, but not to be confused with the following.

Definition 2.3. Let R be a commutative ring and let M be an R-module. The *torsion submodule* M_{tor} (or M_{R-tor}) of M is the subset.

$$M_{tor} = \{x \in M \mid \exists\ a \in R,\ a \text{ is not a zero divisor and such that } ax = 0\}.$$

Note that M_{tor} is an R-submodule of M.

We say that M is *torsion* if $M = M_{tor}$, and that M is *torsionfree* if $M_{tor} = 0$.

If R is not commutative, M_{tor} is not an R-module in general. Torsion submodules occur for instance in the description of finitely generated modules over a PID, see [Lan, Theorem III.7.3].

Definition 2.4. Let R be a ring and let M, N be R-modules. An *R-module homomorphism*, or simply an R-homomorphism from M to N is a group homomorphism $\varphi : M \to N$ such that $\varphi(am) = a\varphi(m)$ for all $a \in R$ and all $m \in M$. We say that φ is injective/surjective or an isomorphism, if it it also injective/surjective or an isomorphism as a group homomorphism, respectively. We write $M \cong N$ if φ is an R-isomorphism. If $M = N$, we call φ an *R-endomorphism* of M, or an *automorphism* if φ is a bijective endomorphism. We write $\mathrm{Hom}_R(M, N)$ for the set of R-homomorphisms $M \to N$, and similarly $\mathrm{Iso}_R(M, N)$ for the R-isomorphisms, $\mathrm{End}_R M$ for the R-endomorphisms and $\mathrm{Aut}_R M$ for the R-automorphisms of M.

Here are a few immediate observations.

- If $R = \mathbb{Z}$, then R-homomorphisms are precisely group homomorphisms.
- The sets $\mathrm{Hom}_R(M, N)$ are abelian groups for the pointwise addition of maps $(f + g)(x) = f(x) + g(x)$ for all $f, g \in \mathrm{Hom}_R(M, N)$ and all $x \in M$.
- The set $\mathrm{End}_R M$ is a ring (noncommutative in general) where the multiplication is the composition of maps $(fg)(x) = f(g(x))$.
- If R is commutative, then $\mathrm{Hom}_R(M, N)$ is an R-module (cf. Exercises 2.3 below).
- An R-module M can equivalently be defined by a ring homomorphism $\rho : R \longrightarrow \mathrm{End}_{\mathbb{Z}} M$, where $\mathrm{End}_{\mathbb{Z}} M$ is the set of group endomorphisms $M \to M$. Indeed, Definition 2.1 above states that the R-module structure of M is an endomorphism of the abelian group M, and the correspondence $a \mapsto \rho(a)$, where $\big(\rho(a)\big)(x) = ax$ for all $x \in M$, is a ring homomorphism since $\rho(a + b) = \rho(a) + \rho(b)$ by the second axiom, and $\rho(ab) = \rho(a)\rho(b)$ by the third axiom, where the right hand side multiplication is the composition of maps in $\mathrm{End}_{\mathbb{Z}} M$.

This last remark leads to the notion of a faithful module.

Definition 2.5. An R-module M is faithful if $\rho : R \to \mathrm{End}_{\mathbb{Z}} M$ is injective, that is, if

$$\ker\big(\rho : R \to \mathrm{End}_{\mathbb{Z}} M\big) = 0.$$

In other words, an R-module M is faithful if and only if the only element $a \in R$ such that $ax = 0$ for all $x \in M$ is $a = 0$.

Example 2.6. If k is a field and V an n-dimensional k-vector space ($n \geq 1$), then $\mathrm{End}_k V$ is isomorphic to the ring $M_n(k)$ of $n \times n$ matrices with coefficients in R, and $\mathrm{Aut}_k V \cong \mathrm{GL}_n(k)$, the unit group of $M_n(k)$. Moreover, V is faithful.

2.1 New modules from old

As seen above, hom-sets of R-modules are R-modules themselves. In a first course on linear algebra, there are some standard constructions which produce new modules from old. Many of these constructions apply to R-modules, for a commutative ring R.

Definition 2.7. Let R be a commutative ring and let M be an R-module. The *(R-)dual of M* is the R-module $M^* = \mathrm{Hom}_R(M, R)$. Thus M^* is an R-module for the R-action: $(af)(x) = af(x)$, for all $a \in R, f \in M^*$ and $x \in M$.

Recall that, given a group homomorphism $\varphi : M \to N$, the set $\ker(\varphi)$ is a normal subgroup of M. In fact any normal subgroup of M and any quotient of M can be expressed by a homomorphism, as $\ker(\varphi)$ and $M/\ker(\varphi)$, respectively.

Definition 2.8. Let R be a ring and let N be an R-submodule of an R-module M. The *quotient* of M by N is the quotient group M/N with induced R-module structure: $a(x+N) = ax + N$, for all $a \in R$ and all $x + N \in M/N$.

If M is an R-module and I is an ideal of R, then the quotient module M/IM is an R/I-module: Since $a(x + IM) = IM$ for all $a \in I$ and all $x + IM \in M/IM$, there is a well-defined R/I-action on M/IM, given by $(a + I)(x + IM) = (ax + IM)$.

We can use R-homomorphisms to obtain new modules.

Proposition 2.9. *Let R be a ring and let $\varphi \in \mathrm{Hom}_R(M, N)$, for some R-modules M and N. Then $\ker(\varphi)$ is an R-submodule of M and $\mathrm{im}(\varphi)$ is an R-submodule of N.*

To summarise, given any R-homomorphism $\varphi : M \to N$, we construct four new modules: $\ker(\varphi)$, $\mathrm{im}(\varphi)$, $M/\ker(\varphi)$ and $N/\mathrm{im}(\varphi)$. The quotient module $N/\mathrm{im}(\varphi)$ is the *cokernel* of φ.

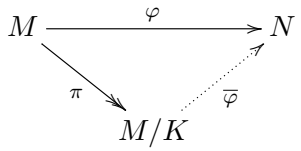
Proof. Let us prove that $\ker(\varphi)$ is an R-submodule of M. We already know that it is a subgroup of M. Pick any $x \in \ker(\varphi)$ and any $a \in R$. Then $\varphi(ax) = a\varphi(x) = a0 = 0$. So $ax \in \ker(\varphi)$, for all $a \in R$ and all $x \in \ker(\varphi)$. Therefore, $\ker(\varphi)$ is a subgroup of M which is closed under the action of R, as was to be shown.

We know that $\mathrm{im}(\varphi)$ is a subgroup of N. To show that it is an R-submodule, let $y \in \mathrm{im}(\varphi)$ and let $a \in R$. For any $x \in \varphi^{-1}(y)$, we have $ay = a\varphi(x) = \varphi(ax) \in \mathrm{im}(\varphi)$. This holds for all $a \in R$ and all $y \in \mathrm{im}(\varphi)$, as required. □

The above leads us to state the first isomorphism theorem for R-modules. (We leave its proof as an exercise, immediate from the above and the first isomorphism theorem for groups.)

Theorem 2.10. *Let R be a ring and let $\varphi : M \to N$ be an R-homomorphism. Then φ induces an R-isomorphism $\overline{\varphi} : M/\ker(\varphi) \to \mathrm{im}(\varphi)$.*

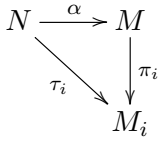
More generally, φ *factors through* M/K for any R-submodule K of $\ker(\varphi)$. Here *factors through* means that there exists an R-homomorphism $\overline{\varphi} : M/K \to N$ such that the following diagram *commutes*, i.e. $\overline{\varphi}\pi = \varphi$:



Now assume that we are given collections of modules. Then we construct new modules as follows.

Definition 2.11. Let R be a ring and let $\{M_i,\ i \in I\}$ be a collection of R-modules.

i. The *product* of $\{M_i,\ i \in I\}$ is a set $\{M, \pi_i,\ i \in I\}$, where M is an R-module and π_i are surjective R-homomorphisms, called *projections*, $\pi_i : M \twoheadrightarrow M_i$ for all $i \in I$, satisfying the following universal property: Whenever there exists an R-module N with R-homomorphisms $\tau_i : N \to M_i$ for all $i \in I$, then there *exists* a *unique* R-homomorphism $\alpha : N \to M$ such that the diagrams



commute for all $i \in I$.

We generally write $\prod_{i \in I} M_i$ instead of $\{M, \pi_i,\ i \in I\}$ and call it the *direct product* of $\{M_i,\ i \in I\}$.

ii. The *coproduct* of $\{M_i,\ i \in I\}$ is a set $\{M, \iota_i,\ i \in I\}$, where M is an R-module and ι_i are injective R-homomorphisms, called *inclusions* $\iota_i : M_i \hookrightarrow M$ for all $i \in I$, satisfying the following universal property: Whenever there exists an R-module N with R-homomorphisms $\sigma_i : M_i \to N$ for all $i \in I$, then there *exists* a *unique* R-homomorphism $\beta : M \to N$ such that the diagrams

$$\begin{array}{ccc} M_i & \xrightarrow{\iota_i} & M \\ & \searrow^{\sigma_i} & \downarrow \beta \\ & & N \end{array} \quad \text{commute for all } i \in I.$$

We generally write $\bigoplus_{i \in I} M_i$ instead of $\{M, \iota_i,\ i \in I\}$ and call it the *direct sum* of $\{M_i,\ i \in I\}$.

In practical terms, the product of $\{M_i,\ i \in I\}$ is isomorphic to the set of all sequences $(x_i)_{i \in I}$ with the structure of abelian group coordinatewise, i.e. $(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I}$, and similarly for the structure of R-module: $a(x_i)_{i \in I} = (ax_i)_{i \in I}$. If $I = \{1, \ldots, n\}$ is finite, then we write $M_1 \times \cdots \times M_n$.

The direct sum $\bigoplus_{i \in I} M_i$ is isomorphic to the R-submodule of $\prod_{i \in I} M_i$ formed by all the sequences with finitely many nonzero coordinates. In particular, $\bigoplus_{i \in I} M_i \cong \prod_{i \in I} M_i$ whenever I is finite. We refer to [Jac, Section 1.5, Vol. II] for more background on these categorical notions.

Before moving on to new constructions, let us consider the hom-sets of direct products and sums of R-modules.

Proposition 2.12. *Let $\{M_i,\ i \in I\}$ be a collection of R-modules and let N be an R-module. There are isomorphisms of R-modules:*

$$\mathrm{Hom}_R(\textstyle\bigoplus_{i \in I} M_i, N) \xrightarrow{\mu} \prod_{i \in I} \mathrm{Hom}_R(M_i, N) \quad \textit{and}$$
$$\mathrm{Hom}_R(N, \textstyle\prod_{i \in I} M_i) \xrightarrow{\nu} \prod_{i \in I} \mathrm{Hom}_R(N, M_i)\ .$$

Proof. Given $\varphi \in \mathrm{Hom}_R(\bigoplus_{i \in I} M_i, N)$, let $\varphi_i = \varphi|_{M_i}$ be the restriction of φ to M_i, for all i, that is, $\varphi_i = \varphi\iota_i : M_i \to N$. The function defined by $\mu(\varphi) = (\varphi_i)_{i \in I}$ is an R-isomorphism. Indeed, by definition, it is a well defined R-module homomorphism, and μ^{-1} is the R-homomorphism sending $\psi = (\psi_i)_{i \in I} \in \prod_{i \in I} \mathrm{Hom}_R(M_i, N)$ to $\psi|_{\bigoplus_{i \in I} M_i}$, the restriction of ψ to the elements of $\bigoplus_{i \in I} M_i \hookrightarrow \sum_{i \in I} M_i$.

The proof for the second statement is similar and left in exercise.

□

2.2 Tensor product of R-modules

In a similar way as we have defined direct product and direct sum of modules, we now construct the tensor product of R-modules. We refer to [Lan, Chapter XVI] for more details. The notion of bilinearity should be already known from linear algebra.

Definition 2.13. Let L, M, N be R-modules and let $f : L \times M \to N$ be a function, where $L \times M$ is the direct product. We say that f is *R-bilinear* if f is R-linear in each variable, i.e. if the restrictions

$$f_{L,y} : L \to N, \quad f_{L,y}(x) = f(x,y) \quad \text{and} \quad f|_{x,M} : M \to N, \quad f|_{x,M}(x,y) = f(x,y)$$

are R-homomorphisms for all $x \in L,\ y \in M$.

Explicitly, for all $x, x' \in L$, all $y, y' \in M$ and all $a \in R$,

$$f(x + x', y) = f(x,y) + f(x',y) \quad f(x, y + y') = f(x,y) + f(x,y') \quad f(ax, y) = af(x,y) = f(x, ay).$$

For instance, for any R-module M, let $M = L^* = \mathrm{Hom}_R(L, R)$ be its R-dual and let $N = R$. The function $t : M^* \times M \to R$, often called *trace map*, defined by $t(\varphi, x) = \varphi(x)$ is an R-bilinear map. Recall that the R-action on M^* is as follows: for $a \in R$ and $\varphi \in M^*$, then $a\varphi$ is the R-homomorphism defined by $(a\varphi)(x) = a\varphi(x)$ for all $x \in M$.

We use bilinear maps to construct the *tensor product* of two R-modules.

Definition 2.14. Let M, N be R-modules. The *tensor product (over R)* of M and N is the R-module $M \otimes_R N$ satisfying the following two conditions:

i. There exists an R-bilinear map $h : M \times N \to M \otimes_R N$.

ii. For all R-modules L and all R-bilinear maps $f : M \times N \to L$, there *exists* a *unique* R-homomorphism $\tilde{f} : M \otimes_R N \to L$ such that $\tilde{f}h = f$, i.e. such that the diagram

$$\begin{array}{ccc} M \times N & \xrightarrow{\quad h \quad} & M \otimes_R N \\ & {\scriptstyle f} \searrow \quad \swarrow {\scriptstyle \tilde{f}} & \\ & L & \end{array} \qquad \text{commutes.}$$

In other words, every R-bilinear map $M \times N \to L$ factors through the R-module $M \otimes_R N$.

We prove that the tensor product of R-modules exists and is unique (up to isomorphism) constructively. Let J be the R-submodule of $M \times N$ generated by all the elements of one of the following forms:

- $(x + x', y) - (x, y) - (x', y)$
- $(x, y + y') - (x, y) - (x, y')$
- $(ax, y) - (x, ay)$, for xll $x \in M,\ y \in N$ and all $a \in R$.

Define

$$M \otimes_R N = (M \times N)/J, \quad \text{and denote } x \otimes y \text{ the class of } (x, y) \text{ in the quotient } (M \times N)/J.$$

The commutative ring R acts on $M \otimes_R N$ by $a(x \otimes y) = ax \otimes y = x \otimes ay$. The R-bilinear map h in Definition 2.14 is the quotient map $M \times N \to M \otimes_R N$.

Observe that the R-action on the direct product $L \times M$ is diagonal, $a(x, y) = (ax, ay)$, not similar to the R-action on $L \otimes_R M$!

Example 2.15. i. Let L, M, N be R-modules, where R is a commutative ring. Using the universal properties of the tensor product, we obtain the R-isomorphisms (details of the proof of the claims in exercise):

- $M \otimes_R R \cong M \cong R \otimes_R M$. In particular, $R \otimes_R R \cong R$.
- $M \otimes_R N \cong N \otimes_R M$.
- $(M \oplus N) \otimes_R L \cong (M \otimes_R L) \oplus (N \otimes_R L)$.
- $(M \otimes_R N) \otimes_R L \cong M \otimes_R (N \otimes_R L)$.
- (Adjunction, cf. [Jac, Section 1.8, Vol I]) $\mathrm{Hom}_R(M \otimes_R N, L) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, L))$.

ii. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n = 0 = \mathbb{Z}[\frac{1}{n}] \otimes \mathbb{Z}/n$ for any $n \geq 1$. More generally, if A is a torsion abelian group such that the orders of the elements are invertible in the abelian group B, then $A \otimes_{\mathbb{Z}} B = 0$. Indeed, if A has n torsion and n is invertible in B, then $1 \otimes 1 = 1 \otimes n\frac{1}{n} = n \otimes \frac{1}{n} = 0 \otimes \frac{1}{n} = 0$.

iii. $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Z}/m \cong \mathbb{Z}/\gcd(m,n)$. Indeed, let $d = \gcd(m,n)$. By the first example, it suffices to show that $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Z}/m \cong \mathbb{Z}/d \otimes_{\mathbb{Z}} \mathbb{Z}$. Note that $(x+n\mathbb{Z}) \otimes (y+m\mathbb{Z}) = (xy+n\mathbb{Z}) \otimes (1+m\mathbb{Z}) = (1+n\mathbb{Z}) \otimes (xy+m\mathbb{Z})$ by definition of $\otimes_{\mathbb{Z}}$. Define the function $f : (x+n\mathbb{Z}) \otimes (y+m\mathbb{Z}) \mapsto (xy+d\mathbb{Z})$, extended $\mathbb{Z}$-linearly to all of $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Z}/m$. Note that f is well-defined since independent of the choice of the representative in $(x+n\mathbb{Z}) \otimes (y+m\mathbb{Z})$. Hence f is a group homomorphism. We check that f is bijective:

- For the injectivity, note that $xy + d\mathbb{Z} = d\mathbb{Z}$ if and only if $d \mid xy$, i.e. if and only if xy is divisible by both m and n, in which case $(x+n\mathbb{Z}) \otimes (y+m\mathbb{Z}) = 0 \in \mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Z}/m$.
- For the surjectivity, notes that $(x+d\mathbb{Z}) = f((x+n\mathbb{Z}) \otimes (1+m\mathbb{Z}))$.

Let M be an R-module and consider the operation

$$(M \otimes_R -) : R\text{–mod} \longrightarrow \text{ R –mod}, \quad \text{N} \longmapsto \text{M} \otimes_{\text{R}} \text{N},$$

where $R-$mod denotes the *category* of R-modules, whose *objects* are the R-modules and whose *morphisms* are the R-homomorphisms. This operation is an example of a *functor* from the category of R-modules to itself. That is,

- $(M \otimes_R -)$ maps R-modules (= the *objects* of $R-$mod) to R-modules.
- For any R-homomorphism $f : N \to N'$, the mapping $(M \otimes_R -)$ induces an R-homomorphism $f_* : M \otimes_R N \to M \otimes_R N'$, defined by $f_*(x \otimes y) = x \otimes f(y)$, for all $x \in M,\ y \in N$. Moreover, $(\mathrm{Id}_N)_* = \mathrm{Id}_{M \otimes_R N}$, and if $g \in \mathrm{Hom}_R(N', N'')$, then $g_* f_* = (gf)_* \in \mathrm{Hom}_R(M \otimes_R N, M \otimes_R N'')$.

Proposition 2.16. *Let M be an R-module, and let $f \in \mathrm{Hom}_R(N, N')$. If f is surjective, then $f_* \in \mathrm{Hom}_R(M \otimes_R N, M \otimes_R N')$ is surjective. In other words, if $0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ is an exact sequence of R-modules (cf. Section 2.4 below), then the induced sequence*

$$M \otimes_R A \xrightarrow{f_*} M \otimes_R B \longrightarrow 0 \qquad \textit{is exact.}$$

That is, the functor $(M \otimes_R -)$ preserves surjections, but not injections. We say that $(M \otimes_R -)$ is a *right exact functor*. To see that it does not preserve injectivity, let $f : \mathbb{Z} \to \mathbb{Q}$ be the inclusion and let $M = \mathbb{Z}/n$ for some $n \in \mathbb{N}$. Then $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n \cong \mathbb{Z}/n$ and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n = 0$, giving $f_* : \mathbb{Z}/n \to 0$, the zero map (see Example 2.15).

Proof. We can represent the statement in the following commutative diagram where the top row is exact:

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \longrightarrow & 0 \\ {\scriptstyle M\otimes_R -}\downarrow & & \downarrow{\scriptstyle M\otimes_R -} & & \\ M \otimes_R A & \xrightarrow{f_*} & M \otimes_R B & & \end{array}$$

We want to show that f_* is surjective. Pick any element of the form $x \otimes y \in M \otimes_R B$. Since f is surjective, $f^{-1}(y) \neq \emptyset$. Let $z \in f^{-1}(y) \subseteq A$. We calculate $f_*(x \otimes z) = x \otimes f(z) = x \otimes y$, which proves that $x \otimes y \in \mathrm{im}(f_*)$. Consequently, by linearity of f_*, any element $\sum_i x_i \otimes y_i \in M \otimes_R B$ is in the image of f', as required. □

Definition 2.17. An R-module M is *flat* if $M \otimes_R -$ preserves injective R-homomorphisms. Hence, M is flat if the functor $M \otimes_R -$ maps a short exact sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ to a short exact sequence $0 \longrightarrow M \otimes_R A \xrightarrow{f_*} M \otimes_R B \xrightarrow{g_*} M \otimes_R C \longrightarrow 0$.

2.3 Finitely generated modules

An R-module M is *finitely generated* if there exists a finite subset $X \subseteq M$ such that every element of M can be expressed as an R-linear combination of elements of X. If $\{x_i, \ldots, x_n\}$ generate M, we write $M = \langle x_1, \ldots, x_n \rangle$. We say that M is *cyclic* if $M = Rx$ if generated by a single element. In this case, Proposition 2.21 shows that $M \cong R/I$ for some ideal I of R. A well-known result states that every finitely generated abelian group is isomorphic to a direct sum of cyclic groups $\mathbb{Z}^n \oplus \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_m$, where $d_1, \ldots, d_m \in \mathbb{N}$ are such that d_i divides d_{i+1} for all i. Hence, any finitely generated abelian group is a quotient of a free abelian group. This result is a special case of finitely generated modules over PIDs. We refer to [Jac, Section 3.8, Vol I] and [Lan, Section III.7].

Definition 2.18. Let R be a ring. A *free R-module* is an R-module F such that there exists a subset $X \subseteq F$ with the property that every function $f : X \to M$ to an R-module M extends uniquely to an R-homomorphism $\tilde{f} : F \to M$. That is, $\tilde{f}$ is an R-homomorphism such that $\tilde{f}(x) = f(x)$ for all $x \in X$. We call X a *basis* of F (see Remark 2.20). F is *finitely generated* if X is a finite set, in which case the cardinality $|X|$ of X is the *rank* of F.

Diagrammatically, it means that given any diagram

$$\begin{array}{ccc} X & \xhookrightarrow{incl} & F \\ {\scriptstyle f}\downarrow & & \\ M & & \end{array} \quad \text{there exists a unique } \tilde{f} \text{ such that} \quad \begin{array}{ccc} X & \xhookrightarrow{incl} & F \\ {\scriptstyle f}\downarrow & \swarrow_{\tilde{f}} & \\ M & & \end{array} \quad \text{commutes.}$$

If F is a finitely generated free R-module, then it is a routine exercise to show that F is isomorphic to a direct sum of copies of the regular module,

$$F \cong \bigoplus_{x \in X} R_x, \quad \text{with } R_x \cong R \text{ for all } x \in X$$

via the extension to F of the function $f : X \to \bigoplus_{x \in X} R_x$ sending $y \in X$ to $(0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 is in the y-th coordinate. The regular R-module R (with the left multiplication by the elements in the ring R) is a free module of rank 1, and every rank one R-module is isomorphic to it. We should show that the rank of a finitely generated free R-module is well-defined for a commutative ring R, and therefore the cardinality of a basis of such module is an invariant. We leave this as a routine exercise, referring to the detailed discussion in [Jac, Section 3.4, Vol I], which also includes a paragraph on finitely generated free modules over rings that are not commutative. The arguments are very similar to the case of finite dimensional vector spaces.

Explicitly, if X is a basis of F, and $f : X \to M$ is a function to an R-module M, then:

- Every element of F *can* be written in a *unique* way as an R-linear combination $\sum_x a_x x$, and
- $\tilde{f}(\sum_x a_x x) = \sum_x a_x f(x)$ in M.

It follows that every finitely generated free R-module is isomorphic to a direct sum of finitely many copies of the regular module R.

Example 2.19. If k is a field, then every k-module is free. Finite dimensional vector spaces are precisely the finitely generated k-modules, and their rank is their dimension.

Remark 2.20. There is a contentious question: *Is the zero module free?* Some conventions declare it to be free, whilst others not. If one assumes the zero module to be free (for any ring), then it means that we allow the empty set to be a basis. If instead we use the universal property of free modules Definition 2.18, then (allowing a basis to be empty), the zero module is free on the empty set, since

the property vacuously holds. We leave these disagreements aside to focus on (in our opinion) more interesting questions and nonzero modules. One property that we bear in mind, and that we show in Lemma 2.24, is that every free module is projective. Since the zero module is projective, we implicitly assume that it is free too.

Proposition 2.21. *Let R be a commutative ring.*

i. Every finitely generated R-module is a quotient of a finitely generated free R-module.

ii. Let M be a finitely generated R-module and let I be an ideal of R. Let $\varphi \in \operatorname{End}_R M$ such that $\operatorname{im}(\varphi) \subseteq IM$. Then φ satisfies an equation of the form $\varphi^n + a_1\varphi^{n-1} + \cdots + a_n = 0$, with $a_i \in I$ for all i.

Note that the result does not concern uniqueness. For instance, by the Chinese remainder theorem, we have $R/(I_1 \cap \cdots \cap I_n) \cong \bigoplus_{i=1}^n R/I_i$, where we have the quotient of a free R-module of rank 1 on the left hand side, and on the right it is the quotient of a free R-module of rank n. Thus, an R-endomorphism may satisfy unrelated equations.

Proof of Proposition 2.21.

i. Let $X = \{x_1, \ldots, x_n\} \subseteq M$ be a generating set for M. Define the function

$$f \ : \ R^n \longrightarrow M, \quad f(a_1, \ldots, a_n) = \sum_{i=1}^n a_i x_i.$$

Then f is a surjective R-homomorphism. Hence, by Theorem 2.10, $M \cong R^n/\ker(f)$ as R-modules.

ii. Pick a set of generators $\{x_1, \ldots, x_n\}$ of M. Then $\varphi(x_i) \in IM$ for all i, and there exist elements $a_{ij} \in I$ such that $\varphi(x_i) = \sum_{j=1}^n a_{ij}x_j$, for all $1 \leq i, j \leq n$. Matrix-wise, these equations can be expressed in the form

$$\sum_{j=1}^n (\delta_{ij}\varphi - a_{ij})x_j = 0, \quad \text{where} \quad \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

Let $A = (\delta_{ij}\varphi - a_{ij}) \in M_n(R)$, and let $\operatorname{Adj}(A)$ denote its adjoint, i.e. the transpose of the cofactor matrix of A. Recall from linear algebra that $(\operatorname{Adj}(A))A = \det(A)I_n$. Hence the above equations give the matrix equation

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \operatorname{Adj}(A)A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \det(A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Expanding the determinant of A, gives the required equation.

□

Example 2.22. Let $R = k[x, y]$ where k is a field. Consider the maximal ideal $M = \langle x, y \rangle$ of R as an R-module. Then M is a finitely generated non-free R-module. Indeed, M is generated as R-module by 2 polynomials, x and y. Note that M is not cyclic, i.e. cannot be generated by a single polynomial, since that polynomial would need to divide both x and y in R. Thus, M has rank 2, since $\{x, y\}$ generates M as R-module. We claim that M is not free since

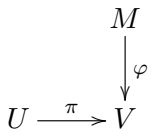
$$0 = 0x + 0y = (-y)x + (x)y.$$

That is, the R-homomorphism $\theta : R \oplus R \to M$, with $\theta(f, g) = fx + gy$ for all $f, g \in R$, yields $\ker(\theta) = (y, -x)(R \oplus R)$ and $M \cong (R \oplus R)/\ker(\theta) \ncong R^2$.

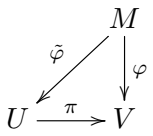
We now introduce two important classes of modules.

Definition 2.23. Let R be a ring, and let M be an R-module.

i. M is *projective* if given any diagram of R-modules and R-homomorphisms

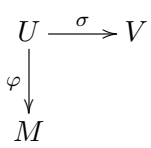


with π surjective, there exists an R-homomorphism $\tilde{\varphi}$ such that

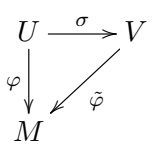


commutes.

ii. M is *injective* if given any diagram of R-modules and R-homomorphisms



with σ injective, there exists an R-homomorphism $\tilde{\varphi}$ such that



commutes.

For instance, if $R = \mathbb{Z}$, then $n\mathbb{Z}$ is projective for any $n \in \mathbb{N}$. Indeed, given any U, φ and π as above, we define $\tilde{\varphi}$ by picking any $x \in \pi^{-1}(\varphi(1))$ and set $\tilde{\varphi}(a) = ax$. It is an exercise to check that $\tilde{\varphi}$ is a group homomorphism, and thus a $\mathbb{Z}$-module homomorphism. Note however that $n\mathbb{Z}$ is not injective, by considering the inclusion $\mathbb{Z} \to \mathbb{Q}$, for instance. It is an exercise to prove that injective $\mathbb{Z}$-modules are precisely the divisible abelian groups (e.g. $\mathbb{Q}$ or $\mathbb{Q}/\mathbb{Z}$).

The following omnibus lemma states some well-known properties of projective modules. There are similar results for injective modules. We leave the proofs in exercise (see the proof of Theorem 2.28 below for an abridged partial proof).

Lemma 2.24. *Let R be a ring.*

i. Any free module is projective.

ii. Let M be an R module. TFAE:

(a) M is projective.

(b) Any short exact sequence (cf. Definition 2.30) $0 \longrightarrow U \xrightarrow{\phi} V \xrightarrow{\pi} M \longrightarrow 0$ splits, i.e. there exists $\psi \in \mathrm{Hom}_R(M, V)$ such that $\pi\psi = \mathrm{Id}_M$.

(c) Any surjective R-homomorphism $V \to M$ splits.

(d) M is a direct summand of a free R-module.

In other words, projective modules resemble free modules, but they are not free in general. We will see below that both notions coincide in some rings.

The Jacobson radical $\mathrm{Rad}(R)$ of a commutative ring R (cf. Definition 1.21) is the intersection of the maximal ideals of R, and it coincides with the set of noninvertible elements of R. Nakayama's lemma (named after the Japanese mathematician Tadashi Nakayama) is an important result in algebra, and it holds in arbitrary rings. Specialising to commutative rings (cf. [Jac, Section 7.8, Vol II] for the general version), we obtain the following.

Theorem 2.25 (Nakayama's lemma)**.** *Let R be a commutative ring and let M be a finitely generated R-module. Suppose that there exists an ideal $I \subseteq \mathrm{Rad}(R)$ such that $IM = M$. Then $M = \{0\}$.*

Proof. Suppose that M is nonzero, and pick a set of generators $X = \{x_1, \ldots, x_n\}$ of M with n minimal. By assumption $M = IM = \mathrm{Rad}(R)M$, saying that there exist $a_1, \ldots, a_n \in \mathrm{Rad}(R)$ such that $x_n = \sum_{i=1}^{n} a_i x_i \in IM$. Thus, $(1 - a_n)x_n = \sum_{i=1}^{n-1} a_i x_i$. By Proposition 1.25, since $a_n \in \mathrm{Rad}(R)$, we have $(1 - a_n) \in R^\times$. It follows that we can write $x_n = \sum_{i=1}^{n-1} (1 - a_n)^{-1} a_i x_i$, which contradicts the minimality of the size of the generating set X. □

Nakayama's lemma has the following two applications.

Corollary 2.26. *Let R be a commutative ring and let M be a finitely generated R-module. Let I be an ideal of R contained in $\mathrm{Rad}(R)$, and let N be a submodule of M. If $M = IM + N$, then $M = N$.*

Proof. We want to show that $I(M/N) = M/N$, and the result follows from Nakayama's lemma applied to the quotient module M/N. By definition, $I(M/N) = \{\sum_i a_i x_i + N \mid a_i \in I,\ x_i \in M,\ \forall\, i\} \subseteq M/N$ (finite sums), and by assumption, we have $M = IM + N$. Therefore, $I(M/N) = M/N$. □

Corollary 2.27. *Let R be a commutative local ring with maximal ideal $J = \mathrm{Rad}(R)$ and residue field $k = R/J$. Let M be a finitely generated R-module and let $x_1, \ldots, x_n \in M$. Denote with an overbar $\overline{x}$ the elements in the quotient module M/JM. TFAE*

i. $x_1, \ldots, x_n$ generate M.

ii. $\overline{x_1}, \ldots, \overline{x_n}$ generate M/JM as a k-vector space.

In other words, $\mathrm{Rad}(R)M$ is the submodule of 'non-generators' of M.

Proof. Suppose that $x_1, \ldots, x_n$ generate M. Since the projection map $M \to M/JM$ is a surjective R-homomorphism, their images generate M/JM as R/J-module, i.e. as k-vector space.

Suppose that $\overline{x_1}, \ldots, \overline{x_n}$ generate M/JM as a k-vector space. Choose elements $\dot{x}_1, \ldots, \dot{x}_n \in M$ with $\dot{x}_i + JM = \overline{x_i}$ in M/JM for all i, and set $N = \langle \dot{x}_1, \ldots, \dot{x}_n \rangle$ to be the submodule of M generated by these elements. (We can choose $\dot{x}_i = x_i$ for all i.) Hence, $(N + JM)/M = M/JM$, giving $M = N + JM$. By Corollary 2.26, we conclude that $M = N$. □

Theorem 2.28. *Let R be a commutative local ring. Then finitely generated projective modules are free.*

Proof. Let M be a finitely generated projective R-module. Suppose that M is a quotient of R^n, where we pick n minimal. Since M is projective, there exists a commutative diagram of R-modules and R-homomorphisms

$$\begin{array}{ccc} & & M \\ & \overset{\theta}{\swarrow} & \downarrow{\scriptstyle \mathrm{Id}_M} \\ R^n & \xrightarrow{\pi} & M \end{array} \qquad \text{with } \theta\pi = \mathrm{Id}_M,$$

showing that M is a direct summand of R^n. Write $R^n = M \oplus N$ for some finitely generated (projective) R-module N. Let $J = \mathrm{Rad}(R)$ be the unique maximal ideal of R. Then

$$JR^n = JM \oplus JN \quad \text{with} \quad JM \subseteq M,\ JN \subseteq N.$$

It follows that $R^n/JR^n = (M + JR^n)/JR^n \oplus (N + JR^n)/JR^n$, as R/J-vector spaces.

Now, R^n/JR^n is an n-dimensional R/J-vector space, possessing two complementary subspaces $(M + JR^n)/JR^n$ and $(N + JR^n)/JR^n$. We obtain an R/J-basis $\{x_1, \ldots, x_n\}$ of R^n/JR^n as the (disjoint) union $\{x_1, \ldots, x_r\} \sqcup \{x_{r+1}, \ldots, x_n\}$ of R/J-bases of $(M + JR^n)/JR^n$ and $(N + JR^n)/JR^n$, respectively. By Corollary 2.27, if $y_i \in R$ is a preimage of x_i under the quotient map $R^n \to R^n/JR^n$ for all i, then $y_1, \ldots, y_n$ generate R^n as an R-module. It follows that $y_1, \ldots, y_r$ generate M as an R-module. Since M is a quotient of $R^n$and we assume n to be minimal, it must be that $r = n$, and $M \cong R^n$.

□

Remark 2.29. Nakayama's lemma applies also to noncommutative rings. In that case, the Jacobson radical is the intersection of the maximal left ideals. We refer to [Jac, Vol II, Sections 4.2 and 7.8]. (Depending on the conventions, we use right ideals instead of left ones.)

The study and applications of projective modules in various algebraically inspired research areas is widespread. We refer to the abundant literature on the subject, and to the recent book by Lombardi and Quitté on the subject [LQ] (also available on arXiv.org).

2.4 Exact sequences

Exact sequences are fundamental tools in pure mathematics.

Definition 2.30. Let R be a ring and let L, M, N be R-modules related to each other in a sequence

$$L \xrightarrow{\varphi} M \xrightarrow{\psi} N \quad \text{of } R\text{-homomorphisms.}$$

We call the sequence *exact in* M if $\ker(\psi) = \mathrm{im}(\varphi)$.

More generally, a sequence

$$\ldots \longrightarrow M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \xrightarrow{\varphi_3} \ldots \tag{1}$$

is *exact* if $\ker(\varphi_{i+1}) = \mathrm{im}(\varphi_i)$ for all i.

We call an exact sequence *short* if it has the form

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0\ ,$$

and *long* if it has more nonzero terms.

Note that the sequence $0 \longrightarrow L \xrightarrow{\varphi} M$ is exact if and only if φ is injective, and $L \xrightarrow{\varphi} M \longrightarrow 0$ is exact if and only if φ is surjective.

For instance, if $R = k[x, y]$, then we have an exact sequence of the form:

$$0 \longrightarrow R \xrightarrow{\varphi} R \oplus R \xrightarrow{\psi} R \xrightarrow{\epsilon} k \longrightarrow 0\ ,$$

where $\varphi(f) = (fy, -fx)$, $\psi(f, g) = xf + yg$ and $\epsilon(f) = f(0, 0)$, the evaluation at $(x, y) = (0, 0)$.

An important question in homological algebra concerns the short exact sequences: how many modules M (up to isomorphism) and maps φ, ψ complete a sequence

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

into a short exact sequence? How do they 'differ'? For instance, consider $R = L = \mathbb{Z}$ and $N = \mathbb{Z}/n$ for some $n \in \mathbb{Z}$. Then we obtain short exact sequences

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n \longrightarrow 0 \quad \text{and}$$

$$0 \longrightarrow \mathbb{Z} \xrightarrow{i_1} \mathbb{Z} \oplus \mathbb{Z}/n \xrightarrow{\pi_2} \mathbb{Z}/n \longrightarrow 0$$

where $\cdot n$ is the multiplication by n map and the other morphisms are the obvious inclusion and projections. The two sequences are genuinely distinct: the first one is *not split* and the second *splits*. By definition, a sequence as in Equation (1) *splits* if there exist R-homomorphisms $\sigma_i : M_{i+1} \to M_i$ for all i such that the compositions $\varphi_i \sigma_i \varphi_i = \varphi_i$ for all i. We leave it as an exercise to prove that a short exact sequence of R-modules splits if and only if the middle module is isomorphic to the direct sum of the other two, and that more generally, a long exact sequence as above splits if and only if $M_i \cong \ker(\varphi_i) \oplus \mathrm{im}(\varphi_{i-1})$.

2.5 Extension of scalars

Let $f : R \to S$ be a ring homomorphism. We want to study the relationship between the representations of R and of S, i.e. between R-modules and S-modules. In this section, we present some aspects of what can be said in the case when R and S are commutative.

Lemma 2.31. *Let $f : R \to S$ be a ring homomorphism.*

i. Every S-module N is an R-module, for the action: $ax = f(a)x$ for all $a \in R$, $x \in N$. In particular, S is an R-module. This construction is called the restriction of scalars *from S to R along f, often written $\operatorname{res}_f M$, or $\operatorname{res}^S_R M$ if f is a ring inclusion.*

ii. Every R-module M gives rise to an S-module $S \otimes_R M$, where $b(a \otimes x) = (ba) \otimes x$ for all $a, b \in S$, $x \in M$. In particular, R gives rise to an S-module $S \otimes_R R$. This construction is called the extension of scalars *from R to S, often written $\operatorname{ind}_f M$, or $\operatorname{ind}^S_R M$ if f is a ring inclusion.*

The proof of Lemma 2.31 is left as a routine verification of the axioms of modules.

Remark 2.32. i. Let $f : R \to S$ be a ring homomorphism and let M be an R-module. In the tensor product $S \otimes_R M$, we regard S as an (S, R)-*bimodule*. That is, S is a left S-module for the left multiplication in S, and a right R-module via f, as above, such that left and right actions *commute*, i.e. $(ax)b = a(bx)$, for all $a, x \in S$ and all $b \in R$.

ii. Consider the inclusion $f : \mathbb{Z} \to \mathbb{Q}$. Then an abelian group A is turned into a $\mathbb{Q}$-vector space $\mathbb{Q} \otimes_{\mathbb{Z}} A$. If A is a torsion abelian group, then $\mathbb{Q} \otimes_{\mathbb{Z}} A$ is the zero vector space (counter-intuitive to the idea of 'extension').

In Section 2.6, we consider the case when $f : R \to R_U$ is the injective ring homomorphism defined by the localisation of R at U, cf. Theorem 1.30.

Beforehand, we prove some elementary properties of the extension of scalars.

Proposition 2.33. *Let $f : R \to S$ be a ring homomorphism.*

i. Let M be a finitely generated R-module. Then $S \otimes_R M$ is finitely generated as an S-module.

ii. Suppose that S is finitely generated as an R-module. Let N be a finitely generated S-module. Then $\operatorname{res}_f N$ is finitely generated as R-module.

Proof. i. Suppose that $x_1, \ldots, x_t$ generate M as an R-module. Then $\{1 \otimes x_i \mid 1 \leq i \leq t\}$ generate $S \otimes_R M$ as an S-module.

ii. Suppose that $a_1, \ldots, a_n$ generate S as an R-module, and that $x_1, \ldots, x_t$ generate N as an S-module. Then the set $\{a_i x_j \mid 1 \leq i \leq n,\ 1 \leq j \leq t\}$ generates N as an R-module.

□

2.6 Localisation of R-modules

Let R be a commutative ring and let U be a multiplicative set of R. In this section, we construct the localisation of R-modules, producing R_U-modules. The method is similar to that of the expansion of ideals with respect to the localisation R_U. Indeed, the localisation of an ideal M of R, i.e. an R-submodule of R, is its expansion M_U with respect to U.

Definition 2.34. Let R_U be the localisation of a commutative ring R with respect to a multiplicative set U of R, and let $\theta : R \to R_U$ be the canonical homomorphism. Let M be an R-module. The *localisation* of M with respect to U is the R_U-module

$$M_U = \{(x, s) \in M \times U\} / \sim$$

where $(x, s) \sim (y, t)$ if and only if there exists $u \in U$ with $u(tx - sy) = 0 \in M$.

As before, we write $\frac{x}{s}$, or possibly $[x, s]$, for the class of (x, s) in the quotient. Let $\frac{x}{s}, \frac{y}{t} \in M_U$, and let $\frac{a}{u} \in R_U$. We define

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st} \quad \text{and} \quad \frac{a}{u}\,\frac{x}{s} = \frac{ax}{us}.$$

It is routine to check that this defines a structure of R_U-module on the abelian group M_U, with $0_{M_U} = \frac{0}{1}$.

If N is an R-module and $f \in \mathrm{Hom}_R(M, N)$, then f induces an R_U-homomorphism

$$f_U : M_U \longrightarrow N_U, \quad f_U\big(\frac{x}{s}\big) = \frac{f(x)}{s}, \quad \text{for all } \tfrac{x}{s} \in M_U.$$

Proposition 2.35. *Let R_U be the localisation of a commutative ring R with respect to a multiplicative set U of R, and let $\theta : R \to R_U$ be the canonical homomorphism. Let M be an R-module.*

i. If M is finitely generated, then $M_U = 0$ if and only if there exists $s \in U$ which annihilates M, i.e. $sM = 0$. (For short, we write 0 instead of the zero module $\{0\}$.)

ii. Consider R_U as an R-module for the action $a\frac{b}{s} = \frac{ab}{s}$. Then $M_U \cong R_U \otimes_R M$ as an R_U-module. Moreover, if N is an R-module and $f \in \mathrm{Hom}_R(M, N)$, then the diagram

$$\begin{array}{ccc} M_U & \xrightarrow{\eta_M} & R_U \otimes_R M \\ {\scriptstyle f_U}\downarrow & & \downarrow{\scriptstyle \mathrm{Id}\otimes f} \\ N_U & \xrightarrow[\eta_N]{} & R_U \otimes_R N \end{array}$$

commutes, and η_M, η_N are R_U-isomorphisms. That is, the map $M_U \mapsto R_U \otimes_R M$ is natural *in M.*

Proof. i. Note that for any $s \in U$ and $x \in M$, we have $\frac{x}{1} = \frac{sx}{s} = s\frac{x}{s}$. So, if $sM = 0$ for some $s \in U$, then $\frac{x}{1} = 0$ in M_U for all $x \in M$, and it follows that $M_U = 0$. Conversely, suppose that M is generated by a finite set X and that $M_U = 0$. The equality $M_U = 0$ implies that $\frac{x}{1} = \frac{0}{1}$ for all $x \in X$. That is, for every $x \in X$, there is $s_x \in U$ such that $s_x x = 0$ in M. Let $s = \prod_{x\in X} s_x \in U$. Then $sM = 0$.

ii. Define

$$\eta : M_U \to R_U \otimes_R M, \quad \eta\big(\frac{x}{s}\big) = \frac{1}{s} \otimes x, \quad \text{for all } \tfrac{x}{s} \in M_U.$$

To prove that η is well defined, we need to show that if $\frac{x}{s} = \frac{y}{t}$ in M_U, then $\eta\big(\frac{x}{s}\big) = \eta\big(\frac{y}{t}\big)$. Let $u \in U$ be such that $u(tx - sy) = 0$, i.e. $tux = suy$. We calculate

$$\begin{aligned} \frac{1}{s} \otimes x = \frac{tu}{stu} \otimes x = \frac{1}{stu} tu \otimes x = \frac{1}{stu} \otimes tux \\ = \frac{1}{stu} \otimes suy = \frac{1}{stu} su \otimes y = \frac{1}{t} \otimes y, \quad \text{as required.} \end{aligned}$$

So η is well defined. A routine exercise shows that η is a group homomorphism.

Conversely, the function $\phi : R_U \times M \to M_U$ given by $\phi(\frac{a}{s}, x) = \frac{ax}{s}$ is R_U bilinear (check left as an exercise), and so it yields a group homomorphism $\phi_* : R_U \otimes_R M \to M_U$, with $\phi_*(\frac{a}{s} \otimes x) = \frac{ax}{s}$, for all $a \in R,\ s \in U$ and $x \in M$.

By construction, we note that the compositions $\phi_*\eta = \mathrm{Id}_{M_U}$ and $\eta\phi_* = \mathrm{Id}_{R_U \otimes_R M}$, which proves that they are inverse of each other and in particular they are group isomorphisms. Since η and ϕ_* are both R_U-linear, they are R_U-isomorphisms.

Finally, to check the commutativity of the diagram, a direct computation gives that

$$((\mathrm{Id}\otimes f)\eta_M)\big(\frac{x}{s}\big) = (\mathrm{Id}\otimes f)(\frac{1}{s} \otimes x) = \frac{1}{s} \otimes f(x) = \eta_N\big(\frac{f(x)}{s}\big) = (\eta_N f_U)\big(\frac{x}{s}\big),$$

for all $\frac{x}{s} \in M_U$, as required.

□

The localisation induces a functor $(-)_U : R\text{–mod} \longrightarrow \mathsf{R_U}\text{–mod}$, where $M \longmapsto M_U$, from the category of R-modules to the category of R_U-modules. That is,

- $(-)_U$ maps R-modules (= the *objects* of R –mod) to R_U-modules (= the *objects* of R_U –mod).
- For any R-homomorphism $f : M \to N$, the induced function $f_U : M_U \to N_U$ is an R_U-homomorphism such that $(\mathrm{Id}_M)_U = \mathrm{Id}_{(M_U)}$, and such that $g_U f_U = (gf)_U \in \mathrm{Hom}_R(M_U, L_U)$ for all $g \in \mathrm{Hom}_R(N, L)$.

Recall from Proposition 2.16 that the functor $(-)_U = (R_U \otimes_R -) : R\text{–mod} \to \mathsf{R_U}\text{–mod}$ is right exact, i.e. sends surjective R-homomorphisms to surjective R_U-homomorphisms. We now show that the localisation is in fact an *exact functor*, i.e. preserves both surjections and injections.

Proposition 2.36. *Let R_U be the localisation of a commutative ring R with respect to a multiplicative set U of R, and let $\theta : R \to R_U$ be the canonical homomorphism. Let M be an R-module.*

i. Let N, N' be R-modules and let $f \in \mathrm{Hom}_R(N, N')$. If f is injective, then $f_U \in \mathrm{Hom}_{R_U}(N_U, N'_U)$ is injective.

ii. If $A \xrightarrow{f} B \xrightarrow{g} C$ is an exact sequence of R-modules, then the induced sequence of R_U-modules $A_U \xrightarrow{f_U} B_U \xrightarrow{g_U} C_U$ is exact.

Proof. Similarly to the proof of Proposition 2.16, it suffices to prove the first part. Let $\frac{x}{s} \in \ker(f_U)$. That is, $\frac{0}{1} = \frac{f(x)}{s}$, which means that there exists $t \in U$ such that $0 = t(0s - 1f(x)) = tf(x) = f(tx)$ because f is an R-homomorphism. The injectivity of f implies that $0 = tx = t(s0 - 1x)$. Hence $\frac{x}{s} = \frac{0}{1}$ and f_U is injective.

□

Corollary 2.37. *Let R be a commutative ring, let M, N be R-modules and let $f : M \to N$ be an R-homomorphism. TFAE.*

i. f is injective.

ii. $f_P : M_P \to N_P$ is injective for all $P \in \mathrm{Spec}(R)$.

iii. $f_P : M_P \to N_P$ is injective for all $P \in \mathrm{MaxSpec}(R)$.

Similarly with surjective instead of injective.

Proof. Proposition 2.36 shows that i implies ii and iii. To show that iii implies i, let $M' = \ker(f)$. By Proposition 2.36, the sequence $0 \longrightarrow (M')_P \longrightarrow M_P \xrightarrow{f_P} N_P$ is exact for every $P \in \mathrm{MaxSpec}(R)$. For all $P \in \mathrm{MaxSpec}(R)$, we have $\ker(f)_P = \ker(f_P) = 0$ since f_P is injective by assumption. We claim that $\ker(f) = 0$. Indeed, suppose that there exists a nonzero element $x \in \ker(f)$, and let $I = \mathrm{Ann}(x) = \{a \in R \mid ax = 0\}$. Then I is a proper ideal of R since $1 \notin I$, and therefore I is contained in some maximal ideal P of R. Now, if $\frac{x}{1} \in \ker(f)_P$, then $\frac{x}{1} = \frac{0}{1}$ since $\ker(f)_P = 0$. That is, there exists $a \in R \setminus P$ such that $ax = 0$, contradicting the fact that $\mathrm{Ann}(x) \subseteq P$. It follows that f is injective.

□

2.7 Noetherian and Artinian modules

In this section, we introduce two important classes of modules satisfying certain *chain conditions*, and show some of their properties.

Definition 2.38. A *chain* is a totally ordered subset of a *poset*, i.e. a partially ordered set. We say that an (infinite) ascending chain $x_1 \leq x_2 \leq \dots$ *stabilises* if there exists an index $N \in \mathbb{N}$ such that $x_n = x_N$ for all $n \geq N$.

For instance, Let X be the poset of subsets of $\{1, \dots, 99\}$ where the order relation is the inclusion. Then, we have numerous chains, for instance the ascending chain $\emptyset \leq \{1\} \leq \{1,2\} \leq \{1,2,3\} \leq \cdots$ and the descending chain $\{1, \dots, 99\} \geq \{1\} \geq \emptyset$. All chains in X stabilise since $\{1, \dots, 99\}$ is finite.

Definition 2.39. Let M be an R-module. Consider the poset of submodules of M, where the order relation is given by the inclusion of submodules.

i. M is *Noetherian* if every ascending chain of submodules of M stabilises.

ii. M is *Artinian* if every descending chain of submodules of M stabilises.

Hence the ring R is Noetherian if R is Noetherian as an R-module, and R is Artinian if R is Artinian as an R-module.

Noetherian algebraic structures are named after the German mathematician Emmy Noether, and *Artinian* after the Austrian mathematician Emil Artin.

It is easy to see that a finite R-module is both Noetherian and Artinian, since any strictly ascending or descending chain has finite length. Note also that the direct sum of finitely many Noetherian (resp. Artinian) modules is Noetherian (resp. Artinian).

The condition of Noetherian and Artinian rings and modules do not require the ring to be commutative (cf. [Jac, Section 3.2, Vol II]).

Example 2.40. Let $R = \mathbb{Z}$ and consider $\mathbb{Z}$-modules, i.e. abelian groups.

i. An abelian group A is Noetherian if and only if A is finitely generated. Indeed, suppose that A is not finitely generated and pick an infinite set $\{a_i \in A \mid \ i \in \mathbb{N}\} \subseteq A$ such that $a_{i+1} \notin A_i = \langle a_1, \dots, a_i \rangle$ for all $i \in \mathbb{N}$. Then the chain $A_1 \leq A_2 \leq A_3 \leq \dots$ does not stabilise. Hence if A is Noetherian, then A is finitely generated. Conversely, suppose that A is finitely generated, i.e. isomorphic to $\mathbb{Z}^f \oplus \mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_t$. Since finite $\mathbb{Z}$-modules are Noetherian, $\mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_t$ is Noetherian. Moreover any nonzero submodule of $\mathbb{Z}$ has the form $k\mathbb{Z}$ for some $k \in \mathbb{N}$, and so any torsionfree cyclic submodule of $\mathbb{Z}$ has finite index in $\mathbb{Z}$. Since $f < \infty$, every ascending chain of submodules of A stabilises.

ii. An abelian group A is Artinian if and only if A is finite. The argument above shows that $\mathbb{Z}$ is not an Artinian $\mathbb{Z}$-module: for instance, $2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \cdots$ does not stabilise.

Proposition 2.41 is useful to determine whether an R-module M is Noetherian, Artinian, both or neither.

Proposition 2.41. *Let M be an R-module. Then:*

i. M is Noetherian if and only if any nonempty collection of submodules of M has a maximal element.

ii. M is Artinian if and only if any nonempty collection of submodules of M has a minimal element.

Proof. We only prove the statement for Noetherian modules; the proof of the statement about Artinian modules is proved in a similar fashion.

We need to show that M is Noetherian if and only if the poset X of submodules of M satisfies the conditions of Zorn's lemma. That is, every chain in X has an upper bound in X.

Suppose that M is Noetherian and let $M_1 \leq M_2 \leq \dots$ be an ascending chain in X. By hypothesis, there exists $N \in \mathbb{N}$ such that $M_n = M_N$ for all $n \geq N$. Hence such M_N is an upper bound of our chain.

By Zorn's lemma, X has a maximal element, proving that any nonempty collection of submodules of M has a maximal element.

Conversely, suppose that any nonempty collection of submodules of M has a maximal element. Let $M_1 \leq M_2 \leq \dots$ be an ascending chain of submodules of M, and set $X = \{M_i \mid i \in \mathbb{N}\}$. By assumption, X has a maximal element, say M_N. That is, since the M_i form a totally ordered set, $M_i \leq M_N$ for all $i \in \mathbb{N}$. So the chain $M_1 \leq M_2 \leq \dots$ must stabilise to this upper bound M_N. It follows that M is Noetherian. □

Noetherian and Artinian R-modules satisfy properties similar to those of soluble groups.

Theorem 2.42. *Let* $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ *be a short exact sequence of* R*-modules and* R*-homomorphisms.*

i. Then M *is Noetherian if and only if both* L *and* N *are Noetherian. In particular, submodules, quotient modules and finite direct sums of Noetherian* R*-modules are Noetherian.*

ii. Then M *is Artinian if and only if both* L *and* N *are Artinian. In particular, submodules, quotient modules and finite direct sums of Artinian* R*-modules are Artinian.*

Proof. We prove the statement for Noetherian modules only. The statement for Artinian modules is very similar.

Observe that the 'In particular' statement is immediate, given that, to every submodule L of M corresponds a quotient module M/L that fit in an exact sequence $0 \longrightarrow L \longrightarrow M \longrightarrow M/L \longrightarrow 0$. Moreover, such sequence splits if and only if $M \cong L \oplus M/L$ as R-modules.

$\boxed{\Rightarrow}$ Suppose that M is Noetherian.

Let $L_1 \subseteq L_2 \subseteq \dots$ be a chain of submodules of L. Since $L_i \cong f(L_i)$ by injectivity of f, we can identify this chain to the chain $f(L_1) \subseteq f(L_2) \subseteq \dots$ of submodules of M. Since M is Noetherian, this chain stabilises, i.e. there exists $k \in \mathbb{N}$ such that $f(L_n) = f(L_k)$ for all $n \geq k$. Hence for such k, we have $L_n = L_k$ for all $n \geq k$ too. It follows that L is Noetherian.

Let $N_1 \subseteq N_2 \subseteq \dots$ be a chain of submodules of N. Then $g^{-1}(N_1) \subseteq g^{-1}(N_2) \subseteq \dots$ is a chain of submodules of M. Since M is Noetherian, this chain stabilises. Note that $N_i = g\big(g^{-1}(N_i)\big)$ for all i. Therefore $N_1 \subseteq N_2 \subseteq \dots$ stabilises too and it follows that N is Noetherian.

$\boxed{\Leftarrow}$ Suppose that L and N are Noetherian. Without loss of generality, we may assume that $L \subseteq M$ and that $N = M/L$

Let $M_1 \subseteq M_2 \subseteq \dots$ be a chain of submodules of M.

Set $L_i = f^{-1}(M_i) = M_i \cap L$. Then we obtain a chain $L_1 \subseteq L_2 \subseteq \dots$ of submodules of L. Since L is Noetherian, this chain stabilises. Pick k large enough so that $L_n = L_k$ for all $n \geq k$. Observe that we may assume that $L = L_k$, i.e. that $N = M/L_k$. Indeed, we can work with the short exact sequence $0 \longrightarrow L_n \longrightarrow M \longrightarrow M/L_n \longrightarrow 0$ instead. The quotient modules $N_i = (M_i + L_k)/L_k \cong M_i/(M_i \cap L_k)$, for $i \geq 1$, form an ascending chain $N_1 \subseteq N_2 \subseteq \dots$ of submodules of N, which stabilises since N is Noetherian. That is, there exists $m \in \mathbb{N}$ such that $N_j = N_m$ for all $j \geq m$. Hence $M_j = M_m$ for all $j \geq m$ too. So the chain $M_1 \subseteq M_2 \subseteq \dots$ stabilises and M is Noetherian.

□

Example 2.43.

- If R is a PID, then the argument we used with $R = \mathbb{Z}$ works and shows that every submodule, quotient module and free R-module of finite rank (i.e. of the form R^n for some $n \in \mathbb{N}$) are Noetherian. Hence, every finitely generated R-module is Noetherian (see Corollary 2.47).
- $\mathbb{Q}$ is not a Noetherian $\mathbb{Z}$-module, since the chain $\mathbb{Z}[\frac{1}{2}] \subseteq \mathbb{Z}[\frac{1}{4}] \subseteq \dots \subseteq \mathbb{Z}[\frac{1}{2^n}] \subseteq \dots$ of $\mathbb{Z}$-submodules of $\mathbb{Q}$ has no maximal element. The short exact sequence $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$ shows that $\mathbb{Q}/\mathbb{Z}$ is not a Noetherian $\mathbb{Z}$-module.

- A field k is Noetherian and Artinian since the only submodules are 0 and k. Hence finite dimensional k-vector spaces too.

Combining some of the above results, we gather the following.

Theorem 2.44. *Let R be a commutative ring.*

i. If R is Noetherian, then any finitely generated R-module is Noetherian.

ii. If R is Artinian, then any finitely generated R-module is Artinian.

Proof. We only prove the statement for Noetherian rings. The assertion for Artinians is proved in a similar fashion.

Suppose that R is Noetherian. Let M be a finitely generated R-module, say $M = \langle x_1, \dots, x_n \rangle$. The multiplication by x map $m_x : R \to Rx$ is a surjective R-homomorphism and therefore $Rx \cong R/\ker(m_x)$, where $\ker(m_x) = \operatorname{Ann}(x)$, for any $x \in M$. Hence, $M \cong \sum_{i=1}^{n} R/\operatorname{Ann}(x_i)$ as R-modules. Since R is Noetherian, every finite sum of quotients of R is Noetherian, by Theorem 2.42 above. □

In Definition 1.21, we introduced the *nilradical* $\operatorname{Nil}(R) = \bigcap_{P \in \operatorname{Spec}(R)} P$ of a commutative ring R. The name suggests that $\operatorname{Nil}(R)$ is a radical ideal, i.e. $\sqrt{\operatorname{Nil}(R)} = \operatorname{Nil}(R)$, which is clear from the fact that $\sqrt{P} = P$ for every prime ideal P.

Note that any nilpotent element $a \in R$ lies in $\operatorname{Nil}(R)$ since $a \in P$ for every $P \in \operatorname{Spec}(R)$. We now prove a stronger result.

Proposition 2.45. *Let R be a commutative ring. If R is Noetherian or Artinian, then $\operatorname{Nil}(R)$ is a nilpotent ideal, i.e. $\operatorname{Nil}(R)^n = 0$ for some $n \in \mathbb{N}$.*

Proof. First suppose that R is Noetherian. Let $\operatorname{Nil}(R) = (x_1, \dots, x_k)$ for some nilpotent elements $x_i \in R$. Pick $m \in \mathbb{N}$ large enough such that $x_i^m = 0$ for all $1 \leq i \leq k$. We claim that $\operatorname{Nil}(R)^{k(m-1)+1}$ is zero. Indeed, any element of $\operatorname{Nil}(R)^{k(m-1)+1}$ is an R-linear combination of monomials of the form $a x_1^{e_1} \cdots x_k^{e_k}$ with $a \in R$ and $\sum_{i=1}^{k} e_i = k(m-1)+1$. So we cannot have the k exponents less that m, i.e. there is some x_i such that $e_1 \geq m$, which forces $a x_1^{e_1} \cdots x_k^{e_k} = 0$. Therefore, $\operatorname{Nil}(R)$ is a nilpotent ideal.

Suppose that R is Artinian. The decreasing sequence $\operatorname{Nil}(R) \supseteq \operatorname{Nil}(R)^2 \supseteq \cdots$ stabilises, i.e. there exists $n \in \mathbb{N}$ such that $\operatorname{Nil}(R)^m = \operatorname{Nil}(R)^n$ for all $m \geq n$. Suppose that $\operatorname{Nil}(R)^n \neq 0$. Let X be the set of ideals I of R such that $I \operatorname{Nil}(R)^n \neq 0$. Since $\operatorname{Nil}(R) \in X$, the set X is a nonempty poset, for the order relation defined by the inclusion of ideals. Note that since R is Artinian, the set X has some minimal element. Pick one of them, say J. Then $J \operatorname{Nil}(R)^n \neq 0$. That is, there exists $x \in J$ such that $x \operatorname{Nil}(R)^n \neq 0$, and since J is minimal, we must have $J = (x)$. In particular, J is finitely generated. By Nakayama's lemma, Theorem 2.25, the equality $\big(J \operatorname{Nil}(R)^n\big) \operatorname{Nil}(R) = J \operatorname{Nil}(R)^n$ implies $J \operatorname{Nil}(R)^n = 0$, a contradiction. Therefore $\operatorname{Nil}(R)^n = 0$ as required.

□

Let us highlight some properties of Noetherian commutative rings.

Theorem 2.46. *Let R be a commutative ring, and let M be an R-module. TFAE*

i. M is Noetherian.

ii. Every submodule of M is Noetherian.

iii. Every submodule of M is finitely generated.

Note that it does not suffice for a module to be finitely generated for it to be Noetherian: ALL its submodules need to be finitely generated. For instance, take any non-Noetherian commutative ring R, such as a polynomial ring with countably many variables $k[x_n,\ n \in \mathbb{N}]$. The regular R-module R is finitely generated (as R-module), but it has infinitely generated R-submodules, such as $\langle x_n,\ n \in \mathbb{N}\rangle = \ker(\varepsilon_0 : R \to k)$, where ε_0 is the evaluation at $(x_n = 0,\ n \in \mathbb{N})$.

Proof. Given Theorem 2.42, it suffices to show that M is Noetherian if and only if every submodule of M is finitely generated.

Suppose that every submodule of M is finitely generated. Let $M_1 \subseteq M_2 \subseteq \dots$ be a chain of submodules of M. Set $N = \bigcup_{i\in\mathbb{N}} M_i$. Then N is a submodule of M and therefore must be finitely generated by assumption. Hence, if the set $X = \{x_1, \dots, x_k\}$ generates N, each x_i belongs to some M_{j_i}, and because X is finite, there exists $n \in \mathbb{N}$ such that $x_i \in M_n$ for all $1 \le i \le k$. Therefore, the chain $M_1 \subseteq M_2 \subseteq \dots$ stabilises and we have $N = M_n$.

Conversely, suppose that M is Noetherian, and let L be a submodule of M. Without loss, suppose that $L \neq 0$ (else L is trivially finitely generated), and pick $x_1 \in L$ nonzero. Set $L_1 = Rx_1$. Next, inductively, pick $x_{i+1} \in L \setminus L_i$, and put $L_{i+1} = L_i + Rx_{i+1}$. We thus get an ascending chain $L_1 \subseteq L_2 \subseteq \dots$. Since every submodule of M is Noetherian, by Theorem 2.42, this chain stabilises, say $L_n = L_k$ for all $n \ge k$. That is, we must have $L = L_k = \langle x_1, \dots, x_k\rangle$, as required. □

Since the submodules of a commutative ring are its ideals, we record the following property.

Corollary 2.47. *A commutative ring is Noetherian if and only if every ideal is finitely generated. In particular, every PID is Noetherian.*

Let us emphasise that Noetherian rings are not PIDs in general. For instance, a power series ring $k[[x]]$ over a field k, or a multivariate polynomial ring $k[x_1, \dots, x_n]$ are not PIDs, but they are Noetherian.

If R is Noetherian, then $\mathrm{Nil}(R)$ is finitely generated, but this need not be the case in a commutative ring. For instance, if $R = \prod_{n\in\mathbb{N}} k[x]/(x^n)$, where k is a field, then $z_n = (0, \dots, 0, x+(x^n), 0, \dots) \in \mathrm{Nil}(R)$ since z_n is nilpotent, for all $n \in \mathbb{N}$. However there is no positive integer m such that $z_n^m = 0$ for all n.

Here is a very important result, named after the German mathematician David Hilbert, which identifies a large class of Noetherian commutative rings. You may recall that R is a UFD $\iff R[x]$ is a UFD. Replacing '*UFD*' with '*Noetherian*', the implication $\boxed{\Longleftarrow}$ is clear by Theorem 2.42, since $R \cong R[x]/(x)$. Hilbert's basis theorem asserts that the implication $\boxed{\Longrightarrow}$ holds too.

Theorem 2.48 (Hilbert's basis theorem)**.** *If R is Noetherian, then $R[x]$ is Noetherian.*

Proof. We invoke Corollary 2.47 and aim to show that every ideal of $R[x]$ is finitely generated. Let I be an ideal of $R[x]$. Suppose that $I \neq 0$. For all non-negative integers n, let

$$J_n = \{a \in R \mid \exists a x^n + \dots + a_1 x + a_0 \in I\} \subset R$$

In particular, $0 = 0x^n \in J_n$ for all $n \ge 0$. Note that every J_n is an ideal of R, and that, if $a \in J_n$, say $ax^n + \dots + a_1x + a_0 \in I$, then $x(ax^n + \dots + a_1x + a_0) \in I$, and so the ideals J_n for a chain $J_0 \subseteq J_1 \subseteq \cdots$. Let $J = \cup_n J_n$. Then J is an ideal of R. Since R is Noetherian, $J = J_d$ for some d large enough, and J is finitely generated. Let $J = J_d = (a_{1,d}, \dots, a_{n_d,d})$. Similarly, every J_k is finitely generated, say $J_k = (a_{1,k}, \dots, a_{n_k,k})$.

For all $1 \le i \le n_k$ and for all $0 \le k \le d$, pick $f_{i,k} \in I$ of the form $f_{i,k} = a_{i,k}x^k + g_{i,k}$, where $\deg(g_{i,k}) < k$. (Note that $g_{i,k} \in I_{k-1}$).

We obtain in this way a finite set $X = \{f_{i,k} \in I \mid 1 \le i \le n_k,\ 0 \le k \le d\}$ of elements of I. Note that since R is Noetherian, every constant polynomial in I lies in $(f_{1,0}, \dots f_{n_0,0})$.

We claim that $I = (X)$. Let $f \in I$, say $f = b_n x^n + f_1$ with $b_n \neq 0$ and $\deg f_1 < n$. To show the statement, we proceed inductively on $n = \deg f$. If $n = 0$ or if $f = 0$, then $f \in R$; that is,

$f \in (f_{1,0}, \dots f_{n_0,0})$. Suppose that $\deg f = n > 0$ and assume that every polynomial of $R[x]$ of degree stricly less than n is contained in (X).

Since $f = b_n x^n + f_1$, we have $b_n \in J_n \subseteq J_d$, and therefore there exist $c_i \in R$ for all $1 \leq i \leq n_d$ such that

$$b_n = \sum_{i=1}^{n_d} c_i a_{i,d} \ , \quad \text{and the polynomial} \quad g = \sum_{i=1}^{n_d} c_i x^{n-d} f_{i,d} \in (X)$$

has leading coefficient b_n and lies in $(f_{1,d}, \dots, f_{n_d,d}) \subseteq (X)$. Hence, $\deg(f-g) < n$ implies that $f - g \in (X)$ by induction. Therefore, $f = g + (f-g) \in (X)$. The theorem follows.

□

Hilbert's basis theorem can be applied iteratively finitely many times.

Corollary 2.49. *If R is Noetherian, then $R[x_1, \dots, x_n]$ is Noetherian. In particular, any multivariate polynomial ring over a field is Noetherian.*

We end this section with a few facts on Artininan rings. Informally, Artinian rings are rarer and smaller than Noetherian rings. We have seen that finite commutative rings are Artinian, and quotient rings of the form $k[x]/I$ are Artinian if k is a field and I an ideal of $k[x]$.

Lemma 2.50. *Let R be an ID. Suppose that R is Artinian. Then R is a field.*

Proof. Let $a \in R$, $a \neq 0$. We need to show that a is invertible. Consider the descending chain of principal ideals $(a) \supseteq (a^2) \supseteq \cdots$ Since R is Artinian, the chain stabilises and there exists $n \in \mathbb{N}$ such that $(a^m) = (a^n)$ for all $m \geq n$. In particular, a^n and a^{n+1} are associated. Since R is an ID, there exists a unit $u \in R^\times$ such that $a^{n+1} = ua^n$. By multiplicative cancellation, since $a^n \neq 0$, we obtain the equality $a = u \in R^\times$, as required.

□

Let R be a commutative ring. An *R-algebra* is a ring A equipped with a ring homomorphism $\lambda : R \to Z(A)$ such that $\lambda(1) = 1$, where $Z(A) = \{z \in A \mid az = za, \ \forall\, a \in A\}$ is the centre of A. Note that $Z(A)$ is a commutative subring of A and that λ endows an R-algebra with a structure of R-module.

For instance, polynomial rings $R[x_1, \dots, x_n]$ and group algebras RG are examples of R-algebras. It is also easy to see that any ring A (with 1) is a $\mathbb{Z}$-algebra, since the image of the unique ring homomorphism defined by sending $1_\mathbb{Z}$ to 1_A lies in the centre of A. (If A is commutative, the kernel of this map gives the characteristic of A, defined in Section 1.)

Lemma 2.51. *Let k be a field, and let A be a commutative k-algebra. If $\dim_k A < \infty$, then A is an Artinian ring.*

Proof. By assumption, A is a finite dimensional k-vector space. As observed in Example 2.43, A is Artinian as k-vector space. Since A-submodules of A are the ideals of A, which are k-vector spaces too, the result follows. □

Proposition 2.52. *Let R be a commutative ring. Suppose that R is Artinian. The following hold.*

i. Prime and maximal ideals of R coincide.

ii. R has finitely many prime ideals.

In particular $\mathrm{Nil}(R) = \mathrm{Rad}(R)$.

Proof. i. We need to show that any prime ideal is maximal. Let I be a prime ideal of R. Then R/I is an Artinian ID. By Lemma 2.50, R/I is a field. Therefore I is a maximal ideal.

ii. Suppose that $\{I_j,\ j \in J\}$ is a family of distinct prime ideals for some indexing set $J \subseteq \mathbb{N}$. We have a descending chain $I_1 \supseteq I_1 \cap I_2 \supseteq \cdots$. Since R is Artinian, the chain stabilises, and so there exists $n \in \mathbb{N}$ such that $I_1 \cap \cdots \cap I_{n+1} = I_1 \cap \cdots \cap I_n$. It follows that $I_1 \cap \cdots \cap I_n \subseteq I_{n+1}$. But since I_{n+1} is prime, we must have $I_j \subseteq I_{n+1}$ for some $1 \leq j \leq n$, by Lemma 1.12. By the first part, it follows that $I_j = I_{n+1}$, which forces $j = n+1$, and $|J|$ must be finite. Therefore R cannot have infinitely many distinct prime ideals.

□

As an immediate consequence of Propositions 2.45 and 2.52, we record the following property of Artinian rings.

Corollary 2.53. *Let R be a commutative Artinian ring, and let $J_1, \ldots, J_s$ be the complete list of maximal ideals. Let $n \in \mathbb{N}$ such that $\mathrm{Nil}(R)^n = 0$. Then $J_1^n \cdots J_s^n = 0$.*

2.8 Exercises

Exercise 2.1. Let R be a commutative ring, let M be an R-module and let I be an ideal of R. Suppose that $IM = \{\sum_{\text{finite}} a_i x_i \mid a_i \in I,\ x_i \in M\} = 0$. Define a structure of R/I-module on M.

Exercise 2.2. Recall that a $\mathbb{Z}$-module is the same as an abelian group. Determine the group structure of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n)$ as an abelian group, for all integers $m, n \geq 2$. More generally, let R be a commutative ring and I, J two ideals of R. Describe $\mathrm{Hom}_R(R/I, R/J)$ as an R-module.

Exercise 2.3. Let R be a commutative ring and let M, N be two R-modules. Verify that $\mathrm{Hom}_R(M, N)$ is an R-module for the R-action $(af)(x) = af(x)$ for all $a \in R, f \in \mathrm{Hom}_R(M, N)$ and $x \in M$. How can you generalise the construction to arbitrary rings and left modules? (cf. [Lan, Section III.2])

Exercise 2.4. Let M be an R-module.

i. Prove that the torsion subgroup $M_{\mathbb{Z}-tor}$ of M, formed by the elements of finite order, is an R-module.

ii. Suppose that R is a commutative ring.

   (a) Prove that the (R-)torsion submodule $M_{tor} = \{x \in M \mid \exists\ a \in R,\ a \neq 0, \text{ such that } ax = 0\}$ is an R-submodule of M.

   (b) Prove that $\left(M/M_{tor}\right)_{tor} = \{0\}$.

iii. Find an example of (non-commutative) ring R and R-module M for which M_{tor} is not an R-submodule of M.

Exercise 2.5. Let R be a commutative ring. The *annihilator* of an R-module M is $\mathrm{Ann}(M) = \{a \in R \mid ax = 0,\ \forall\ x \in M\}$.

i. Prove that M is faithful if and only if $\mathrm{Ann}(M) = \{0\}$.

ii. Prove that $\mathrm{Ann}(M)$ is a two-sided ideal of R.

iii. Prove that M is a faithful module as a module for the quotient ring $R/\mathrm{Ann}(M)$.

Exercise 2.6. Let R be a commutative ring.

- Let M be an R-module. Prove that $\mathrm{Hom}_R(R, M)$ is an R-module isomorphic to M.
- Prove that $\mathrm{End}_R M$ is a unital ring, generally not commutative.

Exercise 2.7. Prove that the categorical definitions of product and coproduct in the category of R-modules agree with the usual notions of direct product and direct sum.

Exercise 2.8. Let R be a commutative ring. Prove that, given any R-homomorphism $\varphi \in \mathrm{Hom}_R(M,N)$, we obtain an exact sequence

$$0 \longrightarrow \ker(\varphi) \xrightarrow{incl} M \xrightarrow{\varphi} N \xrightarrow{\pi} \mathrm{coker}(\varphi) \longrightarrow 0\ .$$

Exercise 2.9. Let R be a ring. Prove that a short exact sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ of R-modules splits if and only if B is isomorphic to $A \oplus C$.

Exercise 2.10 (Five Lemma)**.** Let R be a ring. Suppose that we have a commutative diagram of R-modules and R-homomorphisms, of the form

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{i} & E \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle e} \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{i'} & E' \end{array}\ ,$$

with exact rows. *Commutative* means that all the 'paths' between two modules are equal, e.g. $f'a = bf$.

i. Suppose that b, d are surjective and e injective. Prove that c is surjective.

ii. Suppose that b, d are injective and a surjective. Prove that c is injective.

iii. Suppose that a, b, d, e are isomorphisms. Prove that c is an isomorphism.

Exercise 2.11. Let R be a commutative ring, let I be an ideal contained in $\mathrm{Rad}(R)$ and let $\varphi : M \to N$ be an R-module homomorphism between two R-modules M, N.

i. Prove that φ induces an R-homomorphism $\varphi_* : M/IM \to N/IN$.

ii. Suppose that φ_* is surjective. Prove that φ is surjective.

Exercise 2.12. Let R be a commutative ring and let A, B be two R-modules. Prove that $0 \otimes b = a \otimes 0 = 0_{A \otimes_R B}$ for all $a \in A,\ b \in B$.

Exercise 2.13. Find an example of a UFD R and I, J be proper nonzero ideals of R such that $R/I \otimes_R R/J = 0$. Give the conditions which imply $R/I \otimes_R R/J = 0$ in general.

Exercise 2.14. Adapt the proof of Hilbert's basis theorem 2.48 to show that $R[[x]]$ is Noetherian if R is Noetherian.

Exercise 2.15. Let R be a ring, let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a short exact sequence of R-modules and let M be an R-module.

i. Prove that the sequence

$$0 \longrightarrow \mathrm{Hom}_R(M,A) \xrightarrow{f_*} \mathrm{Hom}_R(M,B) \xrightarrow{g_*} \mathrm{Hom}_R(M,C) \quad \text{is exact,}$$

where $f_*(\varphi) = f\varphi : M \to A \to B$ and similarly for g_*.

ii. Prove that the sequence

$$0 \longrightarrow \mathrm{Hom}_R(C,M) \xrightarrow{g^*} \mathrm{Hom}_R(B,M) \xrightarrow{f^*} \mathrm{Hom}_R(A,M) \quad \text{is exact,}$$

where $g^*(\varphi) = \varphi f : B \to C \to M$ and similarly for f^*.

iii. Find an example where g_* is not surjective, and an example where f^* is not surjective.

Exercise 2.16. Let R be a commutative ring. A commutative diagram of R-modules and R-homomorphisms

$$\Delta = \quad \begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\gamma} \\ C & \xrightarrow[\delta]{} & D \end{array}$$

is a:

i. *Pullback*, if for any pair of morphisms $\alpha' : A' \to B$ and $\beta' : A' \to C$ such that $\delta\beta' = \gamma\alpha'$, there exists a unique R-homomorphism $\theta : A' \to A$ such that $\alpha' = \alpha\theta$ and $\beta' = \beta\theta$.

ii. *Pushout*, if for any pair of morphisms $\gamma' : B \to D'$ and $\delta' : C \to D'$ such that $\delta'\beta = \gamma'\alpha$, there exists a unique R-homomorphism $\pi : D \to D'$ such that $\gamma' = \pi\gamma$ and $\delta' = \pi\delta$.

Prove the following.

i. Any pair of R-homomorphisms $\gamma : B \to D$ and $\delta : C \to D$ can be completed into a pullback. Moreover, in the pullback, $A \cong \{(b, c) \in B \oplus C \mid \gamma(b) = \delta(c)\}$, with the induced maps α, β being the projections onto B and C, respectively.

ii. Any pair of R-homomorphisms $\alpha : A \to B$ and $\beta : A \to C$ can be completed into a pushout. Moreover, in the pushout, $D \cong (B \oplus C)/\langle\big(\alpha(a), -\beta(a)\big) \mid a \in A\rangle$, with the induced maps γ, δ being the compositions of inclusions $B, C \to B \oplus C$ with the projections.

iii. If Δ is a pullback, then $\ker(\delta) \cong \ker(\alpha)$.

iv. If Δ is a pushout, then $\operatorname{coker}(\delta) \cong \operatorname{coker}(\alpha)$.

v. (Schanuel's lemma) Let

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

$$0 \longrightarrow B \xrightarrow{h} Q \xrightarrow{k} M \longrightarrow 0$$

be two exact sequences of R-modules with P and Q projective. Prove that $A \oplus Q \cong B \oplus P$.

Exercise 2.17. Let R be a ring and let M, N be simple R-modules, i.e. their only proper submodule is the zero module. Prove that every nonzero R-homomorphism $M \to N$ is an isomorphism.

Exercise 2.18. Let R be a commutative ring. An R-module M is *divisible* if $aM = M$ for all $0 \neq a \in R$. That is, the multiplication by a map $M \to M$ is a surjective R-homomorphism.

i. Prove that $\mathbb{Q}$ is a divisible $\mathbb{Z}$-module (i.e. abelian group).

ii. Suppose that R is an ID, and let M be a divisible R-module and let N be a torsion R-module. Prove that $M \otimes_R N = 0$.

iii. Suppose that R is an ID and let F be its field of fractions. Prove that $F \otimes_R M$ is a divisible R-module for any R-module M.

iv. Suppose that R is an ID. Prove that an injective R-module is divisible.

Exercise 2.19. Let R be a ring. Prove that an R-module M is injective if and only if, for all R-homomorphisms $\varphi : I \to M$ where I is an ideal of R, then φ extends to R, that is, there exists an R-homomorphism $\tilde{\varphi} : R \to M$ such that $\tilde{\varphi}(a) = \varphi(a)$ for all $a \in I$.

Exercise 2.20. Let R be a PID and let M be a nonzero finitely generated torsionfree R-module. Prove that M is free. (Hint: proceed by induction on the number of generators of M.)

Exercise 2.21. Let R be a commutative ring and let M be an R-module. We say that M is *faithfully flat* if it satisfies the following property: A sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ in $R-$mod is exact if and only if the sequence $0 \longrightarrow M \otimes_R A \xrightarrow{f} M \otimes_R B \xrightarrow{g} M \otimes_R C \longrightarrow 0$ is exact in $R-$mod.

i. Prove that a faithfully flat R-module is flat.

ii. Prove that an R-module M is faithfully flat if and only if M is flat and if $M \otimes_R N = 0$ implies $n = 0$ for any R-module N.

iii. As $\mathbb{Z}$-module, is $\mathbb{Q}$ faithfully flat, flat or neither?

iv. Let $\varphi : R \to S$ be a ring homomorphism, and let M be an S-module. Prove that $\mathrm{res}_\varphi M$ is flat as R-module if and only if the localisation $\mathrm{res}_\varphi(M_P)$ is flat over R_{P^c} for all $P \in \mathrm{Spec}(R)$, where $P^c = \varphi^{-1}(P)$ is the contraction of P.

3 Integral dependence

In this section, we introduce the concept of *integrality* over a ring, and we present results about integral dependence. This subject has numerous applications in algebra.

3.1 Integral extensions

Definition 3.1. Let R be a subring of a commutative ring S (i.e. with $1_R = 1_S$).

i. An element $a \in S$ is *integral over* R if there exists a monic polynomial $f \in R[x]$ with $f(a) = 0$.

ii. The set of elements of S that are integral over R is called the *integral closure* of R in S.

iii. S is an *integral extension* of R if every element of S is integral over R.

iv. Let R be an ID with field of fractions F. Then R is *integrally closed* if R is equal to its integral closure in F.

For instance, $\mathbb{Z}$ is integrally closed, since equal to its integral closure in $\mathbb{Q}$. But this need not be the case for any ID; see Proposition 3.5 below.

By definition, every element of R is integral over R. Hence the integral closure of R in S contains R, but can also be bigger. For instance, if $R = \mathbb{Z}$ and $S = \mathbb{Q}$, then the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$, whilst the integral closure of $\mathbb{Z}$ in $\mathbb{C}$ is the ring of Gaussian integers $\mathbb{Z}[i]$. Note that the ring of Gaussian integers $\mathbb{Z}[i]$ is an integral extension of $\mathbb{Z}$. The elements of the integral closure of $\mathbb{Z}$ in $\mathbb{C}$ are called the *algebraic integers*. (Recall that if R is a UFD with field of fractions F, then a root $\frac{a}{b} \in F$ with $\gcd(a, b) = 1$ of a polynomial $f = \sum_{i=0}^{n} c_i x^i \in R[x]$ satisfies $b \mid c_n$ and $a \mid c_0$.)

In this section, we investigate some properties of integral extensions of commutative rings.

Recall from page 39 that an R-algebra is a ring A with a ring homomorphism $\lambda : R \to Z(A)$, the centre of A, such that λ endows A with a structure of R-module. In particular a ring inclusion $R \hookrightarrow S$, with R commutative, makes S into an R-algebra.

Given elements $a_1, \ldots, a_n \in S$, we can form the R-algebra $R[a_1, \ldots, a_n]$ *generated by* $a_1, \ldots, a_n \in S$. This is the smallest subring of S containing $R, a_1, \ldots, a_n$. For instance, $\mathbb{Z}[i\sqrt{2}]$ is the $\mathbb{Z}$-algebra generated by $i\sqrt{2}$, and it is a $\mathbb{Z}$-subalgebra of $\mathbb{C}$.

We also can consider the R-module generated by $a_1, \ldots, a_n$, denoted

$$Ra_1 + \cdots + Ra_n = \{\sum_{i=1}^{n} b_i a_i \mid b_i \in R, \ \forall\ 1 \leq i \leq n\}.$$

Note that,

$$R \subseteq Ra_1 + \cdots + Ra_n \subseteq R[a_1, \ldots, a_n] \subseteq S.$$

An R-algebra A is:

- *Finitely generated* over R if there exist finitely many elements $a_1, \ldots, a_n \in A$ that generate A as a ring, i.e. $A = R[a_1, \ldots, a_n]$ (polynomials in $a_1, \ldots, a_n$ with coefficients in R).
- *Finite* over R if A is a finitely generated R-module, i.e. there exist finitely many elements $a_1, \ldots, a_n \in A$ such that $A = Ra_1 + \cdots + Ra_n$.

A typical example of a finitely generated R-algebra is a polynomial ring $R[x_1, \ldots, x_n]$. It is not finite since not finitely generated as an R-module since $x_{i_1}^{a_1} \cdots x_{i_k}^{a_k} \notin Ra_1 + \cdots + Ra_n$, unless such monomial is equal to one of the x_j. The ring of Gaussian integers is a finite $\mathbb{Z}$-algebra, since $\mathbb{Z}[i] \cong \mathbb{Z} \oplus \mathbb{Z}i$ as a $\mathbb{Z}$-module.

Note that the a_j's in $R[a_1, \ldots, a_n]$ may be subject to some nontrivial R-linear relation. For instance, $a_1 = i, a_2 = \frac{1}{2} + \frac{i\sqrt{3}}{2} \in \mathbb{C}$ are both integral over $\mathbb{Z}$, since they are primitive 4-th and 6-th roots of 1, respectively, and, $a_1^2 = a_2^3 = -1$ is a nontrivial relation.

Proposition 3.2. *Let R be a subring of a commutative ring S, and let $a \in S$. TFAE.*

(i) a is integral over R.

(ii) The subring $R[a]$ of S is a finite R-algebra.

(ii) There exists a faithful $R[a]$-submodule of S that is finitely generated as R-module.

Proof. (i)$\Longrightarrow$(ii) Suppose that a is integral over R, say $f(a) = 0$ where $f = x^n + b_1 x^{n-1} + \cdots + b_n \in R[x]$. Hence

$$a^n = -(b_1 a^{n-1} + \cdots + b_n) \in Ra + \cdots + Ra^{n-1}.$$

Therefore, every element of $R[a]$ can be expressed as an R-linear combination of $1, a, \ldots, a^{n-1}$, saying that $R[a]$ is a finitely generated R-module.

(ii)$\Longrightarrow$(iii) $R[a]$ is a faithful $R[a]$-module since $1 \in R[a]$.

(iii)$\Longrightarrow$(i) Let M be a faithful $R[a]$-submodule of S that is finitely generated as R-module, and let $v_1, \ldots, v_n \in M$ be a set of generators of M as R-module, i.e. $M = Rv_1 + \cdots + Rv_n$. Consider the multiplication by a map as an R-endomorphism $\mu_a : M \to M$, $\mu_a(x) = ax$. In particular, for all $1 \leq i \leq n$, there exist elements $a_{i,j} \in R$ such that $av_i = \sum_{j=1}^{n} a_{i,j} v_j$. Rearranging the resulting equalities, we can write

$$\begin{aligned}
(a - a_{1,1})v_1 - a_{1,2}v_2 - \cdots - a_{1,n}v_n &= 0 \\
-a_{1,1}v_1 + (a - a_{1,2})v_2 - \cdots - a_{1,n}v_n &= 0 \\
\ddots \qquad\qquad &\vdots \\
-a_{1,1}v_1 - a_{1,2}v_2 - \cdots + (a - a_{1,n})v_n &= 0
\end{aligned}$$

Let $X = aI_n - (a_{i,j})$ be the $n \times n$ matrix with coefficients in R corresponding to this system of linear equations. That is, the above is equivalent to the matrix equation $X \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Let $c \in R[x]$ be the characteristic polynomial of the matrix $(a_{i,j})$, then $c(a) = 0$, which shows that a is a root of a monic polynomial with coefficients in R.

□

Let R be a subring of a commutative ring S, and suppose that $a, b \in S$ are integral over R. Then the R-algebras $R[a], R[b]$ are both finitely generated as R-modules, and hence $R[a, b]$ too. Explicitly, if $\{u_1, \ldots, u_m\}$, $\{v_1, \ldots, v_n\} \subseteq S$ generate $R[a]$ and $R[b]$ as R-modules, respectively, then the set $\{u_i v_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$ generates $R[a, b]$ as R-module. It follows that the sum, difference and product of elements integral over R are integral over R.

Corollary 3.3. *Let R be a subring of a commutative ring S. The integral closure of R in S is a subring of S containing R. In particular, if $a_1, \ldots, a_n \in S$ are integral over R, then $R[a_1, \ldots, a_n]$ is a finite R-algebra.*

Remark 3.4. Let R be a subring of a commutative ring S and let $a \in S$. Let $\overline{R}$ be the integral closure of R in S. Then, a is integral over R, i.e. $a \in \overline{R}$, if and only if $a^m \in \overline{R}$ for any $m \in \mathbb{N}$. Indeed, by Corollary 3.3, if $a \in \overline{R}$, then $a^m \in \overline{R}$ for all $m \in \mathbb{N}$. Conversely, if $f = x^n + b_1 x^{n-1} + \cdots + b_n \in R[x]$ satisfies $f(a^m) = 0$, then $\tilde{f} = x^{mn} + b_1 x^{m(n-1)} + \cdots + b_n \in R[x]$ satisfies $\tilde{f}(a) = 0$.

We end this introduction on integral dependence in commutative rings with the following observation.

Proposition 3.5. *Let R ba a UFD. Then R is integrally closed.*

Proof. Let K be the field of fractions of R, and let $\overline{R}$ be the integral closure of R in K. We want to show that $\overline{R} \subseteq R$, since the converse inclusion is obvious. Let $\frac{a}{b} \in \overline{R}$, with $\gcd(a,b) = 1$. Let $f = x^n + c_1 x^{n-1} + \cdots + c_n \in R[x]$ such that

$$0 = f(\frac{a}{b}) = (\frac{a}{b})^n + c_1(\frac{a}{b})^{n-1} + \cdots + c_{n-1}(\frac{a}{b}) + c_n.$$

Multiplying by b^n and rearranging the terms, we obtain the equation

$$a^n = -b\big(c_1 a^{n-1} + \cdots + c_{n-1} a b^{n-2} + c_n b^{n-1}\big).$$

Since R is a UFD, every prime divisor of b divides a^n, and hence a. But $\gcd(a,b) = 1$, which forces $b \in R^\times$. Thus $\frac{a}{b} \in R$.

□

Remark 3.6. Observe that the theory above generalises to the case when $\varphi : R \hookrightarrow S$ is an injective ring homomorphism.

3.2 Properties of integral extensions

In this brief section, we prove a few properties of integral extensions, starting with a transitivity property.

Proposition 3.7. *Let $R \subseteq S \subseteq T$ be inclusions of commutative rings. Suppose that S is integral over R and that T is integral over S. Then T is integral over R. Hence, the integral closure in T of the integral closure of R in S is equal to the integral closure of R in T.*

Note that if T is an integral extension of R, then T is an integral extension of S and S is an integral extension of R. The converse, stated in Proposition 3.7, is slightly less obvious.

Proof. Let $a \in T$, and let $f = x^n + b_1 x^{n-1} + \cdots + b_n \in S[x]$ such that $f(a) = 0$. Let $A = R[b_1, \ldots, b_n]$. Since $b_1, \ldots, b_n$ are integral over R, the R-algebra A is a finitely generated R-module. Moreover, since a is integral over A, the A-algebra $A[a]$ is a finitely generated A-module, and therefore finitely generated as R-module too. Thus a is integral over R. The result follows. □

Suppose that S is commutative, and let I be an ideal of S. Recall from Definition 1.19 that the *contraction* of I is the ideal $I^c = I \cap R$ of R. Recall also from Definition 1.31 that if U is a multiplicatively closed subset of R, the *localisation* of R at U is denoted R_U. As in Proposition 3.5, let us denote $\frac{a}{u}$ the class $[a,u] \in R_U$, for $a \in R$ and $u \in U$.

Proposition 3.8. *Let R be a subring of a commutative ring S. Suppose that S is integral over R.*

i. Let I be an ideal of S. Then S/I is integral over R/I^c.

ii. Let U be a multiplicatively closed subset of R. Then S_U is integral over R_U.

iii. Suppose that S is an ID. Then S is a field if and only if R is a field.

(Loosely, we could say that integrality is preserved by passage to quotient rings and to localisation.)

Proof. i. Let $\overline{a} := a + I \in S/I$, and let $f = x^n + b_1 x^{n-1} + \cdots + b_n \in R[x]$ such that $f(a) = 0$ for some representative $a \in \overline{a}$. By the isomorphism theorem for rings, $(R+I)/I \cong R/I^c$. Hence, reduction mod I of the coefficients gives the polynomial $\overline{f} = x^n + \overline{b_1} x^{n-1} + \cdots + \overline{b_n} \in R/I^c[x]$, with $\overline{f}(\overline{a}) = \overline{f(a)} = 0$. So $\overline{a}$ is integral over R/I^c.

ii. Let $\frac{a}{u} \in S_U$, and let $f = x^n + b_1 x^{n-1} + \cdots + b_n \in R[x]$ such that $f(a) = 0$. Let $g = x^n + \frac{b_1}{u} x^{n-1} + \cdots + \frac{b_n}{u^n} \in R_U[x]$. Then we check that $g(\frac{a}{u}) = \frac{f(a)}{u^n} = \frac{0}{u^n} = 0$ in R_U.

iii. Note that R is an ID since $R \subseteq S$. Suppose that R is a field, and let $a \in S,\ a \neq 0$. Let $f = x^n + b_1 x^{n-1} + \cdots + b_n \in R[x]$ such that $f(a) = 0$, with $\deg f$ minimal. Hence $b_n \neq 0$ since S is an ID (and so a cannot be a zero divisor). Since R is a field, $b_n^{-1} \in R$ and we calculate

$$\begin{aligned} -b_n &= a^n + b_1 a^{n-1} + \cdots + b_{n-1} a = a(a^{n-1} + b_1 a^{n-2} + \cdots + b_{n-1}) \\ 1 &= -\frac{1}{b_n} a(a^{n-1} + b_1 a^{n-2} + \cdots + b_{n-1}) \quad \text{giving} \\ a^{-1} &= -\frac{1}{b_n}(a^{n-1} + b_1 a^{n-2} + \cdots + b_{n-1}) \in S. \end{aligned}$$

It follows that S is a field.

Conversely, suppose that S is a field, and let $a \in R,\ a \neq 0$. So $a^{-1} \in S$ is integral over R. Pick $f = x^n + b_1 x^{n-1} + \cdots + b_n \in R[x]$ such that $f(a^{-1}) = 0$. Since $a \neq 0$ and R is an ID, multiplication by a^{n-1} in R is injective and we obtain the equation

$$0 = a^{n-1} f(a^{-1}) = a^{-1} + b_1 + b_2 a + \cdots + b_n a^{n-1},$$

That is,

$$a^{-1} = -\big(b_1 + b_2 a + \cdots + b_{n-1} a^{n-2} + b_n a^{n-1}\big) \in R.$$

□

As a consequence of Proposition 3.8, we record the following observation. The proof is left as an exercise.

Corollary 3.9. *Let R be a subring of a commutative ring S and let I be a prime ideal of S. Suppose that S is integral over R. Then $I \in \mathrm{MaxSpec}(S)$ if and only if $I^c \in \mathrm{MaxSpec}(R)$.*

Proof. By assumption, S/I is an ID. By Proposition 3.8, S/I is integral over R/I^c, and S/I is a field if and only if R/I^c too. The result follows. □

3.3 Going-up, and going-down theorems

The going-up and going-down theorems consider chain conditions on prime ideals of R and S when S is an integral extension of R.

We begin with the *going-up* results:

Given an integral ring extension $R \subseteq S$, can we obtain information on $\mathrm{Spec}(S)$ from $\mathrm{Spec}(R)$?

For instance, Proposition 3.8(iii) tells us that, if S is an ID, then $\mathrm{Spec}(R) = \{0\}$ if and only if $\mathrm{Spec}(S) = \{0\}$.

Proposition 3.10. *Let R be a subring of a commutative ring S. Suppose that S is integral over R. Let $P, Q \in \mathrm{Spec}(S)$ with $P \subsetneq Q$. Then $P^c \subsetneq Q^c$.*

Hence, if S is integral over R, then contraction defines an injective function $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$.

Proof. From Section 1.6, $P^c, Q^c \in \mathrm{Spec}(R)$, with $P^c \subseteq Q^c$.

Suppose that $P^c = Q^c$. Let U be the multiplicative subset $U = R \setminus Q^c$ of R. By Proposition 3.8(ii), the localisation S_U is integral over R_U. Moreover, $P^c = Q^c = Q \cap R$ implies that $U \cap P^c = \emptyset$.

By Theorem 1.38, if $P \subsetneq Q$, then $PS_U \subsetneq QS_U$ and P^c is the unique maximal ideal of R_U. Since S_U is integral over R_U, Corollary 3.9 shows that P is the unique maximal ideal of S. But $P \subsetneq Q$; a contradiction. So $P^c \neq Q^c$ as required.

□

Theorem 3.11 (Lying-over theorem)**.** *Let R be a subring of a commutative ring S. Suppose that S is integral over R. For every prime ideal $P \in \mathrm{Spec}(R)$, there exists $Q \in \mathrm{Spec}(S)$ such that $P = Q^c$.*

Hence, if S is integral over R, then contraction defines a bijective function $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$.

Proof. Let $U = R \setminus P$. By Proposition 3.8, S_U is integral over R_U, and since $P \in \mathrm{Spec}(R)$, we know that R_U is local with unique maximal ideal PR_U. By Proposition 3.10, PS_U is a proper ideal of S_U. The commutative diagram $\begin{array}{ccc} S & \longrightarrow & S_U \\ \uparrow & & \uparrow \\ R & \longrightarrow & R_U \end{array}$ may help following the argument below. Here, the maps are the obvious injective ring homomorphisms, regarded as inclusions (slight abuse).

Let J be a maximal ideal of S_U containing PS_U. Then the contraction $J \cap R_U$ is a prime ideal of R_U containing PR_U, which forces the equality $(J \cap R_U) = PR_U$, by maximality of PR_U. Let $Q = J \cap S$ be the contraction of J from S_U to S. Then $Q \in \mathrm{Spec}(S)$, since $J \in \mathrm{Spec}(S_U)$, and we have

$$Q \cap R = (J \cap S) \cap R = (J \cap R_U) \cap R = PR_U \cap R = P \quad \text{since } U = R \setminus P.$$

□

Here is a useful criterion, similar to the lying-over theorem 3.11, without the integrality assumption.

Proposition 3.12. *Let R be a subring of a commutative ring S, and let $P \in \mathrm{Spec}(R)$. There exists $Q \in \mathrm{Spec}(S)$ such that $P = Q^c$ if and only if $P^{ec} = P$.*

Proof. Suppose that there exists $Q \in \mathrm{Spec}(S)$ such that $P = Q^c = Q \cap R$. Note that $P \subseteq (PS \cap R) = P^{ec}$, and that $Q \supseteq (Q \cap R)S = Q^{ce}$. Therefore, $P^{ec} = (Q^c)^{ec} = (Q^{ce})^c \subseteq Q^c = P$, as required.

Conversely, suppose that $P^{ec} = P$ for some $P \in \mathrm{Spec}(R)$, and consider the multiplicative subset $U = R \setminus P$ of S. Since $P^{ec} = P$, we have $PS \cap U = \emptyset$. Therefore, in the localisation S_U, the ideal $(P^e)_U$ is proper. Let $I \in \mathrm{MaxSpec}(S_U)$ such that $(P^e)_U \subseteq I$. Then $Q = \{a \in S \mid \exists\, u \in U, \text{ with } \frac{a}{u} \in I\} \supseteq P^e$ is the preimage of I under the injective ring homomorphism $S \to S_U$. Thus, $Q \in \mathrm{Spec}(S)$, and $Q \cap U = \emptyset$. It follows that $Q \cap R \subseteq P$, and since $P^e \subseteq Q$, we conclude that $P = P^{ec}$ must be equal to Q^c.

□

Theorem 3.13 (Going-up theorem)**.** *Let R be a subring of a commutative ring S. Suppose that S is integral over R. Let $P_1, P_2 \in \mathrm{Spec}(R)$ with $P_1 \subsetneq P_2$, and let $Q_1 \in \mathrm{Spec}(S)$. Suppose that $P_1 = Q_1^c$. Then there exists $Q_2 \in \mathrm{Spec}(S)$ such that $Q_1 \subsetneq Q_2$ and $Q_2^c = P_2$. More generally, given a strictly increasing chain $P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_n$ in $\mathrm{Spec}(R)$, and $Q_1 \in \mathrm{Spec}(S)$ such that $Q_1^c = P_1$, then there exist prime ideals $Q_2, \ldots, Q_n \in \mathrm{Spec}(S)$ such that $Q_i^c = P_i$ for all $1 \leq i \leq n$ and $Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_n$.*

The going-up problem can be visualised as follows:

$$\begin{array}{ccc} S & & \mathrm{Spec}(S) \\ {\scriptstyle integ}\uparrow & & \vdots\, c \\ R & & \mathrm{Spec}(R) \end{array} \qquad \begin{array}{ccccc} Q_1 & \xhookrightarrow{incl} & ? & \cdots & \cdots \\ \downarrow c & & \downarrow c & & \\ P_1 & \xhookrightarrow{incl} & P_2 & \xhookrightarrow{incl} & \cdots \end{array}$$

Proof. It suffices to show the result for $n = 2$. Let $\overline{R} = R/P_1$ and $\overline{S} = S/Q_1$. By Proposition 3.8(i), $\overline{S}$ is integral over $\overline{R}$. By Theorem 3.11, there exists $\overline{Q_2} \in \mathrm{Spec}(\overline{S})$ such that $\overline{Q_2}^c = \overline{P_2}$, where the contraction is with respect to the inclusion $\overline{R} \cong (R + Q_1)/Q_1 \hookrightarrow \overline{S}$. Taking the preimage under the projection map $\pi : S \mapsto \overline{S}$ gives a prime ideal $Q_2 \in \mathrm{Spec}(S)$, and by construction, $Q_2 \cap R = P_2$ and $Q_1 \subsetneq Q_2$.

□

We now reverse the exercise and consider the *going-down* results. For this, we need to make a detour via properties of integral closures and integrally closed IDs, collecting the results we will use in a proposition.

Definition 3.14. i. Let $R \subseteq S$ be a ring extension, let $\overline{R}$ denote the integral closure of R in S and let I be an ideal of R. An element $a \in S$ is *integral over* I if there exists a monic polynomial $f \in R[x]$ such that $f(a) = 0$ and the nonleading coefficients of f lie in I.

ii. The *integral closure* of I in S is the set of elements of S that are integral over I. This is an abelian subgroup of $\overline{R}$ closed under multiplication.

iii. If K/F is a field extension and $a \in K$, we say that a is *algebraic over* F if a is the root of a nonzero polynomial $f \in F[x]$.

iv. The *minimal polynomial* $m_{a,K} \in F[x]$ of a is the monic polynomial of least degree having a as a root. Equivalently, $m_{a,K}$ is the monic generator of the kernel of the evaluation map $\epsilon_a : F[x] \to K$, defined by $\epsilon_a(f) = f(a)$. (Recall that $F[x]$ is a PID.)

For instance, $\sqrt{2} \in \mathbb{R}$ is integral over the ideal (2) of $\mathbb{Z}$ since it is a root of $x^2 - 2$. An example of a minimal polynomial is $x^2 + 1 = m_{i,\mathbb{C}} \in \mathbb{Q}[x]$.

Proposition 3.15. *Let R be a subring of a commutative ring S.*

i. Let U be a multiplicative subset of R and let $\overline{R}$ denote the integral closure of R in S. Then $(\overline{R})_U$ is the integral closure of R_U in S_U.

ii. Suppose that R is an ID. TFAE:

(a) R is integrally closed.

(b) R_P is integrally closed for every $P \in \mathrm{Spec}(R)$.

(c) R_P is integrally closed for every $P \in \mathrm{MaxSpec}(R)$.

iii. Suppose that S is an ID, and that R is integrally closed. Let $a \in S$ be integral over an ideal I of R. Then a is algebraic over the field of fractions K of R, and the nonleading coefficients of its minimal polynomial $m_{a,K} \in R[x]$ are all in $\sqrt{I}$.

iv. Let I be an ideal of R and let $\overline{R}$ denote the integral closure of R in S. The integral closure of I in S is equal to $\sqrt{I\overline{R}}$, the radical of the expansion of I in $\overline{R}$.

Proof. i. By Proposition 3.8, $\overline{R}_U$ is integral over R_U. Conversely, we want to show that for every $\frac{a}{u} \in S_U$ integral over R_U, we have in fact $\frac{a}{u} \in \overline{R}_U$. Since $\frac{a}{u}$ is integral over R_U and $u \in U$, there exists $f = x^n + \frac{b_1}{v_1}x^{n-1} + \cdots + \frac{b_n}{v_n} \in R_U[x]$ such that $f(\frac{a}{1}) = 0$. Let $d = v_1 \cdots v_n$. Multiplying both sides by d^n yields

$$\frac{a^n}{1} = -(\frac{b_1}{v_1}\frac{a^{n-1}}{1} + \cdots + \frac{b_n}{v_n}), \quad \text{whence} \quad \frac{(da)^n}{1} = -(\frac{b_1'}{1}\frac{(da)^{n-1}}{1} + \cdots + \frac{b_n'}{1}).$$

Note that $b_j' = b_j d^j \in R$ for all $1 \leq j \leq n$. By definition of the localisation, there exists $v \in U$ such that $v((da)^n + b_1'(ad)^{n-1} + \cdots + b_n') = 0$, and therefore, putting $w = vd$, we obtain the relation $(aw)^n + vb_1'(aw)^{n-1} + \cdots + v^n b_n' = 0$, showing that aw is integral over R. Since $\frac{a}{u} = \frac{aw}{uw}$, the conclusion follows.

ii. Let K be the field of fractions of R, and let $\overline{R}$ be the integral closure of R in K. Let $f : R \to \overline{R}$ be the inclusion. So $R = \overline{R}$ if and only if f is surjective. By part (i), $R_P = \overline{R}_P$ for every $P \in \mathrm{Spec}(R)$ if and only if the induced inclusion $f_P : R_P \to \overline{R}_P$ is surjective. Similarly for $\mathrm{MaxSpec}(R)$ instead of $\mathrm{Spec}(R)$. Corollary 2.37 shows the equivalence (iia), (iib) and (iic).

iii. Let $b_0, \ldots, b_{n-1} \in K$ such that $m_{a,K} = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n$. Let F be a splitting field for $m_{a,K}$ over K, and let $a_1, \ldots, a_n \in F$ such that $m_{a,K} = \prod_{i=1}^n (x - a_i) \in F[x]$ with $a_1 = a$. The equation $x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n = \prod_{i=1}^n (x - a_i)$ says that, up to signs, every b_i is an elementary symmetric polynomial in $a_1, \ldots, a_n$. Moreover, for all $2 \leq i \leq n$, there exists $\varphi_i \in \mathrm{Aut}_K(F)$, the Galois group of F over K, such that $\varphi_i(a) = a_i$. So $\varphi_i(I) = I$ for all i, since $I \subseteq R$, showing that all the roots a_i of $m_{a,K}$ are integral over I. Therefore, the R-subalgebra $R[a_1, \ldots, a_n]$ of S is finite, which implies that $b_0, \ldots, b_{n-1}$ are integral over I since every b_j is a polynomial in $a_1, \ldots, a_n$. Since R is integrally closed, it follows that $b_i \in \sqrt{I}$ for all $0 \leq i \leq n-1$, as required.

iv. Let $a \in \overline{I}$, and let $f = x^n + b_1 x^{n-1} + \cdots + b_n \in R[x]$ such that $f(a) = 0$ and $b_j \in I^j$ for all $1 \leq j \leq n$. Then $a^n = -(b_1 a^{n-1} + \cdots + b_n) \in \overline{I}$, and $a \in \sqrt{I\overline{R}}$.

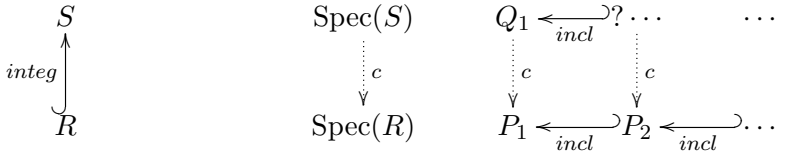
Conversely, let $a \in \sqrt{I\overline{R}}$. Let $n \in \mathbb{N}$ such that $a^n \in I\overline{R}$, say $a^n = \sum_{i=1}^t b_i c_i$ with $b_i \in \overline{R}$ and $c_i \in I$ for all i. Since every b_i is integral over R, the R-algebra $M = R[b_1, \ldots, b_t]$ is finite by Corollary 3.3, and we have an inclusion $a^n M \subseteq IM$ By Proposition 2.21, there exists an equation of the form $\varphi^n + a_1\varphi^{n-1} + \cdots + a_n = 0$, where $a_i \in I$ for all i and $\varphi \in \mathrm{End}_R M$ denotes the multiplication by a^n map. Hence a is integral over I.

□

We are now ready to prove the going-down theorem.

Theorem 3.16 (Going-down theorem)**.** *Let R be a subring of an ID S. Suppose that S is an integral extension of R and that R is integrally closed. Let $P_1, P_2 \in \mathrm{Spec}(R)$ such that $P_2 \subseteq P_1$. Suppose that there exists $Q_1 \in \mathrm{Spec}(S)$ such that $P_1 = Q_1^c$. Then there exists $Q_2 \in \mathrm{Spec}(S)$ such that $Q_2 \subseteq Q_1$ and $Q_2^c = P_2$. More generally, given a strictly decreasing chain $P_1 \supsetneq P_2 \supsetneq \cdots \supsetneq P_n$ in $\mathrm{Spec}(R)$, and $Q_1 \in \mathrm{Spec}(S)$ such that $Q_1^c = P_1$, then there exist prime ideals $Q_2, \ldots, Q_n \in \mathrm{Spec}(S)$ such that $Q_i^c = P_i$ for all $1 \leq i \leq n$ and $Q_1 \supsetneq Q_2 \supsetneq \cdots \supsetneq Q_n$.*

The going-down problem can be visualised as follows:



Proof. It suffices to prove the result for $n = 2$. Let $P_1, P_2 \in \mathrm{Spec}(R)$ such that $P_2 \subseteq P_1$, and let $Q_1 \in \mathrm{Spec}(S)$ such that $P_1 = Q_1^c$. Consider the localisation S_{Q_1}. Note that S_{Q_1} is an extension of R, which need not be integral.

We show that $P_2 S_{Q_1} \cap R = P_2$. The inclusion $P_2 \subseteq P_2 S_{Q_1} \cap R$ is clear. Conversely, let $a = \dfrac{b}{u} \in P_2 S_{Q_1}$ with $b \in P_2 S$ and $u \in S \setminus Q_1$. Since b is integral over P_2, Proposition 3.15(iii) says that the minimal polynomial $m_{b,K}$ of b over the field of fractions K of R has the form

$$m_{b,K} = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n, \quad \text{where } b_i \in \sqrt{P_2} = P_2, \text{ for all } i.$$

Suppose that $a = \dfrac{b}{u} \in P_2 S_{Q_1} \cap R$. Then $u = \dfrac{b}{a}$, where $\dfrac{1}{a} \in K$. It follows that u has minimal polynomial over K of the form

$$m_{u,K} = x^n + \frac{b_1}{a}x^{n-1} + \cdots + \frac{b_{n-1}}{a^{n-1}}x + \frac{b_n}{a^n} \in K[x].$$

Since u is integral over R, taking $I = R$ in Proposition 3.15(iii) shows that $\dfrac{b_i}{a^i} \in R$ for all i. Hence $b_i = (\dfrac{b_i}{a^i})a^i \in P_2 \subsetneq R$.

If we suppose that $a = \frac{b}{u} \notin P_2$, then we must have $(\frac{b_i}{a^i}) \in P_2$, since P_2 is prime. Therefore u is integral over P_2, and so over P_1 too. But this would imply $u \in \sqrt{P_1 S} \subseteq Q_1$ by Proposition 3.15(iv), contradicting the fact that $u \in S \setminus Q_1$. Therefore $a \in P_2$, and it follows that $P_2 S_{Q_1} \cap R = P_2$ as we wanted to show.

By Proposition 3.12, since $P_2 S_{Q_1} \cap R = P_2^{ec} = P_2$, there exists $Q_2^* \in \mathrm{Spec}(S_{Q_1})$ such that $Q_2^* \cap R = P_2$. Let $Q_2 \in \mathrm{Spec}(S)$ be the contraction of the prime ideal Q_2^* along the inclusion $S \hookrightarrow S_{Q_1}$. We have $Q_2 \subseteq Q_1$ and $Q_2 \cap R = Q_2^* \cap R = P_2$.

□

3.4 Dedekind domains

Dedekind domains form a class of commutative rings in which a sort of unique factorisation defined in terms of ideals works. They are named after the German mathematician Richard Dedekind. The study of these rings originates in algebraic number theory.

Definition 3.17. A *Dedekind domain* is an integrally closed Noetherian ID in which nonzero prime and maximal ideals coincide.

In particular, every PID is a Dedekind domain, since Noetherian by Corollary 2.47, integrally closed by Proposition 3.5 and $\mathrm{Spec}(R) = \mathrm{MaxSpec}(R) \cup \{(0)\}$, by Theorem 1.14. Note however that $\mathbb{Z}[x]$ or $k[x, y]$ (k a field) are not Dedekind domains since (x) is a nonzero prime ideal which is not maximal.

The *unique factorisation* in Dedekind domains is as follows.

Theorem 3.18. *Let R be a Dedekind domain, and let I be a nonzero ideal of R. Then, there exist*

- *a unique set $\{P_1, \ldots, P_n\} \subseteq \mathrm{Spec}(R) \setminus \{(0)\}$, and*
- *positive integers $e_1, \ldots, e_n$, such that*

$$I = P_1^{e_1} \cdots P_n^{e_n}.$$

To prove the theorem, we need some technical results about *fractional ideals*. Recall that if R is a subring of some ring S, then S is a left R-module for the R-action defined by left multiplication.

Definition 3.19. Let R be an ID with field of fractions K.

i. A *fractional ideal* is an R-submodule M of K such that there exists $\frac{a}{b} \in K^\times$ with $\frac{a}{b} M \subseteq R$. A fractional ideal is *principal* if it is generated (as R-module) by one element of K.

ii. If M is a fractional ideal of R, we define

$$M^{-1} = \{\frac{a}{b} \in K \mid \frac{a}{b} M \subseteq R\}.$$

iii. If M is a fractional ideal, we call M *invertible* if there exists a fractional ideal M' such that $MM' = R$, where MM' is the R module whose elements are finite sums of the form $\sum_i x_i y_i$, with $x_i \in M$ and $y_i \in M'$.

Example 3.20. The $\mathbb{Z}$-submodule $\mathbb{Z}[\frac{1}{2}]$ of $\mathbb{Q}$ is a principal fractional ideal of $\mathbb{Z}$, and

$$\mathbb{Z}[\frac{1}{2}]^{-1} = \{\frac{a}{b} \in \mathbb{Q} \mid \gcd(a, b) = 1 \text{ and } 2 \text{ divides } a\}.$$

Note that if I is an ideal of R, then I is a fractional ideal and $R \subseteq I^{-1}$; moreover $R^{-1} = R$ is invertible.

Remark 3.21. Let R be a Noetherian ID with field of fractions K. Then any finitely generated R-submodule of K is a fractional ideal of R. Conversely, the fractional ideals of R are precisely the finitely generated R-submodules of K. Indeed, if M is a finitely generated R-submodule of K, say $M = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle$, then $(b_1 \cdots b_n)M \subseteq R$. Conversely, if $M \subseteq K$ is a fractional ideal of R, then, for all $0 \neq a \in R$, multiplication by a yields an R-isomorphism $M \cong aM$ (since a is invertible in K). That is, the R-module M is isomorphic to an ideal of R; therefore it is finitely generated since R is Noetherian.

The following exercise consists of routine verifications of the statements from the definition, and they summarise some elementary properties of fractional ideals.

Lemma 3.22. *Let R be a Dedekind domain not a field, and let $P \in \mathrm{MaxSpec}(R)$.*

i. Let I be a nonzero ideal of R properly contained in P, and let $A = \{a \in R \mid aP \subseteq I\}$. Then A is an ideal of R containing I properly.

ii. P is invertible.

iii. Let I be an invertible fractional ideal of R. Then I is finitely generated as R-module.

Proof. Note that $P \neq (0)$.

i. Since I is an ideal, $I \subseteq A$. It is routine to check that A is an ideal of R. (Note that if $I = (0)$, then $A = (0)$ too since R is an ID.) It remains to show that, assuming that $I \neq (0)$, then A contains elements that are not in I.

   We claim that there exist $P_1, \ldots, P_n \in \mathrm{Spec}(R)$ such that $I \subseteq P_i$ for all i and $\prod_{i=1}^n P_i \subseteq I$ (the P_i's not necessarily distinct). We show the claim by contradiction, and choose an ideal I to be a maximal counterexample to the claim (maximal with respect to inclusion of ideals). In particular, I is not prime, and therefore there exist $a, b \in R$ such that $a, b \notin I$ and $ab \in I$. That is, $I + aR, I + bR$ contain I properly and $(I + aR)(I + bR) \subseteq I$. By maximality assumption on I, the ideals $(I + aR)$ and $(I + bR)$ contain finite products of prime ideals, say $Q_1 \cdots Q_r \subseteq I + aR$ and $Q'_1 \cdots Q'_s \subseteq I + bR$ with $Q_i \supseteq I + aR$ and $Q'_j \supseteq I + bR$ for all i, j. But then $Q_1 \cdots Q_r Q'_1 \cdots Q'_s \subseteq I$ and $Q_i \supseteq (I + aR) \supsetneq I$ and $Q'_j \supseteq (I + bR) \supsetneq I$ for all j, a contradiction. Therefore, the claim holds, i.e. there exist $P_1, \ldots, P_n \in \mathrm{Spec}(R)$ such that $I \subseteq P_i$ for all i and $\prod_{i=1}^n P_i \subseteq I$. Amongst the sets of such ideals, choose one with n minimal.

   The inclusion $\prod_{i=1}^n P_i \subseteq P$ with P prime implies that there exists some j such that $P_j \subseteq P$, without loss, assume $j = 1$. Since P_1 cannot be (0) because $I \subseteq P$, the ideal P_1 is maximal. Therefore, we must have the equality $P_1 = P$, which implies that $\prod_{i=2}^n P_i \subseteq A$ by definition of A. On the other hand, by minimality of n such that $\prod_{i=1}^n P_i \subseteq I$, the ideal $\prod_{i=2}^n P_i$ is not contained in I, which proves the first part.

ii. Let K be the field of fractions of R, and note that $R \subseteq P^{-1} = \{\alpha \in K \mid \alpha P \subseteq R\}$. We claim that the inclusion is proper. Let $0 \neq a \in P$ and apply part (i) to $I = (a)$. Thus $A = \{b \in K \mid bP \subseteq I\}$ is an ideal of R containing (a) properly and $AP \subseteq (a)$. Then $a^{-1} \in K$ and $a^{-1}AP \subseteq a^{-1}aR = R$, whence $a^{-1}A \subseteq P^{-1}$. Moreover, $a^{-1} \notin R$ since $a \in P \subsetneq R$, i.e. $a \notin R^\times$. Hence $P^{-1} \not\subseteq R$.

   So, $P \subseteq PP^{-1} \subseteq R$, with $P \in \mathrm{MaxSpec}(R)$. Therefore, either $PP^{-1} = P$, or $PP^{-1} = R$, since PP^{-1} is an ideal of R. We prove that $PP^{-1} \neq P$. Suppose the contrary, i.e. $PP^{-1} = P$. In this case, P^{-1} is a subring of K containing R, since closed under multiplication: for $\alpha, \beta \in P^{-1}$, then $\alpha\beta P \subseteq \alpha P^{-1} P = \alpha P \subseteq R$, i.e. $\alpha\beta \in P^{-1}$.

   Since R is Noetherian and P^{-1} a fractional ideal of R, the R-module P^{-1} is finitely generated by Remark 3.21. By Proposition 3.2, P^{-1} is an integral ring extension of R, but R is integrally closed in K and therefore we would have $R = P^{-1}$, a contradiction. Therefore, $PP^{-1} = R$, as required.

iii. Note that $1 \in II^{-1} = R$. So write $1 = \sum_{i=1}^{n} a_i x_i$, with $a_i \in I$ and $x_i \in I^{-1}$ for all i. We claim that $I = (a_1, \ldots, a_n)$. Let $b \in I$. Then

$$b = b1 = b\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} (bx_i)a_i, \quad \text{with} \quad bx_i \in II^{-1} = R, \; \forall\, 1 \leq i \leq n.$$

□

Dedekind domains can be seen as a generalisation of UFDs, in the sense that they satisfy a theorem of existence and uniqueness of a factorisation into prime ideals, instead of elements.

Theorem 3.23. *Let R be a Dedekind domain, and let I be a proper nonzero ideal of R. Then, there exist finitely many maximal ideals $P_1, \ldots, P_n$ of R, and positive integers $e_1, \ldots, e_n$ such that*

$$I = \prod_{i=1}^{n} P_i^{e_i}. \tag{2}$$

Furthermore, $\{P_1, \ldots, P_n\}$ and $\{e_1, \ldots, e_n\}$ are uniquely determined by I.

Proof. We start by showing the existence of such a factorisation. We proceed by contradiction. Let I be a nonzero proper ideal of R which does not possess a factorisation as in (2) and choose I maximal with respect to inclusion. That is, for any proper ideal J of R with $I \subsetneq J$, then J has a factorisation into a product of maximal ideals of R.

Note that $I \notin \operatorname{Spec}(R)$ and I is a proper ideal of R. Therefore, I is contained in some maximal ideal, say P. By the proof of Lemma 3.22(ii), P is invertible and $PP^{-1} = R \subsetneq P^{-1}$. So

$$I = IR = IPP^{-1} \subseteq PP^{-1} = R, \quad \text{and, by Lemma 3.22(i)}, \quad I \subsetneq IP^{-1} \quad \text{is an ideal of } R.$$

(Note that $IP^{-1} = \{a \in R \mid aP \subseteq I\}$.)

By maximality of I in our assumption, the ideal IP^{-1} has a factorisation $IP^{-1} = \prod_{i=1}^{n} P_i^{e_i}$ into maximal ideals of R. Thus, using the commutativity of R and Equation (2),

$$I = IR = IP^{-1}P = \big(\prod_{i=1}^{n} P_i^{e_i}\big)P$$

is a factorisation of I into a product of maximal ideals of R, a contradiction with our assumption. Therefore, every proper nonzero ideal of R has a factorisation into a product of maximal ideals of R.

To prove the uniqueness of the factorisation, we proceed by induction on $m = m_I = \sum_{i=1}^{n} e_i$, where the e_i are defined by I as in Equation (2). Equivalently, we can write Equation (2) as a product over all $P \in \operatorname{MaxSpec}(R)$, setting $e_P = 0$ for all but finitely many P.

If $m = 1$, then there is nothing to show since $I = P$ is prime.

Suppose $m > 1$. Choose $Q \in \operatorname{MaxSpec}(R)$ such that $e_Q > 0$, and note that, as above, $QQ^{-1} = R$. Moreover, $I \subsetneq Q$ and, since maximal ideals are invertible, we have $QP \subsetneq P$ for $P \in \operatorname{MaxSpec}(R)$. By Equation (2),

$$IQ^{-1} = \big(\prod_{P \in \operatorname{MaxSpec}(R)} P^{e_P}\big)Q^{-1} = \prod_{P \in \operatorname{MaxSpec}(R)} P^{e'_P}, \quad \text{where}$$

$e'_P = \begin{cases} e_P & \text{if } P \neq Q \\ e_Q - 1 & \text{for } P = Q. \end{cases}$ Hence, $m_{IQ^{-1}} < m$, and by induction, we conclude that the factorisation of IQ^{-1} is unique. It follows that the factorisation of I is unique too.

□

3.5 Exercises

Exercise 3.1. i. Let $f \in \mathbb{Z}[x]$ and let $\frac{a}{b} \in \mathbb{Q}$, in reduced form, such that $f(\frac{a}{b}) = 0$. Prove that b divides the leading coefficient of f and that a divides the constant term

ii. Deduce from it that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Exercise 3.2. Let $z = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ and let $R = \mathbb{Z}[z]$. Prove that R is integrally closed in $\mathbb{Q}[z]$.

Exercise 3.3. i. Prove that $\sqrt{2} + \sqrt{3} \in \mathbb{R}$ is integral over $\mathbb{Z}$.

ii. Find its *minimal polynomial* in $\mathbb{Q}[x]$, that is, the unique monic irreducible polynomial $f \in \mathbb{Q}[x]$ such that $f(\sqrt{2} + \sqrt{3}) = 0$.

Exercise 3.4. Let R be a subring of a commutative ring S and suppose that S is integral over R. Is the contraction map $c : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ injective? surjective? Prove your claims.

Exercise 3.5. Let R be an ID with field of fraction F, and let U be a multiplicative subset of R.

i. Suppose that R is integrally closed. Prove that R_U is integrally closed in F too.

ii. Suppose that R_P is integrally closed for every $P \in \mathrm{MaxSpec}(R)$. Prove that R is integrally closed.

Exercise 3.6. Let R be a subring of a commutative ring S and let M be an R-submodule of S. Suppose that $1 \in M$.

i. Prove that M is faithful as an R-module. That is, $aM = 0$ implies $a = 0$ for all $a \in R$.

ii. Suppose that M is an R-algebra. Prove that M is faithful as an R-algebra.

Exercise 3.7. Prove Corollary 3.9: *Let R be a subring of a commutative ring S and let I be a prime ideal of S. Suppose that S is integral over R. Then I is maximal in S if and only if I^c is maximal in R.*

Exercise 3.8. Let k be a field and let $R = k[x, y]$. Calculate I^{-1} where $I = (x, y)$, and prove that $(I^{-1})^{-1} \neq I$.

Exercise 3.9. Let R be a Dedekind domain with field of fractions K, and let M_1, M_2 be fractional ideals of R. Prove the following.

i. Every nonzero ideal of R is fractional.

ii. The sum $M_1 + M_2$ and the product

$$M_1 M_2 = \{\sum_{i=1}^{n} \frac{a_i}{b_i}\frac{c_i}{d_i} \mid \frac{a_i}{b_i} \in M_1,\ \frac{c_i}{d_i} \in M_2,\ n \in \mathbb{N}\} \quad \text{are fractional ideals of } R.$$

iii. M_1^{-1} is a fractional ideal of R.

iv. If $M_1 M_2 = R$, then $M_2 = M_1^{-1}$.

v. The set of invertible fractional ideals of R forms an abelian multiplicative group with multiplicative identity R.

Exercise 3.10. Let R be a Dedekind domain and let U be a multiplicative subset of R. Prove that R_U is Dedekind too.

Exercise 3.11. Let $\mathbb{Z}[t^2] = R \subseteq S = \mathbb{Z}[t, \sqrt{3}]$. Apply the going-up theorem to find chains of prime ideals in S lifting the following chains in R. In each case describe the inclusions $R/P_1 \hookrightarrow S/Q_1$ and $R/P_2 \hookrightarrow S/Q_2$.

(i) $0 \subseteq (13) \subseteq (t^2 - 1, 13)$.

(ii) $0 \subseteq (t^2 - 1) \subseteq (t^2 - 1, 13)$.

(iii) $0 \subseteq (t^2 + 1) \subseteq (t^2 + 1, 13)$.

(iv) $0 \subseteq (t^2) \subseteq (t^2, 13)$.

Exercise 3.12. Let R be a subring of a commutative ring S and let I, I' and J, J' be ideals of R and of S, respectively. Prove the following

i. If $J \subseteq J'$, then $J^c \subseteq J'^c$.

ii. If $I \subseteq I'$, then $I^e \subseteq I'^e$.

iii. $I \subseteq I^{ec}$ and $J^{ce} \subseteq J$.

iv. $I^{ece} = I^e$ and $J^{cec} = J^c$.

Exercise 3.13. Let R be a Dedekind domain. Prove that a fractional ideal is invertible if and only if it is projective.

4 Prime and maximal ideal spectra

Let R be a commutative ring. We define and study topological spaces whose underlying sets are the sets of prime and of maximal ideals of R, respectively $\mathrm{Spec}(R)$, the *prime ideal spectrum* of R, and $\mathrm{MaxSpec}(R)$, the *maximal ideal spectrum* of R.

We begin this section with a brief review of the relevant topological background for our purposes.

Definition 4.1. A *topological space* is a set X together with a collection $\mathcal{C}$ of subsets of X, called a *topology*, subject to the following axioms:

i. $\emptyset$ and X are in $\mathcal{C}$.

ii. Let $\{C_i,\ i \in I\} \subseteq \mathcal{C}$, where I is any indexing set. Then $\bigcap_{i \in I} C_i$ is in $\mathcal{C}$.

iii. Let $C, C' \in \mathcal{C}$, then $C \cup C'$ is in $\mathcal{C}$.

The elements of $\mathcal{C}$ are the *closed sets* of X. The complement of a closed set is an *open set*. The elements of X are called *points*. If $x \in X$, a *neighbourhood* of x is an open set containing x.

A topology is often defined using open sets instead of closed ones, but in the context of the Zariski topology, it is more convenient to define it using closed sets. The axioms defining a topology on X using a class of open sets $\mathcal{O}$ instead of closed sets are adjusted accordingly:

i. $\emptyset$ and X are in $\mathcal{O}$.

ii. Let $\{U_i,\ i \in I\} \subseteq \mathcal{O}$, where I is any indexing set. Then $\big(\bigcup_{i \in I} U_i\big) \in \mathcal{O}$.

iii. Let $U, U' \in \mathcal{O}$, then $(U \cap U') \in \mathcal{O}$.

In general, subsets of a topological space are neither closed, nor open, while some sets can be *clopen*, i.e. open and closed (e.g. $\emptyset$ and the whole set). The *closure* of a subset $Y \subseteq X$ is the smallest closed set $\overline{Y}$ containining Y, i.e.

$$\overline{Y} = \bigcap_{C \in \mathcal{C},\ Y \subseteq C} C.$$

Note that, for all $C, Y \subset X$,

- Y is closed if and only if $Y = \overline{Y}$
- If $Y \subseteq C = \overline{C}$, then $\overline{Y} \subseteq \overline{C}$.

A subset Y of X is *dense* if $\overline{Y} = X$.

A set can be endowed with different topologies.

Example 4.2. The set $\mathbb{R}$ of real numbers is a topological space for at least three distinct topologies:

i. The *trivial* topology, with $\mathcal{C} = \{\emptyset, X\}$.

ii. The *discrete* topology, with $\mathcal{C} = \mathcal{P}(\mathbb{R})$: every subset is clopen.

iii. The *standard* (or usual) topology. This is the topology commonly defined by taking the set of open sets to be arbitrary disjoint unions of open intervals. That is, $U \subseteq \mathbb{R}$ is open if and only if for all $x \in U$, there exists $\varepsilon > 0$ such that $(x - \varepsilon, x + \varepsilon) \subseteq U$.

We refer to [G. Bredon, *Topology and geometry*, Graduate Texts in Mathematics, 139, Springer, 1993] for the background on topology topology.

4.1 Zariski topology

Let R be a commutative ring. In this section, we define a topology on $\mathrm{Spec}(R)$. For this, we identify a collection of closed subsets of $\mathrm{Spec}(R)$. By definition, the *points* of $\mathrm{Spec}(R)$ (as a topological space) are the prime ideals of R.

Definition 4.3. Let R be a commutative ring and let X be a subset of R. We define the set

$$V(X) := \{P \in \mathrm{Spec}(R) \mid X \subseteq P\}.$$

For instance,

i. $V(\{0\}) = V(\emptyset) = \mathrm{Spec}(R)$.

ii. $V(R^\times) = \emptyset$.

iii. $V(P) = \{P\}$ if and only if $P \in \mathrm{MaxSpec}(R)$. In other words, the closed points of $\mathrm{Spec}(R)$ are the maximal ideals of R.

iv. $X \subseteq Y \subseteq R$ implies $V(Y) \subseteq V(X)$. That is, the function $V : \mathcal{P}(R) \to \mathcal{P}(\mathrm{Spec}(R))$ is an order reversing function from the power set of R to that of $\mathrm{Spec}(R)$.

Note that if X is a subset of R, then $V(X) = V((X))$, where (X) is the ideal generated by X.

Proposition 4.4. *Let $\{X_s,\ s \in S\}$ be a collection of subsets of R and let I, J be ideals of R, where S is any indexing set. Then $V(\bigcup_{s\in S} X_s) = \bigcap_{s\in S} V(X_s)$ and $V(I \cap J) = V(I) \cup V(J)$.*

The collection $\mathcal{C} = \{V(X) \mid X \subset R\}$ defines a topology on $\mathrm{Spec}(R)$, called the Zariski topology*: $\mathcal{C}$ is the collection of closed subsets of $\mathrm{Spec}(R)$.*

The closure of a subset $X \subseteq \mathrm{Spec}(R)$ is $\overline{X} = V(X)$. In particular, $\overline{(0)} = \mathrm{Spec}(R)$, since every prime ideal contains the zero ideal, and $\overline{\{P\}} = \{P\}$ if and only if $P \in \mathrm{MaxSpec}(R)$.

Proof of Proposition 4.4. We check the axioms of a topology to prove that $\mathcal{C}$ defines a topology on $\mathrm{Spec}(R)$.

i. As noted above, $\emptyset = V(\{1\})$ and $\mathrm{Spec}(R) = V(\emptyset)$.

ii. Let $\{X_s,\ s \in S\}$ be a collection of subsets of R, where S is any indexing set. Then,

$$\begin{aligned} V\big(\bigcup_{s\in S} X_s\big) &= \{P \in \mathrm{Spec}(R) \mid P \supseteq X_s,\ \forall\, s \in S\} \\ &= \bigcap_{s\in S} \{P \in \mathrm{Spec}(R) \mid P \supseteq X_s\} = \bigcap_{s\in S} V(X_s). \end{aligned}$$

So, the intersection of an arbitrary collection of elements in $\mathcal{C}$ is an element of $\mathcal{C}$.

iii. Since $V(X) = V((X))$ for any $X \subset R$, any element of $\mathcal{C}$ can be represented as $V(I)$ for some ideal I. So, let I, J be ideals of R. Then

$$\begin{aligned} V(I \cap J) &= \{P \in \mathrm{Spec}(R) \mid I \cap J \subseteq P\} \\ &= \{P \in \mathrm{Spec}(R) \mid I \subseteq P\} \cup \{P \in \mathrm{Spec}(R) \mid J \subseteq P\} = V(I) \cup V(J), \end{aligned}$$

where the second equality follows from the fact that P is prime (see Exercise 1.12). That is, the union of two elements of $\mathcal{C}$ is an element of $\mathcal{C}$.

□

Given a topological space X, a subset $Y \subseteq X$ is a topological space for the *subspace topology*: If $\mathcal{C}$ is the collection of closed sets of X, then $\{C \subseteq Y \mid \exists\, D \in \mathcal{C} \text{ with } C = D \cap Y\}$ is the collection of closed sets of Y. (Similarly if the topology is given by the collection of open sets of X.) For instance, $\mathrm{MaxSpec}(R)$ is a topological space for the subspace topology of $\mathrm{Spec}(R)$. To specify the subspace topology, we write

$$V_{\max}(A) = \{P \in \mathrm{MaxSpec}(R) \mid A \subseteq P\}.$$

The open sets of $\mathrm{Spec}(R)$ are the arbitrary unions of sets of the form

$$U_X \stackrel{\text{def}}{=} \mathrm{Spec}(R) \setminus V(X) = \mathrm{Spec}(R) \setminus \big(\bigcap_{a \in X} V(a) \big) = \bigcup_{a \in X} \mathrm{Spec}(R) \setminus V(a).$$

In particular, $U_a = \{P \in \mathrm{Spec}(R) \mid a \notin P\}$, for $a \in R$.

Corollary 4.5. *Let $\mathcal{O}$ denote the set of open sets of $\mathrm{Spec}(R)$. The function $\theta : R \to \mathcal{O}$, defined by $\theta(a) = U_a$ satisfies the following properties:*

i. $U_{ab} = U_a \cap U_b$ *for all* $a, b \in R$.

ii. $U_a = \emptyset \iff a \in \mathrm{Nil}(R)$, *i.e. if and only if* a *is nilpotent.*

iii. $U_a = \mathrm{Spec}(R) \iff a \in R^\times$.

Proof. i. If $P \in \mathrm{Spec}(R)$ contains ab, then at least one of a or b is in P, by definition of a prime ideal. So $ab \notin P$ if and only if $a \notin P$ and $b \notin P$.

ii. $U_a = \emptyset$ if and only if a is in every prime ideal.

iii. $U_a = \mathrm{Spec}(R)$ if and only if a is not contained in any prime ideal, i.e if and only if $aR = R$.

□

Lemma 4.6. *Let $Y \subseteq \mathrm{Spec}(R)$ and let*

$$D_Y = \bigcap_{P \in Y} P$$

be the intersection of all the prime ideals contained in Y. Then $V(D_Y) = V(Y)$ is the closure of Y in $\mathrm{Spec}(R)$ for the Zariski topology.

Proof. By definition, D_Y is an ideal of R, and $V(D_Y) = \{P \in \mathrm{Spec}(R) \mid P \supseteq \bigcap_{Q \in Y} Q\}$. Note that $Y \subseteq V(D_Y)$ since $P \in V(D_Y)$ for all $P \in Y$. Since $V(D_Y)$ is a closed set of $\mathrm{Spec}(R)$, we have $V(Y) \subseteq V(D_Y)$.

To show that $V(D_Y)$ is the smallest closed set of $\mathrm{Spec}(R)$ containing Y, suppose that $X \subseteq R$ is such that $Y \subseteq V(X)$. That is,

$$P \in V(X),\ \forall\, P \in Y \iff P \supseteq X,\ \forall\, P \in Y \iff \bigcap_{P \in Y} P \supseteq X \iff D_Y \supseteq X \iff V(D_Y) \subseteq V(X)$$

since the mapping $V(-)$ is order reversing. Therefore any closed subset of $\mathrm{Spec}(R)$ containing Y must contain $V(D_Y)$, and $V(Y) = V(D_Y)$.

□

The *morphisms* in the category of topological spaces are the continuous maps. A function $f : X \to Y$ between topological spaces is *continuous* if the preimage $f^{-1}(U)$ of any open set U of Y by f is an open set of X, or equivalently the preimage of any closed set of Y is closed in X. Note that, if $U \subseteq Y$ is open, then $f^{-1}(Y \setminus U) \cap f^{-1}(U) = \emptyset$, since any element x in such intersection would have $f(x) \in ((Y \setminus U) \cap U) = \emptyset$. Hence $f^{-1}(Y \setminus U) = X \setminus f^{-1}(U)$.

A *homeomorphism* of topological spaces X and Y is a continuous bijective map $f : X \to Y$ with continuous inverse.

Example 4.7. The identity map $\mathrm{Id} : \mathbb{R}_{dis} \to \mathbb{R}$, where the codomain is $\mathbb{R}$, with the usual topology, and the domain is $\mathbb{R}_{dis}$, with the discrete topology, is a continuous bijection, but not a homeomorphism.

Proposition 4.8. *Let R be a commutative ring and let $\pi : R \to R/N$ be the quotient map, where $N = \mathrm{Nil}(R)$. Then π induces a homeomorphism between the prime ideal spectra, $\pi_* : \mathrm{Spec}(R) \to \mathrm{Spec}(\overline{R})$, where $\pi_*(P) = \pi(P)$ for $P \in \mathrm{Spec}(R)$.*

Proof. Note that π_* is well defined since $\pi(P) \in \mathrm{Spec}(R/N)$ for all $P \in \mathrm{Spec}(R)$, by surjectivity of π. Moreover, π_* is bijective since $N = \mathrm{Nil}(R)$ is contained in every prime ideal of R, implying that the prime ideals of R/N and of R are in 1-1 correspondence.

To prove continuity of π_* and π_*^{-1}, note that, for a subset $A \subseteq R$, we have

$$\pi_*(V(A)) = \{P/N \in \mathrm{Spec}(R/N) \mid P \in V(A)\} = \{\pi(P) \mid P \in \mathrm{Spec}(R),\ P \supseteq A\} = V(\pi(A)),$$

since $N \subseteq P$ for all $P \in \mathrm{Spec}(R)$. Hence, π_* maps closed sets to closed sets. Moreover, $\pi_*^{-1}(V(\pi(A))) = \pi_*^{-1}(\pi_*(V(A))) = V(A)$, showing that π_*^{-1} maps closed sets to closed sets too. □

4.2 Idempotents of R and connectedness of $\mathrm{Spec}(R)$

Definition 4.9. A topological space X is *connected* if X cannot be written as the disjoint union of two nonempty open sets. Equivalently, X is connected if the only clopen sets of X are X and $\emptyset$. If X is not connected, we say that X is *disconnected*.

We will prove in Theorem 4.12 how connectedness of $\mathrm{Spec}(R)$ (as a toplogical space with the Zariski topology) relates to the idempotents in R, which can lead to useful insights about R. For instance, A. Dress proved in [A. Dress, *A characterization of solvable groups*, Math Z. **110** (1969), 213–217] that the prime ideal spectrum of the Burnside ring of a finite group G is connected if and only if G is soluble.

The objective of this section is to prove that $\mathrm{Spec}(R)$ is disconnected if and only if R contains an idempotent different from $0, 1$. An *idempotent* of R is an element $e \in R$ such that $e^2 = e$. For instance $(0, 1) \in \mathbb{Z} \oplus \mathbb{Z}$ is an idempotent.

Recall from Definition 1.7 that a *nil* ideal is an ideal whose elements are all nilpotent.

Proposition 4.10. *Let R be a commutative ring, and let I be a nil ideal of R. Let $\pi : R \to \overline{R} = R/I$ be the quotient map, and let us denote $\overline{X} = \pi(X)$ for any subset or element of R. Suppose that $\overline{f} \in \overline{R}$ is an idempotent of $\overline{R}$. Then there exists a unique idempotent $e \in R$ such that $\overline{e} = \overline{f}$.*

Proof. Let $f \in \pi^{-1}(\overline{f})$. Thus, $f^2 - f \in \ker(\overline{(-)}) = I$, and so there exists $n \in \mathbb{N}$ such that $(f^2 - f)^n = 0$. Now, $(f + 1)(f^2 - f) = f^3 - f \in I$, since I is an ideal. Inductively, for $m \geq 2$,

$$\sum_{i=0}^{m-2} f^i(f^2 - f) = f^m - f \in I, \quad \text{and so } f^m - f \in I \text{ for all } m \in \mathbb{N}.$$

From the equalities

$$0 = (f - f^2)^n = \big(f(1 - f)\big)^n = f^n(1 - f)^n \quad \text{and} \quad 1 = f + (1 - f)$$

we deduce that

$$1 = 1^{2n-1} = (f + (1-f))^{2n-1} = \sum_{i=0}^{2n-1} \binom{2n-1}{i} f^i (1-f)^{2n-i-1}. \tag{3}$$

Put

$$\begin{aligned} e_1 &= \sum_{i=0}^{n-1} \binom{2n-1}{i} f^i (1-f)^{2n-i-1} \quad \text{and} \\ e_2 &= \sum_{i=n}^{2n-1} \binom{2n-1}{i} f^i (1-f)^{2n-i-1}, \quad \text{giving} \\ 1 &= e_1 + e_2. \end{aligned}$$

Moreover, $e_1 e_2 = 0$, since each term in the product of the sums is a multiple of $f^n(1-f)^n = 0$. It follows that $e_1^2 = e_1(1-e_2) = e_1 - e_1 e_2 = e_1$, and similarly, $e_2^2 = e_2$.

Note also that every term of the sum in Equation (3) is a multiple of $(f^2 - f)$, except for the indices $i = 0$, where it is $(1-f)^{2n-1}$, and $i = 2n-1$, where it is f^{2n-1}. Hence, $(1-f)^{2n-1} - e_1,\ f^{2n-1} - e_2 \in I$ since $(f^2 - f) \in I$.

Putting these remarks together, given that $f^m - f \in I$ for all $m \in \mathbb{N}$ and $f^{2n-1} - e_2 \in I$, we obtain $f - e_2 \in I$, and so $\overline{e_2} = \overline{f}$. Therefore $e = e_2$ is an idempotent of R satisfying $\overline{e} = \overline{f}$. It remains to prove the uniqueness.

Since $I = \ker(\pi)$, we have the preimage $\pi^{-1}(\overline{f}) = e + I \subseteq R$. Let $y \in I$ such that $(e+y)^2 = e + y$. Since $e^2 = e$, this gives $y^2 + 2ey = y$, or equivalently, $y^2 = y(1-2e)$. Thus $y^3 = y^2(1-2e) = y(1-2e)^2$. Now, $(1-2e)^2 = 1 - 4e + 4e = 1$, and so $y^3 = y$. Since I is nil, y is nilpotent, but since $y^3 = y$, we must have $y = 0$, showing the uniqueness of e.

□

Remark 4.11. The existence of lift of idempotents in Proposition 4.10 does not require R to be commutative, since for any $a \in R$, for any ring R, we have $a(1-a) = (1-a)a$. The commutativity of R is only required to show the uniqueness of a lift $e \in R$ of an idempotent $\overline{f} \in \overline{R}$, see [Jac, Proposition 7.14, vol II].

As observed above, the open sets of $\mathrm{Spec}(R)$ are the complements of closed sets, i.e. unions of sets of the form $U_X = \mathrm{Spec}(R) \setminus V(X)$. In particular, $U_a = \{P \in \mathrm{Spec}(R) \mid a \notin P\}$, for $a \in R$. We consider the case when such open set is defined by an idempotent.

Theorem 4.12. *Let R be a commutative ring and let $e = e^2 \in R$ be an idempotent. Then U_e is a clopen set in $\mathrm{Spec}(R)$ (for the Zariski topology). Moreover, every clopen set is of this form, and the map $e \mapsto U_e$ is a bijection from the set of idempotents of R to the set of clopen subsets of $\mathrm{Spec}(R)$.*

In particular, $\mathrm{Spec}(R)$ is connected if and only if the only idempotents of R are $0, 1$.

For instance, $\mathrm{Spec}(\mathbb{Z} \oplus \mathbb{Z}) = U_{(0,1)} \sqcup U_{(1,0)} = \{\mathbb{Z} \oplus (p) \mid\ p \text{ prime}\} \sqcup \{(p) \oplus \mathbb{Z} \mid\ p \text{ prime}\}$. Note in this example that $(1,0) = 1_{\mathbb{Z}\oplus\mathbb{Z}} - (0,1)$ and that the union is disjoint.

Proof. Since $e(1-e) = e - e^2 = 0$ and $e + (1-e) = 1$, if $P \in \mathrm{Spec}(R)$, then P contains exactly one of e or $1-e$. So, $\mathrm{Spec}(R) = U_e \sqcup U_{(1-e)}$ is the disjoint union of two nonempty clopen sets.

It remains to show that every clopen set is of the form U_e for some unique idempotent $e = e^2 \in R$. We first prove the existence of such e. Now, $\emptyset = U_0$ and $\mathrm{Spec}(R) = U_1$, with $0, 1$ idempotents of R.

Let $\emptyset \neq V \subsetneq \mathrm{Spec}(R)$ be a clopen set, and let $V' = \mathrm{Spec}(R) \setminus V$. Let $\pi : R \to R/N$ be the quotient map, where $N = \mathrm{Nil}(R)$. By Proposition 4.8, π induces a homeomorphism $\pi_* : \mathrm{Spec}(R) \to \mathrm{Spec}(R/N)$. For convenience, and since that should not cause any confusion, we write π instead of π_*. Since π is a homeomorphism $\pi(V)$ is a clopen set in $\mathrm{Spec}(R/N)$ with complement $\mathrm{Spec}(R/N) \setminus \pi(V) = \pi(V')$.

Consider the ideals of R/N

$$D = D_{\pi(V)} = \bigcap_{P \in V} P/N \quad \text{and} \quad D' = D_{\pi(V')} = \bigcap_{P \in V'} P/N.$$

Then $V(D) = \{P/N \in \operatorname{Spec}(R/N) \mid D \subseteq P/N\} = \pi(V)$ and $V(D') = \pi(V')$, since $\pi(V)$ and $\pi(V')$ are closed.

Suppose that there exists $P/N \in \operatorname{Spec}(R/N)$ such that $P/N \supseteq D \cup D'$. The inclusion $D \subseteq P/N$ implies that $P/N \in V(D) = \pi(V)$, and similarly, $P/N \in \pi(V')$. But then, $P/N \in \pi(V) \cap \pi(V') = \emptyset$, which is impossible. Therefore, no prime ideal of R/N contains $D \cup D'$, implying that $(D \cup D') = R/N$ is improper.

Since $\pi(V') = \operatorname{Spec}(R/N) \setminus \pi(V)$, any prime ideal of R/N must lie in exactly one of $\pi(V)$ or $\pi(V')$, and so contain exactly one of D or D'. So, for all $P/N \in \operatorname{Spec}(R/N)$, then $(D \cap D') \subseteq P/N$. For this inclusion to hold for all prime ideals, we must have $D \cap D' \subseteq \operatorname{Nil}(R/N) = (0)$, since R/N is reduced, by Exercise 1.18. Hence $R/N = D \cup D' = D \oplus D'$. It follows that there exists $f \in D$ such that $1 = f + (1-f) \in R/N$ and $(1-f) \in D'$. Since $f(1-f) \in D \cap D' = (0)$, we have $f(1-f) = 0$. Together with the equality $1 = f + (1-f)$, we conclude that $D = fR/N$ and $D' = (1-f)R/N$. Moreover $f + (1-f) = 1 = 1^2 = (f + (1-f))^2 = f^2 + (1-f)^2$, with $f, f^2 \in D$ and $(1-f), (1-f)^2 \in D'$. Therefore $f^2 = f$, $(1-f)^2 = (1-f)$ are the multiplicative identity elements of D and D', respectively. By Proposition 4.10, there exists a unique idempotent $e \in R$ such that $\pi(e) = f$.

If I is an ideal of R, then $e \in I$ if and only if $f \in \pi(I)$, if and only if $\pi(I) \supseteq D = fR/N$. In particular $P \in \operatorname{Spec}(R)$ contains e if and only if $\pi(P) \in V(D) = \pi(V)$, if and only if $P \in V$. In other words, $P \in U_{(1-e)} \iff e \in P \iff P \in V$, and it follows that $V = U_{(1-e)}$. By symmetry, $V' = U_e$.

It remains to prove the uniqueness of the idempotent $e \in R$. That is $U_e \neq U_{e'}$ for any two distinct idempotents e, e'. As above, write $R/N = D \oplus D' = fR/N \oplus (1-f)R/N$, with $f = \pi(e)$. By definition,

$$\begin{aligned}
\pi(U_e) &= \{\pi(P) \in \operatorname{Spec}(R/N) \mid f \notin \pi(P)\} \\
&= \{\pi(P) \in \operatorname{Spec}(R/N) \mid 1 - f \in \pi(P)\} \\
&= \{\pi(P) \in \operatorname{Spec}(R/N) \mid (1-f)R/N \subseteq \pi(P)\},
\end{aligned}$$

and similarly, $\pi(U_{1-e}) = \{\pi(P) \in \operatorname{Spec}(R/N) \mid fR/N \subseteq \pi(P)\}$.

Therefore, $D_{\pi(U_e)} \supseteq (1-f)R/N$ and $D_{\pi(U_{1-e})} \supseteq fR/N$. But since $R/N = fR/N \oplus (1-f)R/N$, we must have $fR/N = D_{\pi(U_e)}$ and $(1-f)R/N = D_{\pi(U_{1-e})}$. Hence, by Proposition 4.10, e and $1-e$ are the unique idempotents in $\pi^{-1}(f)$ and in $\pi^{-1}(1-f)$, respectively. The result follows.

□

4.3 Exercises

Exercise 4.1. Find $V(1176) \subseteq \operatorname{Spec}(\mathbb{Z})$.

Exercise 4.2. Let $R = \mathbb{Q}[x]$ and let $f = x^3 - 3x^2 + 2x$.

i. Find $V((f))$.

ii. Let $I = (x^2 + 1)$ and set $\overline{R} = R/I$. Find $V((\overline{f})) \subseteq \operatorname{Spec}(\overline{R})$.

Exercise 4.3. Let $R = \mathbb{Z} \times \mathbb{Z}/42$. Find all the idempotents of R.

Exercise 4.4. A *basis* of a topological space X is a subset $\mathcal{B}$ of the collection of open sets of X such that any open set is the union of a subset of $\mathcal{B}$. For instance, a basis for the usual topology on $\mathbb{R}$ is the set of all open intervals of $\mathbb{R}$. The space X is *Hausdorff* if given any two distinct points $x, y \in X$, there exist open neighbourhoods U_x and U_y of x and y, respectively, with $U_x \cap U_y = \emptyset$. The space X is *compact* if, given any collection $\{U_i,\ i \in I\}$ of open sets of X such that $X = \bigcup_{i \in I} U_i$, there exists a

finite subset $J \subseteq I$ such that $X = \bigcup_{j \in J} U_j$. (In some textbooks, this is the definition of *paracompact* or *quasi-compact*, whilst compact means paracompact Hausdorff. We follow [G. Bredon, *Topology and geometry*, Graduate Texts in Mathematics 139, Springer, 1993; Definition I.7.2].)

i. Find a basis of $\mathrm{Spec}(R)$ for any commutative ring R.

ii. Prove that $\mathrm{Spec}(R)$ is compact for any commutative ring R.

iii. Find an example of R such that $\mathrm{Spec}(R)$ is Hausdorff.

iv. Find an example of R such that $\mathrm{Spec}(R)$ is not Hausdorff.

Exercise 4.5. Let $R = k[x]$ where k is a field. Prove that there exist proper open subsets U, U' of $\mathrm{Spec}(R)$ such that $\mathrm{Spec}(R) = U \cup U'$.

Exercise 4.6. [Jac, Exercise 7.5.1, vol II] Let $f : R \to S$ be a ring homomorphism with R, S commutative. Suppose that f is surjective. Prove that $\mathrm{im}(f^*) = V(\ker(f))$, where f^* is the induced function $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$, defined by $f^*(P) = f^{-1}(P)$ for $P \in \mathrm{Spec}(S)$. (The map f^* defines a homeomorphism $\mathrm{Spec}(S) \to V(\ker(f))$.

Exercise 4.7. [Jac, Exercise 7.5.4, vol II] Let R be a commutative ring and let $P \in \mathrm{Spec}(R)$. Consider the ideal $I = \big(\{e = e^2 \in P\}\big)$ generated by the idempotents of R lying in P.

i. Prove that the only idempotents of R/I are $0, 1$.

ii. Prove that the prime ideals containing I form the connected component of $\mathrm{Spec}(R)$ containing P.

Exercise 4.8. [Isa, Lemma 14.7] Let R be a commutative ring and let I be a minimal ideal of R. That is, $I \neq 0$ and the only ideals of R contained in I are 0 and I. Suppose that $I^2 \neq 0$. Prove that there exists an idempotent $e \in R$ such that $I = Re$.

Exercise 4.9. Let R be a commutative ring and let I be an ideal of R. The *I-adic topology* on an R-module M is defined by taking as open sets the unions of the subsets of M of the form $U_{x,n} = x + I^n M$ for $x \in M$ and $n \in \mathbb{N}$.

i. Prove that the collection $\{U_{x,n} \mid x \in M,\ n \in \mathbb{N}\}$ defines a topology on M.

ii. Suppose that R is Noetherian, that $I = \mathrm{Rad}(R)$ and that M is finitely generated. Prove that the I-adic topology on M is Hausdorff (cf. Exercise 4.4).

iii. Prove that the I-adic topology on M is Hausdorff if and only if $\bigcap_{n \in \mathbb{N}} I^n M = 0$ for any countable intersection.

iv. Let $R = M = \mathbb{Z}$ and let $I = (p)$, where p is prime. Prove that the (p)-adic topology on $\mathbb{Z}$ is compact Hausdorff.

5 A brief taste of algebraic geometry: algebraic sets and Hilbert's Nullstellensatz

In this section, we introduce some concepts of algebraic geometry, building on Section 4. The main result that we will state is Hilbert's Nullstellensatz, which means *zero-locus-theorem* in German. We consider multivariate polynomial rings over a field, and study the correspondence between sets of polynomials and that of their simultaneous zeros, seen as the intersection of graphs in some appropriate space. For instance, if $R = \mathbb{R}[x, y]$, the polynomial $x^2 - y$ corresponds to the set of the real plane $\mathbb{R}^2$ which is the graph of the parabola $y = x^2$, whereas the polynomial $x^2 + y^2 + 1$ gives the emptyset. However, if we use $\mathbb{C}$ instead of $\mathbb{R}$, then the graph of $x^2 + y^2 + 1 = 0$ is a circle of radius i centred at the origin of $\mathbb{C}^2$.

The following definition should be reminiscent of Definition 3.1.

Definition 5.1. Let K be a field extension of the field k.

i. An element $a \in K$ is *algebraic over* k if there exists a nonzero polynomial $f \in k[x]$ such that $f(a) = 0$. The extension K is *algebraic* if every element of K is algebraic over k.

ii. An element of K which is not algebraic over k is called *transcendental* over k. K is a *transcendental field extension* of k if K contains transcendental elements of k. The *transcendence degree* of K over k is the cardinality of a *transcendence basis* of K, i.e. a set $\{u_1, \ldots, u_d\} \subseteq K$ of maximal cardinality that is formed of transcendental elements that are algebraically independent (i.e. there exists no nonzero polynomial $f \in k[x_1, \ldots, x_d]$ such that $f(u_1, \ldots, u_d) = 0$).

iii. The *algebraic closure* of k in K is the subfield of K formed by the elements of K that are algebraic over k.

iv. k is *algebraically closed* if every nonconstant polynomial $f \in k[x]$ has a root in k.

Given any field k, there *exists* a *unique (up to field isomorphism)* field $\overline{k}$ which is an algebraic extension of k and $\overline{k}$ is algebraically closed (cf. [Jac, Section 8.1, vol II]).

Lemma 5.2. *Let R be an ID with field of fractions k, let K be a field extension of k, and let $a \in K$ be an algebraic element over k. Then, there exists $d \in R$ such that da is integral over R.*

Proof. Let $f = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n \in k[x]$ such that $f(a) = 0$. (Without loss, we may assume that the leading coefficient 1.) Let $d \in R$ be a common denominator for $\{b_1, \ldots, b_n\}$. We calculate

$$\begin{aligned} 0 = f(a) = d^n f(a) &= d^n a^n + d^n(b_1 a^{n-1}) + \cdots + d^n(b_{n-1}a) + d^n b_n \\ &= (da)^n + db_1(da)^{n-1} \cdots + d^{n-1}b_{n-1}(da) + d^n b_n. \end{aligned}$$

That is, da is a root of $x^n + db_1 x^{n-1} \cdots + d^{n-1}b_{n-1}x + d^n b_n \in R[x]$, as required.

□

5.1 Algebraic sets

We consider multivariate polynomial rings $k[x_1, \ldots, x_n]$, where k is a field, and we endow k^n with the Zariski topology 'extrapolated' from that on $\mathrm{Spec}(k[x_1, \ldots, x_n])$. This will help us construct a correspondence

$$\{ \text{ ideals of } k[x_1, \ldots, x_n]\} \longleftrightarrow \{ \text{ subsets of } K^n\},$$

where K is an extension field of k. For this, we identify a polynomial $f \in k[x_1, \ldots, x_n]$ with the set of its roots in K^n. For instance, $f = x^2 + y^2 - 1 \in \mathbb{R}[x]$ corresponds to a circle of radius 1 centred at the origin of $\mathbb{R}^2$.

Definition 5.3. Let k be a field and consider the multivariate polynomial ring $k[x_1, \ldots, x_n]$. Let A be a subset of $k[x_1, \ldots, x_n]$, and let K be an extension field of k. Define

$$V_K(A) = \{\mathbf{a} = (a_1, \ldots, a_n) \in K^n \mid f(\mathbf{a}) = 0, \ \forall\ f \in A\} \ \subseteq \ K^n.$$

$V_K(A)$ is the *algebraic set* defined by A over k in K^n. We write $V(A)$ instead of $V_K(A)$ if $k = K$.

Similarly to what we observed in Section 4.1, we have

- $V_K(A) = V_K((A)) = V_K(\sqrt{(A)})$,
- $V_K(\{0\}) = K^n$ and
- $V_K(k[x_1, \ldots, x_n]) = \emptyset$.

Algebraic sets depend on the fields k and K; in particular $V(A) \subseteq V_K(A)$. On the other hand, different subsets of $k[x_1, \ldots, x_n]$ can define the same algebraic set, as can be seen from the first point above. The next observation tells us that it suffices to consider the finite subsets of $k[x_1, \ldots, x_n]$.

Proposition 5.4. *Let k be a field and let $k[x_1, \ldots, x_n]$ be a multivariate polynomial ring. Every algebraic set over k is of the form $V(A)$ for some finite subset A of $k[x_1, \ldots, x_n]$.*

Proof. By Corollary 2.49, $k[x_1, \ldots, x_n]$ is Noetherian. Therefore (A) is finitely generated, say $(A) = (f_1, \ldots, f_m)$ for some $f_i \in k[x_1, \ldots, x_n]$. Hence $V(A) = V((A)) = V(\{f_1, \ldots, f_m\})$. □

The correspondence $V_K(-)$ defines a function from the ideals of $k[x_1, \ldots, x_n]$ to the subsets of K^n. We now define a function going the other way around. We present a slightly simplified version of it, sufficient for our purposes, and leave the full generality to a course in algebraic geometry.

Definition 5.5. Let k be a field and let $R = k[x_1, \ldots, x_n]$ a multivariate polynomial ring. Let $X \subseteq k^n$. Define

$$I(X) = \{f \in R \mid f(\mathbf{a}) = 0 \ \forall\ \mathbf{a} \in X\}.$$

To be precise, we should write $I_k(X)$ instead of $I(X)$, but our abuse of notation should not cause confusion since we consider k only. We call $I(X)$ the *annihilating ideal* of X in R.

We refer to Exercise 5.2 to check that $I(X)$ is indeed an ideal of R. Similarly to what we observed with prime ideals and the Zariski topology on $\mathrm{Spec}(R)$, we record the following:

- $\sqrt{J} \subseteq I(V(J)))$ for any ideal J of $k[x_1, \ldots, x_n]$, since, as observed above, for a subset X of $k[x_1, \ldots, x_n]$, we have $V(\sqrt{(X)}) = V(X)$, and since any $f \in \sqrt{J}$ vanishes on all the points of $V(\sqrt{J})$.
- If $X \subseteq Y \subset k^n$, then $I((Y)) \subseteq I((X))$.

The correspondences

$$\mathcal{P}(k^n) \underset{V(-)}{\overset{I(-)}{\rightleftarrows}} \mathcal{I}(k[x_1, \ldots, x_n])$$

between the subsets of k^n and the ideals of $k[x_1, \ldots, x_n]$ are the basic tools that allow us to think of ideals geometrically: ideals correspond to sets of points in a vector space.

5.2 Towards Hilbert's Nullstellensatz

As noted above, the field of coefficients matters when considering algebraic sets. Ideally, given some polynomial $f \in k[x_1, \ldots, x_n]$, we would like k to contain *all* the roots of f, i.e. to be algebraically closed.

Remark 5.6. Let k be a field. The polynomial ring $k[x]$ contains infinitely many distinct monic irreducible polynomials. If $|k|$ is infinite, then $\{x - a \mid a \in k\}$ is an infinite set of such polynomials, and so this fact is clear. What may be less so is that it is also true if $|k|$ is finite. The proof is similar to the proof of the existence of infinitely many distinct prime numbers (in $\mathbb{Z}$). Indeed, suppose that $f_1, \ldots, f_n \in k[x]$ are distinct monic irreducible polynomials (note that we can assume $n \geq 2$ since $x, x+1$ are two distinct monic irreducible polynomials in any $k[x]$). Set $f = f_1 \cdots f_n + 1 \in k[x]$. By construction, $\gcd(f_i, f) = 1$ for all $1 \leq i \leq n$, and f is monic. Since $k[x]$ is a UFD, f is divisible by some monic irreducible polynomial, necessarily distinct from $f_1, \ldots, f_n$. Hence, no matter how big n is, we always can find another distinct monic irreducible polynomial.

Remark 5.6 is useful to show Zariski's lemma. Recall that a field extension K of k is a k-algebra, see Section 3.1 for the definitions of finite and finitely generated algebras.

Theorem 5.7 (Zariski's lemma)**.** *Let K be an extension field of the field k such that K is a finitely generated k-algebra. Then K is algebraic over k, and hence K is a finite k-algebra. In particular, if $k = \overline{k}$, then $K = k$.*

Proof. We proceed by induction on the minimum number $n \geq 0$ of generators of K as a k-algebra. If $n = 0$, then the assertion holds trivially. Suppose $n \geq 1$. That is, there exists $a_1, \ldots, a_n \in K$ such that $K = k[a_1, \ldots, a_n]$. So K is algebraic over k if and only if a_i is algebraic over k for all i. Suppose this is false, and without loss of generality, assume that a_1 is not algebraic over k. Then, $k[a_1] \cong k[x]$, since a_1 does not satisfy any polynomial equation. The field of fractions $k(a_1)$ of $k[a_1]$ is an intermediary field extension $k \subsetneq k(a_1) \subseteq K$, and $K = \big(k(a_1)\big)[a_2, \ldots, a_n]$ is a finitely generated $k(a_1)$-algebra requiring fewer generators than K. By induction, K is algebraic over $k(a_1)$. By Lemma 5.2, for all $2 \leq j \leq n$, there exists a nonzero $d_j \in k[a_1]$ such that $d_j a_j$ is integral over $k[a_1]$. Let $d = d_2 \cdots d_n$. Then, the elements $da_2, \ldots, da_n$ are integral over $k[a_1]$. It follows that $k[a_1, da_2, \ldots, da_n]$ is integral over $k[a_1]$.

Let $u \in K = k[a_1, \ldots, a_n]$, and consider u as a polynomial in $a_1, \ldots, a_n$ with coefficients in k. Since da_j is integral over $k[a_1]$ for all $2 \leq j \leq n$, there exists $N \in \mathbb{N}$ such that $d^N u \in k[a_1, da_2, \ldots, da_n]$. Then $d^N u$ is integral over $k[a_1]$.

By Proposition 3.5, since $k[a_1]$ is a UFD, it is integrally closed in $k(a_1)$. So $d^N u \in k[a_1]$.

This holds for every $u \in k(a_1)$. Hence, for any monic irreducible polynomial $p \in k[a_1] \cong k[x]$, then $d^N u \in k[a_1]$, where $u = \frac{1}{p}$. But then d^N is divisible by infinitely many distinct irreducible elements by Remark 5.6, which is impossible unless $d = 0$. Therefore, our initial assumption is wrong, and a_1 must be algebraic over k. The result follows.

□

Two immediate consequences of Zariski's lemma are recorded in Corollary 5.8. Recall that every ideal of a ring R is the kernel of some ring homomorphism with domain R.

Corollary 5.8. *Let k be a field, and let R be a finitely generated k-algebra.*

i. Every maximal ideal of R is the kernel of a ring homomorphism $\pi : R \to K$, where K is a finite field extension of k.

ii. Let K be a extension field of k with $k \subseteq K \subseteq R$. Then K is algebraic over k.

Proof. i. Let $J \in \mathrm{MaxSpec}(R)$, and let $\pi : R \to R/J$ be the quotient map. Then R/J is a field since J is maximal.

The composition $k \xrightarrow{\rho} R \xrightarrow{\pi} K$ is injective, where ρ is the injective ring homomorphism defined by $\rho(1_k) = 1_R$. Indeed, $J \cap \mathrm{im}(\rho) = \{0\}$ since the nonzero elements of k are invertible in R and J is proper by assumption. Hence, R/J is a field extension of k which is finitely generated as k-algebra. Therefore R/J is algebraic over k by Zariski's lemma.

ii. Similarly as above, note that if J is a maximal ideal of R, then $J \cap K = \{0\}$, since the nonzero elements of K are invertible in R. The same argument as above shows that we have field extensions $k \subseteq K \subseteq R/J$ for any $J \in \mathrm{MaxSpec}(R)$. By the first part, R/J is algebraic over k, and so K too, by transitivity.

□

We now prove an important and famous result.

Theorem 5.9 (Noether normalisation theorem)**.** *Let $R = k[u_1, \ldots, u_m]$ be a finitely generated k-algebra over a field k with transcendence degree $r \leq m$. Then, there exist transcendental elements $v_1, \ldots, v_r \in R$ that are algebraically independent and such that R is integral over $k[v_1, \ldots, v_r]$.*

Proof. We proceed by induction on $m - r \geq 0$. The result holds if $r = m$ since we then take $v_i = u_i$ for $1 \leq i \leq m$. Suppose $m > r$. By assumption, the u_i's are algebraically dependent, i.e. there exists $f \in R$ such that $f(u_1, \ldots, u_m) = 0$, where $0 \neq f = \sum a_{j_1,\ldots,j_m} x_1^{j_1} \cdots x_m^{j_m} \in k[x_1, \ldots, x_m]$. Let X be the (finite) set of monomials in $x_1, \ldots, x_m$ occurring in f. For every $x_1^{j_1} \cdots x_m^{j_m} \in X$, define the polynomial $j_1 + j_2 t + \cdots + j_m t^{m-1} \in \mathbb{Z}[t]$. The resulting polynomials are pairwise distinct and have at most m roots (counted with multiplicities). Since $\mathbb{Z}$ is infinite, there exists an integer $d \geq 0$ such that the evaluations $j_1 + j_2 d + \cdots + j_m d^{m-1}$ are distinct too.

Now consider $f(x_1, x_1^d + y_2, \ldots, x_1^{d^{m-1}} + y_m) \in k[x_1, y_2, \ldots, y_m]$. We compute

$$\begin{aligned} f(x_1, x_1^d + y_2, \ldots, x_1^{d^{m-1}} + y_m) &= \sum a_{j_1,\ldots,j_m} x_1^{j_1} (x_1^d + y_2)^{j_2} \cdots (x_1^{d^{m-1}} + y_m)^{j_m} \\ &= \sum a_{j_1,\ldots,j_m} x_1^{j_1 + j_2 d + \cdots + j_m d^{m-1}} + g \end{aligned}$$

where $g \in k[x_1, y_2, \ldots, y_m]$ has degree in x_1 that is strictly smaller than $j_1 + j_2 d + \cdots + j_m d^{m-1}$. Therefore, there exists $b \in k^\times$ such that $bf(x_1, x_1^d + y_2, \ldots, x_1^{d^{m-1}} + y_m)$ is monic in $A[x_1]$, where $A = k[y_2, \ldots, y_m]$. Put $w_i = u_i - u_i^{d^{i-1}}$ for $2 \leq i \leq m$. The equality $bf(u_1, u_1^d + w_2, \ldots, u_1^{d^{m-1}} + w_m) = 0$ implies that u_1 is integral over $k[w_2, \ldots, w_m]$. The result follow by induction, since the transcendence degree of $k[w_2, \ldots, w_m]$ is one less than that of R.

□

Noether normalisation theorem has numerous applications, mostly oriented towards algebraic geometry. In particular, the theorem is useful in the proof of Hilbert's Nullstellensatz. We state and prove two versions of Hilbert's Nullstellensatz a 'weak' and a 'strong' version of the theorem.

Theorem 5.10 (Weak Hilbert's Nullstellensatz)**.** *Let k be a field with algebraic closure $\overline{k}$. Then, for every proper ideal I of the polynomial ring $k[x_1, \ldots, x_n]$, the set $V_{\overline{k}}(I)$ is nonempty. That is, there exists $\mathbf{a} = (a_1, \ldots, a_n) \in \overline{k}^n$ such that $f(\mathbf{a}) = 0$ for all $f \in I$.*

The statement clearly holds when $n = 1$, since every nonconstant polynomial in $k[x]$ has a root in $\overline{k}$. But if $n > 1$, then the statement is less obvious.

Proof. Let $R = k[x_1, \ldots, x_n]$. Let I be a proper ideal of R and let P be a maximal ideal of R containing I. By Corollary 5.8(i), R/P is a finite field extension of k, and so we have a tower of field extensions $k \hookrightarrow R/P \hookrightarrow \overline{k}$. Note that $P \cap k = \{0\}$ and that if $k = \overline{k}$, then $k \cong R/P$. Thus, the composition of the quotient map with the inclusion, $\phi = \iota\pi : R \xrightarrow{\pi} R/P \xrightarrow{\iota} \overline{k}$ is a k-algebra homomorphism with $P \subseteq \ker(\phi)$ and with $\phi(a) = a$ for all $a \in k$. By Noether normalisation theorem 5.9, there exist

$u_1, \ldots, u_r \in R$ such that R is integral over $S = k[u_1, \ldots, u_r]$ with the u_i's algebraically independent. It follows that for any $f \in I$, then

$$0 = \phi(f) = f(\phi(x_1), \ldots, \phi(x_n)).$$

Therefore $(\phi(x_1), \ldots, \phi(x_n)) \in V_{\overline{k}}(I) \neq \emptyset$. □

It is important to note that the result is valid for an algebraic set in $\overline{k}^n$ and not in k^n in this case. For instance, let $R = \mathbb{R}[x, y]$ and let $I = (x^2 + y^2 + 1)$. Then we calculate $V_{\mathbb{R}}(I) = \emptyset$, whilst $V_{\mathbb{C}}(I) = \{(z_1, z_2) \in \mathbb{C}^2 \mid z_1^2 + z_2^2 = -1\}$ is the complex 1-sphere of radius i.

The argument used in the proof of Theorem 5.10 raises the question of finding the maximal ideals in $\overline{k}[x_1, \ldots, x_n]$. If k is algebraically closed, the Nullstellensatz provides a complete description of the maximal ideals of $k[x_1, \ldots, x_n]$, by establishing a bijection between $\mathrm{MaxSpec}(k[x_1, \ldots, x_n])$ and the points of k^n.

Corollary 5.11. *Let $k = \overline{k}$ be an algebraically closed field. Then*

$$\mathrm{MaxSpec}(k[x_1, \ldots, x_n]) = \{(x_1 - a_1, \ldots, x_n - a_n) \mid a_i \in k,\ \forall\ 1 \leq i \leq n\}.$$

Explicitly, the function

$$k^n \to \mathrm{MaxSpec}(k[x_1, \ldots, x_n]), \quad \textit{mapping} \quad (a_1, \ldots, a_n) \mapsto (x_1 - a_1, \ldots, x_n - a_n)$$

is a bijection.

Proof. Note that every ideal of the form $J = (x_1 - a_1, \ldots, x_n - a_n)$ with the $a_i \in k$ is maximal since $k[x_1, \ldots, x_n]/J \cong k$ is a field.

Conversely, to prove that any maximal ideal is of that form, we use the weak Nullstellensatz. Let $J \in \mathrm{MaxSpec}(k[x_1, \ldots, x_n])$. Then $V(J) \neq \emptyset$, and there exists $\mathbf{a} = (a_1, \ldots, a_n) \in k^n$ such that $f(\mathbf{a}) = 0$ for all $f \in J$. Consider $I(\{\mathbf{a}\})$. By definition of $I(-)$, we have $J \subseteq I(\{\mathbf{a}\})$. Since J is maximal and $I(\{\mathbf{a}\}) \neq k[x_1, \ldots, x_n]$, we have $J = I(\{\mathbf{a}\})$, as required.

□

Theorem 5.12 (Strong Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field. Let J be an ideal of the polynomial ring $k[x_1, \ldots, x_n]$. Then $I(V(J)) = \sqrt{J}$. That is, if $f \in k[x_1, \ldots, x_n]$ vanishes on all the zeros $\mathbf{a} \in V(J)$ of J in k^n, then there exists $d \in \mathbb{N}$ such that $f^d \in J$.*

Proof. The statement trivially holds for $J = (0)$. So suppose J nonzero and let $f \in I(V(J))$, i.e. $f \in k[x_1, \ldots, x_n]$ vanishes on all the zeros $\mathbf{a} \in V(J)$ of J in k^n. Since $k[x_1, \ldots, x_n]$ is Noetherian, J is finitely generated. Let $g_1, \ldots, g_m \in J$ be a set of generators of J. Consider the system of $m + 1$ polynomial equations in $n + 1$ variables $x_1, \ldots, x_n, y$,

$$\begin{aligned} g_i &= 0 \quad \text{for all } 1 \leq i \leq m \\ 1 - yf &= 0 \end{aligned}$$

If $(a_1, \ldots, a_n, b) \in k^{n+1}$ satisfies all the equations $g_i = 0$, then $\mathbf{a} = (a_1, \ldots, a_n) \in V(J)$, and $f(\mathbf{a}) = 0$ since $f \in I(V(J))$. But then $(1 - yf)(a_1, \ldots, a_n, b) = 1 - bf(a_1, \ldots, a_n) = 1 \neq 0$. By the weak Nullstellensatz (which applies since k is algebraically closed), the corresponding ideal is improper, i.e.

$$(g_1, \ldots, g_m, 1 - yf) = k[x_1, \ldots, x_n, y] \quad \text{since } V(\{g_1, \ldots, g_m, 1 - yf\}) = \emptyset.$$

Therefore, there exist $h_1, \ldots, h_{m+1} \in k[x_1, \ldots, x_n, y]$ such that

$$1 = \sum_{i=1}^{m} h_i g_i + h_{m+1}(1 - yf). \tag{4}$$

Define a k-algebra homomorphism $\varphi : k[x_1, \ldots, x_n, y] \to k(x_1, \ldots, x_n)$, where $k(x_1, \ldots, x_n)$ is the field of fractions of $k[x_1, \ldots, x_n]$, by setting

$$\varphi(x_i) = x_i, \ \forall\, 1 \leq i \leq n \quad \text{and} \quad \varphi(y) = f^{-1}.$$

Applied to Equation (4), we obtain

$$\begin{aligned} 1 = \varphi(1) &= \sum_{i=1}^{m} \varphi(h_i)\varphi(g_i) + \varphi(h_{m+1})\varphi(1 - yf) \\ &= \sum_{i=1}^{m} h_i(x_1, \ldots, x_n, f^{-1}) g_i(x_1, \ldots, x_n) + h_{m+1}(x_1, \ldots, x_n)(1 - f^{-1}f) \\ &= \sum_{i=1}^{m} h_i(x_1, \ldots, x_n, f^{-1}) g_i(x_1, \ldots, x_n) = \sum_{i=1}^{m} \frac{u_i}{f^{N_i}}, \end{aligned}$$

for some $u_1, \ldots, u_m \in k[x_1, \ldots, x_n]$ and positive integers $N_1, \ldots, N_m$, after putting every term of the sum on a common denominator. Note that $u_1, \ldots, u_m \in J$ since they are $k[x_1, \ldots, x_n]$-linear combinations of $g_1, \ldots, g_m$.

Let $N = \max\{N_1, \ldots, N_m\}$. Then,

$$f^N = f^N \cdot 1 = f^N \big(\sum_{i=1}^{m} \frac{u_i}{f^{N_i}} \big) = \sum_{i=1}^{m} u_i f^{N - N_i} \in J,$$

which proves that $f \in \sqrt{J}$, and $I(V(J)) \subseteq \sqrt{J}$.

Conversely, since $V(X) = V((X)) = V(\sqrt{(X)})$ for any subset X of $k[x_1, \ldots, x_n]$, we have $\sqrt{J} \subseteq I(V(\sqrt{J})) = I(V(J)) \subseteq \sqrt{J}$, which forces the equality.

□

Corollary 5.13. *Let k be an algebraically closed field and let J_1, J_2 be two ideals of $k[x_1, \ldots, x_n]$ such that $V(J_1) = V(J_2)$. Then $\sqrt{J_1} = \sqrt{J_2}$.*

Proof. By the strong Nullstellensatz, $\sqrt{J_1} = I(V(J_1)) = I(V(J_2)) = \sqrt{J_2}$.

□

5.3 Exercises

Exercise 5.1. Let k be an algebraically closed field. Prove that k is infinite.

Exercise 5.2. Let k be a field and let $R = k[x_1, \ldots, x_n]$ a multivariate polynomial ring. Let $A \subseteq k^n$.

i. Prove that $I(A)$ is an ideal of R.

ii. Prove that $I(V(I(A))) = I(A)$.

Exercise 5.3. Let k be an algebraically closed field, and let $\{I_j,\ j \in J\}$ be an infinite set of proper nonzero ideals of $k[x]$ with $I_j \neq I_{j'}$ whenever $j \neq j'$. Prove that $\bigcup_{j \in J} V(I_j) \neq V\big(\bigcap_{j \in J} I_j\big)$ and find an example where the inclusion is proper.

Exercise 5.4. Let k be an algebraically closed field. Prove that the correspondences

$$\mathcal{P}(k^n) \underset{V(-)}{\overset{I(-)}{\rightleftarrows}} \mathcal{I}(k[x_1, \ldots, x_n])$$

between the subsets of k^n and the ideals of $k[x_1, \ldots, x_n]$ are bijective functions between the set of algebraic subsets of k^n and radical ideals of $k[x_1, \ldots, x_n]$, and that they are inverse of each other.

Exercise 5.5. An algebraic set is *irreducible* if it is not the disjoint union of two nonempty disjoint algebraic sets. For instance, with $k[x, y]$, the set $V(xy - 1)$ is irreducible, but $V(x^2 - y^2)$ is not irreducible. Geometrically, $V(xy - 1)$ is the hyperbola $y = \frac{1}{x}$ in k^2, and $V(x^2 - y^2)$ is the union of the two lines $y = \pm x$.

Let $V(I)$ be an algebraic set with I a proper ideal of $k[x_1, \ldots, x_n]$ and with k algebraically closed. Prove that $V(I)$ is irreducible if and only if $I \in \mathrm{Spec}(k[x_1, \ldots, x_n])$.

Exercise 5.6. Let k be a field and consider the polynomial ring $k[x, y, z]$. Write the following algebraic sets as the disjoint of irreducible ones (cf. Exercise 5.5). Discuss the different cases according to the characteristic of k.

i. $V(x^2 + 3xy^2 - 4z^3)$.

ii. $V(y^6 - xz^3)$.

Exercise 5.7. Let $R = k[x_1, \ldots, x_n]$ where k is a field, and let $P \in \mathrm{MaxSpec}(R)$. Prove that I/IP is a finite dimensional k-vector space.

6 Primary decomposition

Let R be a commutative ring, and let I, J_1, J_2 be ideals of R with I prime. Suppose that $I \supseteq J_1 \cap J_2$. Then, $I \supseteq J_1$ or $I \supseteq J_2$, by Lemma 1.12. Recall that $J_1 J_2$ is the ideal of R whose elements are the finite sums $\sum_n a_n b_n$ with $a_n \in J_1$ and $b_n \in J_2$ for all n, and that $J_1 J_2 \subseteq J_1 \cap J_2$.

The main result of this section is *Lasker-Noether theorem*, a result about the existence and uniqueness (in some subtle sense) of the decomposition of ideals in any Noetherian ring into finite intersections of primary ideals. This is somewhat similar to the factorisation of elements into products of powers of prime (or irreducible) elements in a UFD, e.g. $600 = 2^3 \cdot 3 \cdot 5^2$. The theorem is named after the German mathematicians Emanuel Lasker and Emmy Noether.

We follow the treatment in [Jac, Section 7.13, Vol. II] for most of the section; in particular, we present the slightly more general perspective of primary submodules of a Noetherian ring, which we then specialise to ideals.

6.1 Primary submodules

Let R be a Noetherian commutative ring and let M be an R-module. Recall that the R-endomorphisms of M form the ring $\operatorname{End}_R M$ where the addition is pointwise addition and multiplication is the composition of maps. That is, $(f+g)(m) = f(m) + g(m)$ and $(fg)(m) = f\big(g(m)\big)$, for all $f, g \in \operatorname{End}_R M$ and all $m \in M$. For every $a \in R$, let $a_M : M \to M$ be the R-endomorphism of M defined by $a_M(x) = ax$ for all $x \in M$. The map $\rho_M : R \to \operatorname{End}_R M$ given by $\rho_M(a) = a_M$ is itself a ring homomorphism, with $\operatorname{im}(\rho_M)$ a central subring of $\operatorname{End}_R M$, i.e. $\rho_M f = f \rho_M$ for all $f \in \operatorname{End}_R M$.

Some of the results we will see do not require R to be Noetherian, however, for simplicity, we assume throughout that R is Noetherian.

Definition 6.1. Let R be a Noetherian commutative ring and let M be an R-module. The *annihilator* of M is $\operatorname{Ann}_R(M) = \{a \in R \mid ax = 0,\ \forall\, x \in M\}$.

If $x \in M$, then we write $\operatorname{Ann}_R(x)$ instead of $\operatorname{Ann}_R(Rx)$ for the annihilator of the R-submodule of M generated by x.

Observe that $\operatorname{Ann}_R(M) = \bigcap_{x \in M} \operatorname{Ann}_R(x) = \ker(\rho_M)$ is an ideal of R.

Definition 6.2. Let R be a Noetherian commutative ring and let M be an R-module. Let $a \in R$ be such that there exists a nonzero $x \in M$ with $ax = 0$. We call a a *zero divisor* of M.

Note that the definition of a zero divisor of an R-module includes $0 \in R$, which allows us to say that the elements of R which are not zero divisors are precisely those for which a_M is injective. Moreover, by definition, we note that

$$\{a_M \in \operatorname{End}_R M \mid\ \exists\, n \in \mathbb{N}, \text{ with } a_M^n = 0_M\} \overset{1-1}{\longleftrightarrow} \sqrt{\ker(\rho_M)} = \sqrt{\operatorname{Ann}_R(M)} \tag{5}$$

In other words, the set of nilpotent R-endomorphisms of M of the form a_M for some $a \in R$ is in bijection with the radical of the annihilator of M.

Similarly, for any given $x \in M$,

$$\sqrt{\operatorname{Ann}_R(x)} \overset{1-1}{\longleftrightarrow} \{a_M \in \operatorname{End}_R M \mid\ \exists\, n \in \mathbb{N}, \text{ with } a^n x = 0\} \tag{6}$$

is the set of such R-endomorphisms of M whose restriction to the submodule Rx is nilpotent.

Definition 6.3. Let R be a commutative Noetherian ring and let M be an R-module. A proper submodule N of M is *primary* if, for every $a \in R$, the map $a_{M/N}$ is either injective or nilpotent.

If $M = R$, then we say that a proper ideal I of R is *primary* if I is a primary submodule of the regular R-module R. In other words, I is primary if whenever $a, b \in R$ are such that $ab \in I$ and $b \notin I$, then $a \in \sqrt{I}$, i.e. $a_{R/I}$ is either injective or nilpotent.

Observe that prime ideals are primary ideals.

If N is a proper submodule of M, then the map $a_{M/N} \in \mathrm{End}_R\, M/N$ is not injective if and only if there exists $b \in M$ such that $ab + N = N$, i.e. $ab \in N$. Hence, N is primary if, for any $a \in R$ such that a_M is not injective, then $a_{M/N} \in \mathrm{Nil}(\mathrm{End}_R\, M/N)$, i.e. the set of zero divisors of M/N is equal to $\sqrt{\mathrm{Ann}_R(M/N)}$.

Example 6.4. Let $R = \mathbb{Z}[x]$, and consider the ideals $I = (x^2 - 1)$ and $J = (x^3)$ of R.

Then I is not primary since $\ker\big((x+1)_{R/I}\big) = (x-1) \neq (0_{R/I})$ and $(x+1)^n \notin (x^2-1)$ for all $n \in \mathbb{N}$, showing that $(x+1)_{R/I}$ is neither injective nor nilpotent on R/I.

On the other hand, (x^3) is primary since $a_{R/J}$ is nilpotent if and only if $a \in (x)$, and is injective otherwise, i.e. $\mathrm{Nil}(\mathrm{End}_R\, R/J) = (x) = \sqrt{\mathrm{Ann}_R(1)}$.

Let us observe a property of primary submodules.

Lemma 6.5. *Let R be a commutative Noetherian ring and let M be an R-module. Let N be a primary submodule of M. Then $\sqrt{\mathrm{Ann}_R(M/N)} \in \mathrm{Spec}(R)$.*

Proof. Let $a, b \in R$ such that $a, b \notin \sqrt{\mathrm{Ann}_R(M/N)}$. Since N is a primary submodule of M, this is equivalent to saying that the R-endomorphisms $a_{M/N}, b_{M/N}$ of M/N are injective. Hence, so is their product $a_{M/N} b_{M/N} = (ab)_{M/N}$. Therefore $ab \notin \sqrt{\mathrm{Ann}_R(M/N)}$. □

Definition 6.6. Let R be a commutative Noetherian ring and let M be an R-module. The prime ideal $P = \sqrt{\mathrm{Ann}_R(M/N)}$ is the *associated prime ideal* of the primary submodule N, and we say that N is *P-primary*.

For instance, if $M = R$ and I is a primary ideal of R, then the associated prime ideal of I is $\sqrt{I}$.

Example 6.7. Let $R = \mathbb{Z}$.

i. The ideal (27) is 3-primary with associated prime ideal (3). Indeed, for any $a, b \in \mathbb{Z}$ such that $ab \in (27)$, at least one of a or b is a multiple of 3.

ii. Let $M = \mathbb{Z}/(p^{i_1}) \oplus \cdots \oplus \mathbb{Z}/(p^{i_n})$ be a finite torsion $\mathbb{Z}$-module, for some prime p. Then (0) is a (p)-primary submodule of M, since for any $x \in M$, there exists $n \in \mathbb{N}$ such that $p^n x = 0$. The associated prime ideal of (0) is (p).

Proposition 6.8. *Let R be a commutative Noetherian ring, and let I be a maximal ideal of R. Then, for any $n \in \mathbb{N}$, any ideal J of R with $I^n \subseteq J \subseteq I$ is I-primary.*

Proof. By assumption, $J \subsetneq R$. Suppose that for some $a, b \in R$, we have $ab \in J$. We want to show that $a^m \in J$ for some $m \in \mathbb{N}$, or else $b \in J$ (i.e. $a_{R/J}$ is nilpotent or injective).

If $a \in I$, then $a^n \in I^n \subseteq J$.

If $a \notin I$, then $a + I \in R/I$ is nonzero. Since I is maximal, R/I is a field and $(a + I) \in R/I^\times$. Let $c \in R$ such that $ac \in 1 + I$ in R/I. Then, $(ac-1)^n \in J$, i.e. $(ac-1) \in \mathrm{Nil}(R/J)$. It follows that $1 + (ac-1) \in (ac + J) \in R/J^\times$, by Proposition 1.25. Therefore $(a + J) \in (R/J)^\times$, and we conclude that if $ab \in J$, then we must have $b \in J$. □

This result can be used to construct examples of primary ideals which are not powers of prime ideals. For instance, let $R = k[x, y]$ where k is a field, let $I = (x, y)$ and let $J = (x^2, y)$. Then $I^2 = (x^2, xy, y^2) \subset J \subset I$, where the inclusions are proper. Hence J is an I-primary ideal which is not a power of I. Let us stress the fact that Proposition 6.8 considers *maximal* ideals. Indeed, it is not true in general that if $P \in \mathrm{Spec}(R)$, with R commutative Noetherian, then P^n is primary for $n \geq 2$.

Proposition 6.9. *Let R be a commutative Noetherian ring and let M be an R-module. Let $P \in \mathrm{Spec}(R)$ and let N_1, N_2 be P-primary submodules of M. The following hold.*

i. $N_1 \cap N_2$ *is a* P*-primary submodule of* M*.*

ii. Let $x \in M$ *and define* $I_x(N_1) = \{a \in R \mid \exists\, n \in \mathbb{N},\ \text{with } a^n x \in N_1\}$*. Then*

$$I_x(N_1) = \begin{cases} P & \text{if } x \notin N_1 \\ R & \text{if } x \in N_1. \end{cases}$$

Proof. i. By assumption, $N_1 \cap N_2$ is a proper submodule of M. Let $a \in P$, and choose $n \in \mathbb{N}$ such that $\mathrm{im}(a_M^n) \subseteq (N_1 \cap N_2)$, which is possible since N_1, N_2 are P-primary submodules of M. That is, $P \subseteq \sqrt{\mathrm{Ann}_R(M/(N_1 \cap N_2))}$. Now, pick $a \in R \setminus P$, and let $x \in M \setminus (N_1 \cap N_2)$; without loss of generality, we may assume that $x \notin N_1$. Then $ax \notin N_1$ since $P = \sqrt{\mathrm{Ann}_R(M/N_1)}$ implies that $a_{M/N_1} \in \mathrm{End}_R(M/N_1)$ is injective. It follows that $ax \notin N_1 \cap N_2$ for all $x \in M \setminus (N_1 \cap N_2)$. Therefore $\mathrm{Ann}_R(M/(N_1 \cap N_2)) \subseteq P$, and $\sqrt{\mathrm{Ann}_R(M/(N_1 \cap N_2))} \subseteq P$ since P is prime. Thus $\sqrt{\mathrm{Ann}_R(M/(N_1 \cap N_2))} = P$, i.e. $N_1 \cap N_2$ is P-primary.

ii. If $x \in N_1$, then any $a \in R$ satisfies $ax \in N_1$ since N_1 is an R-module, and so $I_x(N_1) = R$.

Suppose that $x \notin N_1$. By assumption, $P = \sqrt{\mathrm{Ann}_R(M/N_1)} \subseteq I_x(N_1)$. Conversely, $P \supseteq I_x(N_1)$ since for any $a \in R \setminus P$ the map a_{M/N_1} is injective.

□

Proposition 6.9 extends from two to any finite number of P-primary submodules of a given R-module, where $P \in \mathrm{Spec}(R)$.

Corollary 6.10. *Let* R *be a commutative Noetherian ring, let* $P \in \mathrm{Spec}(R)$*, and let* M *be an* R*-module. The intersection of finitely many* P*-primary* R*-submodules of* M *is* P*-primary.*

6.2 Lasker-Noether theorem

Definition 6.11. Let R be a commutative Noetherian ring, let M be an R-module and let N be a proper submodule of M. If there exist primary submodules $Q_1, \ldots, Q_s$ of M such that $N = Q_1 \cap \cdots \cap Q_s$, we call such expression a *primary decomposition of* N. We call the set $\{Q_1, \ldots, Q_s\}$ *irredundant* if $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$.

Lasker-Noether theorem asserts existence and uniqueness of primary decompositions. We start with the proof of the uniqueness of primary decompositions.

Theorem 6.12. *Let* R *be a commutative Noetherian ring, let* M *be an* R*-module and let* N *be a proper submodule of* M*. Suppose that* $Q_1, \ldots, Q_s$ *are primary submodules of* M *such that* $N = Q_1 \cap \cdots \cap Q_s$*, and that the set* $\{Q_1 \ldots, Q_s\}$ *is irredundant. Let* $P_1, \ldots, P_s$ *be the associated primes of* $Q_1, \ldots, Q_s$*, respectively. The following hold.*

i. Let P *be a prime ideal. Then* P *is in the set* $\{P_1, \ldots, P_s\}$ *if and only if there exists* $x \in M$ *such that* $P = I_x(N)$*, as defined in Proposition 6.9. Hence, the set of associated primes* $\{P_1, \ldots, P_s\}$ *is independent of the choice of irredundant primary decomposition of* N*.*

ii. The set $P_1 \cup \cdots \cup P_s$ *is the set of zero divisors of* M/N*.*

iii. $P_1 \cap \cdots \cap P_s = \sqrt{\ker(\rho_{M/N})}$*, where* $\rho_{M/N} : R \to \mathrm{End}_R(M/N)$ *is the ring homomorphism defined by* $\big(\rho_{M/N}(a)\big)(x) = a_{M/N}(x) = ax$ *for all* $a \in R$ *and* $x \in M/N$*.*

Proof. i. By definition of the ideals $I_x(N)$, if $N = Q_1 \cap \cdots \cap Q_s$, then $I_x(N) = I_x(Q_1) \cap \cdots \cap I_x(Q_s)$. By Proposition 6.9,

$$I_x(Q_i) = \begin{cases} P_i & \text{if } x \notin Q_i \\ R & \text{if } x \in Q_i. \end{cases}$$

and it follows that $I_x(N) = P_{i_1} \cap \cdots \cap P_{i_m}$, where $i_1, \ldots, i_m$ are the indices i for which $x \notin Q_i$.

Suppose that $I_x(N) = P$, with P a prime ideal. Then

$$P = P_{i_1} \cap \cdots \cap P_{i_m},$$

which forces $P_{i_j} \subseteq P$ for some j since P is prime (cf. Lemma 1.12). Therefore, $P = P_{i_j}$ for some $1 \leq j \leq m$.

Conversely, since the decomposition is irredundant, for every P_i, there exists $x_i \in M$ such that $x_i \in \bigcap_{j \neq i} Q_j$ and $x_i \notin Q_i$. Then by Proposition 6.9, $I_{x_i}(N) = P_i$.

ii. By i., if $a \in P_i$, then there exist $x \in M \setminus N$ and $m \in \mathbb{N}$ such that $a^m x \in N$. Choose m minimal, i.e. such that $a^{m-1}x \notin N$. Note that a is a zero divisor of M/N since $a \in \mathrm{Ann}_R(a^{m-1}x + N)$. Hence $P_1 \cup \cdots \cup P_s$ is contained in the set of zero divisors of M/N.

Conversely, let $a \in R$ be a zero divisor of M/N, and pick $x \in M \setminus N$ such that $ax \in N$. Since $N = Q_1 \cap \cdots \cap Q_s$, then $x \notin Q_i$ for some i. Now, $ax \in N \subseteq Q_i$ implies that $a_{M/Q_i} \in \mathrm{End}_R(M/Q_i)$ is not injective, and so must be nilpotent since Q_i is primary. It follows that $a \in P_i = \sqrt{\mathrm{Ann}_R(M/Q_i)}$.

iii. The set $\sqrt{\mathrm{Ann}_R(M/N)}$ is formed by all the elements $a \in R$ such that there exists $m \in \mathbb{N}$ with $a^m M \subseteq N$. Equivalently, $\sqrt{\ker(\rho_{M/N})}$ is the set of elements $a \in R$ such that there exists $m_i \in \mathbb{N}$ with $a^{m_i} M \subseteq Q_i$, i.e. $a \in P_i$, for all $1 \leq i \leq s$.

□

Theorem 6.12 tells us that the set $\mathrm{Ass}_R(N) = \{P_1, \ldots, P_s\}$ of *associated prime ideals of* N is unique. Moreover, combining this result with Corollary 6.10 tells us that N is primary if and only if $\mathrm{Ass}_R(N) = \{P\}$.

Remark 6.13. In the notation of Theorem 6.12, if N has a primary decomposition as above, then we may assume that the primary modules Q_i have distinct associated primes. Indeed, we can group the Q_i's with the same associated prime P together and replace them by their intersection, itself P-primary. Following [Jac, Section 7.13, Vol. II], we call such a decomposition *normal*. This establishes a 1-1 correspondence between the primary modules Q_i in a primary decomposition of a proper submodule N of M, and their associated prime ideals.

Definition 6.14. Let R be a commutative Noetherian ring, let M be an R-module and let N be a proper submodule of M.

i. A primary submodule Q in a normal primary decomposition of N of M is *isolated* if its associated prime ideal is minimal in the set of associated prime ideals of N. (*Minimal* with respect to inclusion.)

ii. Suppose that M is Noetherian. We call N *intersection indecomposable* if $N \neq N_1 \cap N_2$ for proper submodules N_1, N_2 of M with $N \neq N_1, N_2$.

Observe that there can be many irredundant primary decompositions of an ideal. For instance, in the above example with $R = k[x, y]$ where k is a field, $I = (x, y)$ and $J = (x^2, y)$, we have distinct such decompositions of the form $J = (x) \cap (ax + y, x^2)$, for $a \in k$. Instead, the associated prime ideals are (x) and (x, y) independently of the decomposition chosen. Note that (x) is an isolated prime ideal, and that (x, y) is intersection indecomposable since maximal.

Proposition 6.15. *Let R be a commutative Noetherian ring and let M be a Noetherian R-module. The following hold.*

i. Every proper submodule of M can be written as an intersection of finitely many intersection indecomposable submodules of M.

ii. Every intersection indecomposable submodule of M is primary.

Proof. i. Let X be the set of proper submodules of M which cannot be written as an intersection of finitely many intersection indecomposable submodules of M. Then X is a poset, and if X is nonempty, then any totally ordered subset $N_1 \subseteq N_2 \subseteq \dots$ of X has an upper bound $\cup_{n\in\mathbb{N}} N_n$ in X. By Zorn's lemma, X has some maximal element, say N. That is, N is not intersection indecomposable, say, there exist R-modules N_1, N_2 such that $N \subsetneq N_1, N_2 \subsetneq M$ with $N = N_1 \cap N_2$. Since $N \subsetneq N_1, N_2$, the maximality of N in X implies that N_1, N_2 can be written as intersection of finitely many intersection indecomposable submodules of M. But then so does N. Therefore, X must be empty.

ii. Let N be a proper submodule of M. Suppose that N is not primary. Then, by definition, there exists $a \in R$ such that the map $a_{M/N} \in \mathrm{End}_R\, M/N$ is neither injective nor nilpotent. Hence we obtain an ascending chain of proper submodules of M/N:

$$0 \subsetneq \ker(a_{M/N}) \subseteq \ker(a^2_{M/N}) \subseteq \cdots \subsetneq M/N.$$

Since M is Noetherian, M/N too and the chain must stabilise, i.e. there exists $n \in \mathbb{N}$ and and R-module $N \subsetneq N_1 \subsetneq M$ such that

$$N_1/N = \ker(a^m_{M/N}) = \ker(a^n_{M/N}) \quad \text{for all } m \geq n.$$

Let $N_2 = a^n M + N = \{a^n x + y \mid x \in M,\ y \in N\}$. Note that $N \subsetneq N_2 \subsetneq M$. We claim that $N = N_1 \cap N_2$. The inclusion $N \subseteq N_1 \cap N_2$ holds by definition of N_1, N_2. Conversely, let $z \in N_1 \cap N_2$. That is, $a^n z \in N$ since $z \in N_1$, and $z = a^n x + y$ for some $x \in M$ and $y \in N$, since $z \in N_2$. It follows that $a^n z = a^{2n} x + a^n y$ lies in N, and hence $a^{2n} x = a^n z - a^n y \in N$. Since $2n \geq n$, we have $\ker(a^{2n}_{M/N}) = \ker(a^n_{M/N}) = N_1/N$. It follows that $a^n x \in N$ too, and so $z = a^n x + y \in N$, showing that $N = N_1 \cap N_2$, as asserted. Therefore, N is not intersection indecomposable. The result follows by contrapositive.

□

The existence of primary decompositions is an immediate corollary of Proposition 6.15.

Theorem 6.16. *Let R be a commutative Noetherian ring and let M be a Noetherian R-module. Any proper submodule of M has a normal primary decomposition. Moreover, the set of associated prime ideals is unique.*

In [AM], the theory of primary decompositions is given in terms of ideals instead of modules. We have presented the more general version from [Jac, Section 7.13, Vol II]. For completeness, we state the results in terms of primary ideals, leaving the proofs as exercises.

Definition 6.17. Let R be a commutative Noetherian ring. Let I be an ideal of R. We call I *irreducible* if I is an intersection indecomposable R-submodule of R. That is, $I \neq R$ and I cannot be written as the intersection of two ideals containing I properly.

Proposition 6.18. *Let R be a commutative Noetherian ring. Every proper ideal of R can be written as the intersection of finitely many irreducible ideals.*

Let I be an ideal of R and consider the projection map $\pi : R \to R/I$. Suppose that $a, b \in R$ are such that $\pi(ab) = I$. By definition, I is primary if and only if $R/I \neq 0$ and $a_{R/I}$ is injective or nilpotent on R/I, i.e. $\pi(b) = I$ or $a^n \in I$ for some $n \in \mathbb{N}$, respectively. Equivalently, $R/I \neq 0$, and every zero divisor of R/I is nilpotent.

In particular, a primary ideal can be seen as associated to a prime ideal, namely its radical.

Definition 6.19. Let R be a commutative Noetherian ring. Let I, P be ideals of R and suppose that P is prime. We call I *P-primary* if:

- I is primary, and
- $\sqrt{I} = P$.

Note that a prime ideal may have numerous primary ideals associated with it.

Proposition 6.20. *Let R be a commutative Noetherian commutative ring. Let I, J be P-primary ideals of R. Then $I \cap J$ is P-primary. Hence, the intersection of finitely many P-primary ideals of R is also P-primary.*

The primary ideals are what we need to express the analogue of a *factorisation* of ideals in a ring, which is the main result in this section.

Definition 6.21. Let R be a commutative Noetherian ring. A *primary decomposition* of a proper ideal I of R is an intersection

$$I = \bigcap_{1 \leq i \leq t} J_i, \quad \text{where } J_1, \ldots, J_t \text{ are primary ideals.}$$

We call such a decomposition *minimal* if $J_i \neq J_j$ for all $i \neq j$, and if $J_i \not\supseteq \bigcap_{j \neq i} J_j$ for all $1 \leq i \leq t$.

Theorem 6.22. *Let R be a commutative Noetherian ring. Any proper ideal of R admits a minimal primary decomposition, which is unique, in the sense that the set of associated prime ideals of such a decomposition is independent of the decomposition chosen. That is,*

- *For every proper ideal I of R, there exist primary ideals $J_1, \ldots, J_t$ such that $I = \bigcap_{1 \leq i \leq t} J_i$, and*
- *The set of associated prime ideals $\{\sqrt{J_1}, \ldots, \sqrt{J_t}\}$ is unique and irredundant.*

The proof of Theorem 6.22 in this context uses the colon ideals, defined for any commutative ring.

Definition 6.23. Let R be a commutative ring, let I be an ideal of R, and let X be a subset of R. The *colon ideal* $(I \colon X)$ is the ideal

$$(I \colon X) = \{a \in R \mid aX \subseteq I\}, \quad \text{where} \quad aX = \{ax \mid x \in X\} \subseteq R.$$

Observe that $(I \colon X)$ is indeed an ideal: since $0 \in (I \colon X)$, then $(I \colon X) \neq \emptyset$. If $a, b \in (I \colon X)$, then $(a - b)X = \{(a - b)x = ax - bx \mid x \in X\} = aX + (-b)X \subseteq I$ because $bx \in I$ if and only if $-bx \in I$ for all $b, x \in R$. Hence $(I \colon X)$ is a subgroup of R. Finally, if $a \in R$ and $b \in (I \colon X)$, then $(ab)X = a(bX) \subseteq I$ since I is an ideal.

Note that $I \subseteq (I \colon X)$ and that $(I \colon X) = (I \colon (X))$, where (X) is the ideal generated by the set X.

Here are some elementary properties of colon ideals.

- If $I = I_1 \cap I_2$, then $(I \colon X) = (I_1 \colon X) \cap (I_2 \colon X)$. Indeed, $a \in (I_1 \colon X) \cap (I_2 \colon X)$ if and only if $aX \subseteq I_i$ for $i = 1, 2$, i.e. $aX \subseteq I$.

- If X is an ideal of the form $X = J_1 + J_2$ with J_1, J_2 ideals of R, then $(I\colon J_1+J_2) = (I\colon J_1)\cap(I\colon J_2)$. Indeed, $a \in (I\colon J_1) \cap (I\colon J_2)$ if and only if $a \in R$ satisfies $aJ_i \subseteq I$ for $i = 1, 2$, and since I is an ideal, this holds if and only if $aJ_1 + aJ_2 = \{ab_1 + ab_2 \mid b_i \in J_i,\ i = 1, 2\} \subseteq I$. Therefore $(I\colon J_1) \cap (I\colon J_2) = (I\colon J_1 + J_2)$.
- If $X \subseteq Y$, then $(I\colon Y) \subseteq (I\colon X)$. Indeed, $a \in (I\colon Y)$ implies $aX \subseteq aY \subseteq I$.

The following lemma is the analogue of Lemma 6.15.

Lemma 6.24. *Let R be a commutative Noetherian ring.*

i. An irreducible ideal of R is primary.

ii. Any proper ideal of R admits a minimal primary decomposition.

Let R be a commutative Noetherian ring, let $a \in R$ and let I be an ideal of R. Suppose that $I = J_1 \cap \cdots \cap J_s$ is a minimal primary decomposition of I. Then we calculate

$$\begin{aligned}\sqrt{(I\colon a)} &= \sqrt{(J_1 \cap \cdots \cap J_s\colon a)} \\ &= \bigcap_{i=1}^{s} \sqrt{(J_i\colon a)} = \bigcap_{a\notin J_i} \sqrt{J_i},\end{aligned}$$

where the last equality follows from the observation that if J is a primary ideal, then

$$\sqrt{(J\colon a)} = \begin{cases} R & \text{if } a \in J \\ \sqrt{J} & \text{otherwise.}\end{cases}$$

(Compare with the ideal $I_x(N_1)$ introduced in Proposition 6.9.)

Definition 6.25. Let R be a commutative ring and let I be a proper ideal of R. A *minimal prime ideal of I* is a prime ideal P of R such that $I \subseteq P$ and there is no prime ideal Q of R such that $I \subseteq Q \subset P$.

If $I = (0)$, then we simply speak of the *minimal prime ideals* (of R).

Note that if R is an ID, then (0) is the unique minimal prime ideal of R.

Proposition 6.26. *Let R be a commutative Noetherian ring, and let I be a proper ideal of R.*

i. Every minimal prime ideal of I is contained in an associated prime ideal of I. Hence the minimal prime ideals of I are precisely the minimal elements of the set of associated prime ideals of I.

ii. R has finitely many minimal prime ideals. Thus, if $P_1, \ldots, P_s$ are the minimal prime ideals of R, then $\bigcap_{i=1}^{s} P_i = \mathrm{Nil}(R)$.

Proof. i. Let P be a prime ideal of R with $I \subseteq P$ and let $I = J_1 \cap \cdots \cap J_s$ be a minimal primary decomposition of I. Then $P \supseteq \sqrt{I} = \sqrt{J_1} \cap \cdots \cap \sqrt{J_s}$, where the $\sqrt{J_i}$'s are the associated prime ideals of I. By Lemma 1.12, at least one of the $\sqrt{J_i}$ is contained in P, as required.

ii. The minimal prime ideals of R are the minimal associated prime ideals of (0). By Theorem 6.16, there are finitely many of them. Hence, if $P_1, \ldots, P_s$ are the minimal prime ideals of R, then by Theorem 1.23, we have

$$\mathrm{Nil}(R) = \bigcap_{P} P \ \subseteq \ \bigcap_{i=1}^{s} P_i, \quad \text{where } P \text{ runs through all the prime ideals of } R.$$

Since every prime ideal P contains some minimal prime ideal, by the first part, we conclude that the inclusion is in fact an equality. The result follows.

□

From the definition, it is immediate that prime ideals are primary (recall that R/I is an ID if and only if I is prime), and we have seen that the converse does not hold in general. If $R = \mathbb{Z}$, for instance, we note that the primary ideals need not be prime, since they are of the form (p^n), for p prime and $n \in \mathbb{N}$. Hence, in $\mathbb{Z}$, primary and irreducible ideals coincide. This is a property of all PIDs.

Lemma 6.27. *Let R be a commutative Noetherian ring, and let I be an ideal of R. Then, there exists $n \in \mathbb{N}$ such that $(\sqrt{I})^n \subseteq I$. In particular, if I is P-primary for some $P \in \mathrm{Spec}(R)$, then there exists $n \in \mathbb{N}$ such that $P^n \subseteq I$. It follows that if R is a PID, then any primary ideal is of the form (p^n) for some prime element $p \in R$ and some $n \in \mathbb{N}$.*

Proof. By assumption, $\sqrt{I}$ is generated by finitely many elements, say $x_1, \ldots, x_s$, and for each, there exists $d_i \in \mathbb{N}$ such that $x_i^{d_i} \in I$. Any element of $\sqrt{I}$ is a linear combination $y = \sum_i a_i x_i$ with $a_i \in R$ for all i. Let $n = \sum_i n_i$ (or at least $\sum_i n_i - (s-1)$), then $y^n \in I$ since every monomial in y^n contains $x_j^{n_j}$ as factor. Therefore $(\sqrt{I})^n \subseteq I$. In particular, if I is primary, then $\sqrt{I}$ is its associated prime ideal. If moreover R is a PID, then $\sqrt{I} = (p)$ for some prime element $p \in R$. □

For the use of computer algebra software for computing primary decompositions, we refer to
`http://magma.maths.usyd.edu.au/magma/handbook/text/1279#dpoly_ideal:primarydecomposition`

6.3 Exercises

Exercise 6.1. Let R be a ring and let M be an R-module. Prove that $\mathrm{Ann}_R(x)$ and $\mathrm{Ann}_R(M)$ are ideals of R.

Exercise 6.2. Let R be a PID and let M be a finitely generated R-module. Describe the primary submodules of M. You may use (without proof) the structure theorem for finitely generated modules over PIDs, namely, $M = M_{tor} \oplus M_{tf}$, where the torsion submodule $M_{tor} = \{x \in M \mid \exists\, 0 \neq a \in R \,:\, ax = 0\}$ of M is finite and M_{tf} is a finitely generated torsionfree R-module, cf. [Lan, Section III.7].

Exercise 6.3. Let R be a PID and let $P \in \mathrm{Spec}(R)$. Prove that every P-primary ideal of R is a power of P.

Exercise 6.4. Let R be a commutative ring. Prove that R has a unique minimal prime ideal if and only if R is an ID?

Exercise 6.5. Find the minimal prime ideals of $R = \mathbb{C}[x,y]/(xy)$ and of $S = \mathbb{C}[x,y]/(x^2y, xy^3)$.

Exercise 6.6.
i. Let $R = k[x,y,z]/(xy - z^2)$, and let $P = (x,z)$ and $Q = P^2$. Prove that Q is not primary.

ii. Let R be a commutative ring. Prove that if $P \in \mathrm{Spec}(R)$, then P is the unique minimal prime over P^n.

Exercise 6.7. Let R be a commutative ring. Prove that an ideal is primary if and only if it has exactly one associated prime.

Exercise 6.8. Let k be a field and let $R = k[x,y]$.

i. For $a \in k$, define $Q_a = (y - ax, x)$. Prove that Q_a is a primary ideal and find its associated prime.

ii. Using the Q_a's or otherwise, find two distinct primary decompositions of $I = (x^2, xy)$.

Exercise 6.9. Complete the proofs of Propositions 6.18 6.20, Theorem 6.22 and Lemma 6.24.

Exercise 6.10. Let R be a commutative ring.

i. Let $Q \subseteq P$ be ideals of R with $P \in \operatorname{Spec}(R)$ and Q primary. Prove that QR_P is a primary ideal of R_P and that $\sqrt{Q}R_P = \sqrt{QR_P}$. Hence there is a bijection

$$\{\text{primary ideals of } R \text{ contained in } P\} \leftrightarrow \{\text{primary ideals of } R_P\}$$

ii. Let I be an ideal in R with minimal primary decomposition $I = Q_1 \cap \cdots \cap Q_n$ in R. Describe a minimal primary decomposition of IR_P and the set of associated primes of IR_P.

iii. For I as above, describe a minimal primary decomposition of $IR_P \cap R$ (the saturation of I) and the set of associated primes for $IR_P \cap R$.

Exercise 6.11. Let $R = k[x, y, z]$ be a polynomial ring over a field k. Let $P_1 = (x, y)$, $P_2 = (x, z)$ and $P_3 = (x, y, z)$.

i. check that $P_1, P_2, P_3 \in \operatorname{Spec}(R)$.

ii. Let $I = P_1P_2$. Prove that $I = P_1 \cap P_2 \cap P_3^2$ is a minimal primary decomposition of I.

iii. Find $\operatorname{Ass}_R(I)$.

7 Dimension in commutative rings

The *dimension* is a useful invariant of algebraic structures, e.g. vector spaces. In this section, we introduce one concept of dimension of commutative rings (there are other sort of dimensions).

7.1 Height of ideals and Krull dimension of rings

Definition 7.1. Let R be a commutative ring.

i. Let P be a prime ideal of R. The *height* of P is:

$$\mathrm{ht}(P) = \sup\{h \mid \exists\, P_0 \subsetneq \cdots \subsetneq P_h = P,\ P_i \in \mathrm{Spec}(R)\}.$$

That is, $\mathrm{ht}(P)$ is the supremum of the lengths of strictly decreasing chains of prime ideals contained in P, possibly $\mathrm{ht}(P) = \infty$ if there exist chains of infinite length.

ii. Let I be an ideal of R. The *height* of I is

$$\mathrm{ht}(I) = \inf\{\mathrm{ht}(P) \mid P \in \mathrm{Spec}(R) \text{ with } I \subseteq P\}.$$

iii. The *Krull dimension* of R is

$$\dim(R) = \sup\{\mathrm{ht}(P) \mid P \in \mathrm{Spec}(R)\}.$$

Equivalently, $\dim(R) = \sup\{\mathrm{ht}(P) \mid P \in \mathrm{MaxSpec}(R)\}$, since every (prime) ideal is contained in a maximal ideal and maximal ideals are prime. Note that maximal ideals in a commutative ring need not have the same height.

Example 7.2.

i. Let R be a PID or a Dedekind domain. Then $\mathrm{Spec}(R) = \mathrm{MaxSpec}(R) \cup \{(0)\}$. So $\dim(R) = 1$ if R is not a field, and $\dim(k) = \mathrm{ht}(0) = 0$ since $\mathrm{Spec}(R) = \{(0)\}$.

ii. Let R be a commutative ring. Then $\mathrm{ht}(0) = 0$. Indeed, if R is an ID, then 0 is prime and contained in every ideal. If R is not an ID, then, by definition, $\mathrm{ht}(0) = \inf\{\mathrm{ht}(P) \mid P \in \mathrm{Spec}(R)\} = 0$ since the height of any minimal prime ideal is 0.

iii. If R is a local ring, with unique maximal ideal I, then $\dim(R) = \mathrm{ht}(I)$, since every prime ideal is contained in I, and therefore any chain of prime ideals can be extended to one ending in I.

The rings that we will consider are the polynomial rings over a field. Intuitively, we may think that $\dim(k[x_1, \ldots, x_n]) = n$, given that $\dim(k) = 0$ and $\dim(k[x]) = 1$. It is indeed correct, and we leave the proof in exercise.

Example 7.3. Let $R = \mathbb{Z}_{(p)}[x]$ be the polynomial ring with coefficients in $\mathbb{Z}_{(p)}$, the localisation of $\mathbb{Z}$ at (p). Let $I = (p, x)$. Note that I is a maximal ideal of R, since $R/I \cong \mathbb{F}_p$ is a field. We calculate $\mathrm{ht}(I) \geq 2$, since $0 \subsetneq (p) \subsetneq I$ is a chain of prime ideals. (It is in fact $= 2$ by Krull's Hauptidealsatz 7.12.) Let $J = (px - 1)$. We claim that $R/J \cong \mathbb{Q}$. Indeed, consider the evaluation map $\epsilon_{\frac{1}{p}} : R \to \mathbb{Q}$, where $\epsilon_{\frac{1}{p}}(f) = f(\frac{1}{p})$ for all $f \in R$. Using the remainder theorem, we see that $\ker(\epsilon_{\frac{1}{p}}) = J$. Moreover, for any $\frac{a}{b} \in \mathbb{Q}$, in reduced form, write $b = p^d t$, where $\gcd(p, t) = 1$. Thus $t \in \mathbb{Z}_{(p)}^{\times}$, and we note that $\frac{a}{b} = \epsilon_{\frac{1}{p}}(at^{-1}x^d) \in \mathrm{im}(\epsilon_{\frac{1}{p}})$. By the isomorphism theorem, $R/J \cong \mathbb{Q}$ is a field and so J is maximal. The polynomial $px - 1$ is irreducible in R, and therefore 0 is the unique prime ideal properly contained in the principal ideal J. It follows that $\mathrm{ht}(J) = 1 < \mathrm{ht}(I)$.

We end this section with a result about IDs of positive dimension. Since fields have dimension 0, we must look for non-fields.

Recall that in a UFD, prime and irreducible elements coincide. Therefore, nonzero prime and maximal ideals coincide in a PID. This proves the following.

Lemma 7.4. *Let R be a PID. Then $\dim(R) = 1$ if and only if R is not a field.*

Hence rings like $\mathbb{Z}, k[x], \mathbb{Z}[\sqrt{d}]$ for $d \in \{-2, -1, 2, 3\}$ are all of dimension 1. The above result is not an if and only if, as shown by the next example.

Example 7.5. Let $R = \mathbb{Z}[i\sqrt{5}] \subseteq \mathbb{C}$. Then R is a Noetherian ID with dimension 1, but it is not a UFD (hence not a PID). Indeed, we have two genuinely distinct factorisations of 9 into products of irreducible elements:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}).$$

We leave the proof of the irreducibility of $3, 2 \pm i\sqrt{5} \in R$ as an exercise.

7.2 Dimension of Artinian commutative rings

We have seen that Artinian commutative rings are 'small' compared to non-Artinian ones. For instance, finite rings and finite dimensional algebras over fields are Artinian. We now consider the dimension of such rings.

Recall that Proposition 2.52 states that prime and maximal ideals coincide in an Artinian commutative ring, and that there are finitely many of them. So, any chain of prime ideals has a single term. That is, every maximal ideal has height 0, and therefore $\dim(R) = 0$, proving the following lemma.

Lemma 7.6. *Let R be a commutative ring. Suppose that R is Artinian. Then $\dim(R) = 0$.*

This observation leads us to a characterisation of Artinian rings.

Theorem 7.7. *Let R be a commutative ring. Then R is Artinian if and only if R is Noetherian and $\dim(R) = 0$.*

Proof. From Proposition 2.45, we know that $\mathrm{Nil}(R)$ is nilpotent whenever R is Noetherian or Artinian, and moreover $\mathrm{Rad}(R) = \mathrm{Nil}(R)$ is an intersection of finitely many ideals if R is Artinian. We also know from Proposition 6.26 that if R is Noetherian, then R has finitely many minimal prime ideals. So if R is Noetherian and of dimension zero, then the minimal prime ideals must also be all the maximal ideals of R. Therefore, we can assume that R is a commutative ring which has finitely many maximal ideals, say $J_1, \ldots, J_s$ with $J_1 \cap \cdots \cap J_s = \mathrm{Nil}(R)$ a nilpotent ideal (Proposition 2.45). So, there exists $n \in \mathbb{N}$ such that $(0) = (J_1 \cdots J_s)^n = J_1^n \cdots J_s^n$. To prove the theorem, is thus equivalent to show that such a ring is Artinian if and only if it is Noetherian.

Pick n minimal such that $(0) = (J_1 \cdots J_s)^n$, and consider the chain of ideals:

$$V_0 = 0 \subseteq \underbrace{J_1^n \cdots J_s^{n-1}}_{V_1} \subseteq \underbrace{J_1^n \cdots J_{s-1}^n J_s^{n-2}}_{V_2} \subseteq \cdots \subseteq \underbrace{J_1^2}_{V_{t-2}} \subseteq \underbrace{J_1}_{V_{t-1}} \subseteq R = V_t$$

where $t = sn+1$. Using that $0 \longrightarrow V_{i-1} \longrightarrow V_i \longrightarrow V_i/V_{i-1} \longrightarrow 0$ is exact for all i, Theorem 2.42 shows that R is Noetherian if and only if every successive quotient V_i/V_{i-1} is Noetherian, and similarly for Artinian. Note that every V_i/V_{i-1} is annihilated by some J_j (e.g. J_1 annihilates R/V_{t-1}). Thus, the R-modules V_i/V_{i-1} are also R/J_j-vector spaces for suitable index j.

It follows that R is Artinian if and only if every V_i/V_{i-1} is a finite dimensional R/J_j-vector space (by Theorem 2.42 and descending chain condition). Thus, R is Artinian if and only if every V_i/V_{i-1} is Noetherian, which holds if and only if R is Noetherian (by Theorem 2.42 and ascending chain condition). □

The above results lead to the following criteria for a local Noetherian commutative ring to be Artinian.

Theorem 7.8. *Let R be a local Noetherian commutative ring, with unique maximal ideal J. TFAE.*

i. R is Artinian.

ii. $\dim(R) = 0$, i.e. J is the unique prime ideal of R.

iii. J is nilpotent.

Proof. (i)$\Longleftrightarrow$(ii) is Theorem 7.7.

Suppose that (ii) holds. Then J must be the unique prime ideal of R, and so $J = \mathrm{Nil}(R)$ is nilpotent by Proposition 2.45.

Suppose that (iii) holds. Then every element of J is nilpotent, thus contained in $\mathrm{Nil}(R)$ by Theorem 1.23, and it follows that $J = \mathrm{Nil}(R)$. Therefore, J is the unique prime ideal of R. □

We conclude with the characterisation of Artinian commutative rings.

Theorem 7.9. *Let R be an Artinian commutative ring. Then R is a direct product of finitely many local Artinian commutative rings.*

Proof. Let $J_1, \ldots, J_s$ be the complete set of distinct maximal ideals of R, as in the proof of Theorem 7.7. By Lemmas 1.6 and 1.24, we have $(0) = J_1^n \cap \cdots \cap J_s^n = J_1^n \cdots J_s^n$, for some $n \in \mathbb{N}$. Building on the proof of Theorem 7.7, we obtain a ring isomorphism $R \cong \prod_{i-1}^{s} R/J_i^n$, where every R/J_i^n is a local Artinian commutative ring. □

7.3 Krull's principal ideal theorem and generalisation

The Krull's principal ideal theorem, or *Hauptidealsatz* is a key result about Noetherian commutative rings. It is named after the German mathematician Wolfgang Krull. We first introduce a construction that is given in Exercise 7.4.

Definition 7.10. Let R be a commutative ring and let P be a prime ideal of R. Write R_P for the localisation of R at P and $\frac{a}{u}$ instead of $[a, u]$ for $a, u \in R,\ u \notin P$. For $n \in \mathbb{N}$, write

$$P^{(n)} = \{a \in R \mid \exists\ b \in R \setminus P, \quad \text{such that} \quad ab \in P^n\} = (P^n)^{ec}$$

for the saturation of P^n with respect to the localisation R_P of R at the multiplicative set $R \setminus P$ (cf. definition 1.39), where the expansion is with respect to the natural injective ring homomorphism $R \to R_P$. The ideal $P^{(n)}$ is a *symbolic power of* P.

By definition, we have $P^n \subseteq P^{(n)} \subseteq P$, from which we deduce that $\sqrt{P^{(n)}} = P$, for all $P \in \mathrm{Spec}(R)$ and all $n \in \mathbb{N}$. Moreover, $P^{(n)}$ is P-primary by Proposition 6.8 applied to the local ring R_P.

We use symbolic powers of prime ideals to show the original Krull's Hauptidealsatz.

Theorem 7.11. *Let R be a Noetherian commutative ring and let (x) be a proper principal ideal of R. Let P be a minimal prime ideal of (x). Then $\mathrm{ht}(P) \leq 1$.*

Before the proof, let us motivate the result with a classical example. Let $R = k[x_1, \ldots, x_n]$ with k a field. Then R is Noetherian commutative. Let (f) be a principal prime ideal of R. Since R is a UFD, f is an irreducible polynomial, and (f) is maximal amonst the proper principal ideals of R. Theorem 7.11 asserts that $\mathrm{ht}(f) = 1$ since $0 \subsetneq (f)$ is a chain of prime ideals of R leading up to (f) of maximal length.

Conversely, if P is a prime ideal of R of height 1, then for any nonzero polynomial $f \in P$, say $f = p_1^{e_1} \cdots p_s^{e_s}$ with p_i irreducible for all i, we must have $p_i \in P$ for some i. Since $\mathrm{ht}(P) = 1$, it follows that $P = (p_i) \supsetneq 0$ is principal.

Proof. Note that if R is Artinian, then $\mathrm{ht}(P) = 0$. There is no loss of generality in replacing R with the localisation R_P of R at P, and so supposing that P is the unique maximal ideal of R. Recall that the prime ideals of R_P are in 1-1 correspondence with the prime ideals of R contained in P. In particular, $\mathrm{ht}(P) = 0$ if and only if R_P is Artinian.

Since $\dim(R) = \mathrm{ht}(P)$, we want to show that $\mathrm{ht}(P) = 1$ if R_P is not Artinian. Suppose that J is a prime ideal properly contained in P. Note that $x \notin J$ since we assume that P is a minimal prime ideal of (x). Consider the descending chain of the symbolic powers of J:

$$J \supseteq J^{(2)} \supseteq J^{(3)} \supseteq \cdots$$

We claim that the chain stabilises. Write $\overline{R} = R/(x)$ for the quotient ring. Similarly, denote with an overbar $\overline{\bullet}$ the image of an element or subset $\bullet \in R$ by the quotient map $R \to \overline{R}$. By Corollary 1.18 and our assumptions, $\overline{P}$ is the unique maximal ideal of $\overline{R}$. In fact, $\overline{P}$ is also a minimal prime ideal of $\overline{R}$ since P is a minimal prime ideal of (x). So $\overline{R}$ is Noetherian (local) of dimension 0, and Theorem 7.7 says that $\overline{R}$ is Artinian. Therefore the descending chain $\overline{J} \supseteq \overline{J^{(2)}} \supseteq \overline{J^{(3)}} \supseteq \cdots$ stabilises. That is, there exists $n \in \mathbb{N}$ such that $\overline{J^{(n)}} = \overline{J^{(m)}}$ for all $m \geq n$, from which it follows that $J^{(n)} \subseteq J^{(m)} + (x)$ for all $m \geq n$.

For any $y \in J^{(n)}$ and $m \geq n$, we can write $y = a + bx$ for some $a \in J^{(m)}$ and some $b \in R$. Since $J^{(m)} \subseteq J^{(n)}$, we have $bx = y - a \in J^{(n)}$. Moreover, since $x \notin J$ and $J^{(n)}$ is P-primary, we must have $b \in J^{(n)}$. Therefore, $J^{(n)} = J^{(m)} + (x)J^{(n)}$ for all $m \geq n$. By Theorem 2.25, it follows that $J^{(n)} = J^{(m)}$ for all $m \geq n$. We also conclude that the expansion JR_J of J along the inclusion of (the local Noetherian commutative ring) R into its localisation at J satisfies $(JR_J)^n = 0$.

Hence R_J is an Artinian commutative local ring, which implies that $\mathrm{ht}(J) = \dim(R_J) = 0$. Since this holds for any prime ideal properly contained in P, we conclude that $\mathrm{ht}(P) = 1$, as required.

□

Theorem 7.11 leads to a generalisation for Noetherian commutative rings. Arguing inductively on the number of generators of ideals, we obtain the following.

Theorem 7.12. *Let R be a Noetherian commutative ring and let I be a proper ideal of R that can be generated by n elements, for some $n \in \mathbb{N}$. Then $\mathrm{ht}(I) \leq n$.*

Proof. Let P be a minimal prime ideal of I, and write $I = (x_1, \ldots, x_n)$. As in the proof of Theorem 7.11, we can suppose that R is local with unique maximal ideal P.

We proceed by induction. If $n = 1$, the result holds by Theorem 7.11. Suppose $n > 1$. Let J be a prime ideal properly contained in P, maximal for this property. That is, if J' is a prime ideal of R with $J \subseteq J' \subsetneq P$, then $J = J'$. Also, there exists i such that $x_i \notin J$. Without loss of generality, suppose that $x_1 \notin J$. Then $J \subsetneq J + (x_1) \subseteq P$ (note that $J + (x_1)$ need not be prime). Consider $\overline{R} = R/\big(J + (x_1)\big)$. Since there are no prime ideals strictly between J and P, the quotient ideal $\overline{P}$ is the unique maximal ideal of $\overline{R}$ and the unique minimal prime, implying that $\overline{P}$ is nilpotent in $\overline{R}$, by Theorem 7.8.

In other words, there exists $m \in \mathbb{N}$ such that $x_j^m = y_j + a_j x_1 \in J + (x_1)$ for some $y_j \in J$ and $a_j \in R$, for all $1 \leq j \leq n$.

Hence, any prime ideal containing $x_1, y_2, \ldots, y_n$ also contains $x_1, \ldots, x_n$.

Let $\widehat{R} = R/(y_2, \ldots, y_n)$. Then $\widehat{P}$ is a minimal prime ideal of the principal ideal $\widehat{(x_1)}$. By Theorem 7.11, we have $\dim(\widehat{P}) \leq 1$, which forces $\dim(\widehat{J}) = 0$. That is, J is a minimal prime ideal of $(y_2, \ldots, y_n)$.

By induction, applied to $\overline{R}$, we have $\mathrm{ht}(J) \leq n - 1$, and the result follows.

□

Since in a Noetherian commutative ring all ideals are finitely generated, we record the following consequence of Theorem 7.12.

Corollary 7.13. *Let R be a Noetherian commutative ring. Then any ideal has finite height.*

A classical application of Krull's Hauptidealsatz is with polynomial rings. If $R = k[x_1, \ldots, x_n]$, we have for instance $\mathrm{ht}(x_1, \ldots, x_n) \leq n$, and since

$$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subset \cdots \subsetneq (x_1, \ldots, x_n)$$

is an irredundant chain of prime ideals, we conclude that $\mathrm{ht}(x_1, \ldots, x_n) = n$.

7.4 Exercises

Exercise 7.1. Let $R = \mathbb{Z}[i\sqrt{5}] \subseteq \mathbb{C}$. Prove that $3, 2 \pm i\sqrt{5} \in R$ are irreducible elements.

Exercise 7.2. Let k be a field and let R be the subring of $k[x]$ formed by all the polynomials $f = \sum_{i=0}^{n} a_i x^i$ with $a_1 = 0$.

i. Prove that R is not a UFD.

ii. Calculate $\dim(R)$.

Exercise 7.3. Let R be a Dedekind domain. Prove that $\dim(R) \leq 1$.

Exercise 7.4. Let R be a commutative ring and let $P \in \mathrm{Spec}(R)$. Prove that the n-th symbolic power of P,

$$P^{(n)} = \{r \in R \mid \exists\, s \notin P \text{ such that } sr \in P^n\} = \bigcup_{s \notin P} (P^n \colon \{s\})$$

is a P-primary ideal, where $(P^n \colon \{s\})$ is the colon ideal (cf. Definition 6.23).

References

[AM] M. Atiyah and I. MacDonald, *Introduction to Commutative Algebra*, Westview Press, 1994.

[Bou] N. Bourbaki, *Algèbre commutative. Èlements de mathématiques*, or English translation; any edition.

[Eis] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer, 1995.

[GP] G.-M. Greuel and G. Pfister, *A Singular introduction to commutative algebra*, Springer, 2002.

[Hun] T. W. Hungerford, *Algebra*, Springer-Verlag 1974.

[Isa] I. M. Isaacs, *Algebra - A graduate course*, Graduate Studies in Mathematics 100, American Mathematical Society, 2009.

[Jac] N. Jacobson, *Basic Algebra I and II*, W. H. Freeman and Company, 1985 and 1989.

[Lan] S. Lang, *Algebra*, Graduate Texts in Mathematics 211 (revised 3rd edition), Springer, 2002; or Addison-Wesley Pub. Co, 1965 (or other edition).

[LQ] H. Lombardi and C. Quitté, *Commutative algebra: Constructive methods. Finite projective modules*, Algebra and Applications, Springer, 2015.

[Rei] M. Reid, *Undergraduate commutative algebra*, London Mathematical Society Student Texts **29**, Cambridge University Press, 1995.

[ZZZ] ...and many more, including James S. Milne's notes `https://www.jmilne.org/math/xnotes/CA.pdf`!

Index