MATH5253M: Commutative algebra and algebraic geometry

Eleonore Faber

e.m.faber@leeds.ac.uk
www.maths.leeds.ac.uk/$\sim$pmtemf

adapted from O.H. King and K. Houston

2018

Contents

Introduction . . . 2

I Commutative Algebra **3**

1 Revision of rings . . . 3
2 Revision of ideals . . . 5
3 Prime ideals . . . 7
4 Maximal ideals . . . 9
5 Polynomial ring $K[x_1, \ldots, x_n]$ . . . 11
6 Localisation . . . 13
7 The radical, nilradical and Jacobson radical . . . 16
8 Modules . . . 18
9 Nakayama's Lemma . . . 20
10 Exact sequences . . . 21
11 Free modules . . . 25
12 Noetherian rings and modules . . . 27
13 Hilbert's Basis Theorem . . . 29
14 Primary decomposition . . . 30
15 Noether normalisation and Hilbert's Nullstellensatz . . . 34

Introduction

Books:

- Miles Reid - Undergraduate algebraic geometry, LMS Student Texts 12, CUP, 1988.
- Miles Reid - Undergraduate commutative algebra, LMS Student Texts 29, CUP, 1995.
- M.F. Atiyah and I.G. MacDonald - Introduction to commutative algebra, Westview Press, 1994
- David Cox, John Little, and Donal O'Shea - Ideals, Varieties, and Algorithms, UTM Springer, Third Edition, 2007.
- Rodney Sharp - Steps in commutative algebra 2nd Ed, LMS Student Texts 51, CUP, 2000.
- Robin Hartshorne - Algebraic Geometry, Springer Verlag, 1997. (First chapter only)
- W. Fulton - Algebraic Curves.

Part I

Commutative Algebra

1 Revision of rings

Definition 1.1. A *ring* is a triple $(R, +, \cdot)$ of a set R and two binary operations

$$\begin{aligned} + : R \times R &\longrightarrow R \quad \text{(addition)} \\ \cdot : R \times R &\longrightarrow R \quad \text{(multiplication)} \end{aligned}$$

such that the following hold:

(i) $(R, +)$ is an abelian group, with identity $0 = 0_R$;

(ii) there is an element $1 = 1_R$ such that $1 \cdot r = r \cdot 1 = r$ for all $r \in R$;

(iii) $\cdot$ is associative, i.e. $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ for all $r, s, t \in R$;

(iv) $\cdot$ distributes over $+$, i.e. $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(s + t) \cdot r = s \cdot r + t \cdot r$ for all $r, s, t \in R$.

We will often abbreviate the triple $(R, +, \cdot)$ to just R with the operations implicit, and moreover the multiplication $r \cdot s$ to just rs.

Definition 1.2. A ring R is called *commutative* if $rs = sr$ for all $r, s \in R$.

Remark. In this course all rings will be commutative rings, and so hereafter we will take "ring" to mean "commutative ring".

Example 1.3. (i) $\mathbb{Z}$, the set of integers.

(ii) $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, the integers modulo n.

(iii) $\mathbb{R}$, the set of real numbers.

(iv) $\mathbb{C}$, the set of complex numbers.

(v) $\mathcal{C}[0, 1]$, the set of continuous functions on $[0, 1]$.

(vi) Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

(vii) Let X be any set, and define $\mathfrak{F}_X = \mathbb{R}^X = \{\text{functions } f : X \longrightarrow \mathbb{R}\}$. Define $+, \cdot : \mathfrak{F}_X \times \mathfrak{F}_X \longrightarrow \mathfrak{F}_X$ by

$$\begin{aligned} (f + g) : X &\to \mathbb{R} \\ x &\mapsto f(x) + g(x), \end{aligned}$$

$$\begin{aligned} (f \cdot g) : X &\to \mathbb{R} \\ x &\mapsto f(x)g(x). \end{aligned}$$

Then $\mathfrak{F}_X$ is a commutative ring, with additive identity $0_{\mathfrak{F}_X} : x \mapsto 0$ and multiplicative identity $1_{\mathfrak{F}_X} : x \mapsto 1$.

(viii) We can also construct new rings from old ones. Let R be any commutative ring, and define

$$R[x] = \{\text{polynomials in } x \text{ with coefficients in } R\} = \left\{ \sum_{i=0}^{n} r_i x^i : n \in \mathbb{N} \text{ and } r_i \in R \ \forall i \right\}.$$

This is also a commutative ring. We can then define $R[x_1, \dots, x_n]$ inductively by

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

This is just polynomials in the variables $x_1, \dots, x_n$ with coefficients in R.

(ix) $R[[x]] = \{\text{formal power series in } x \text{ with coefficients in } R\} = \left\{ \sum_{i=0}^{\infty} r_i x^i : r_i \in R \ \forall i \right\}$. Note that these are formal objects, not necessarily functions from R to R. For instance, $\sum_{i=0}^{\infty} x^i$ is an element of $\mathbb{R}[[x]]$, but we cannot evaluate this at $x = 1$ so it does not define a function $\mathbb{R} \to \mathbb{R}$.

Definition 1.4. A *field* is a ring K where every element other than 0_K has a multiplicative inverse. Formally, for each $r \in K \backslash \{0\}$ there exists an $r^{-1} \in K \backslash \{0\}$ such that $rr^{-1} = r^{-1}r = 1_K$.

Example 1.5. (i) Familiar fields are $\mathbb{C}, \mathbb{R}, \mathbb{Q}$. Another example is $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ for any prime p.

(ii) $\mathbb{Z}$ itself is not a field, nor is the set $\mathbb{Z}[i]$ of Gaussian integers. For instance, $2 + 0i$ has no inverse. In fact the units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

We will now see another way of constructing rings and fields from old ones:

Example 1.6. Let R, S be rings. The Cartesian product $R \times S = (R \times S, +, \cdot)$ of R and S is also a ring, where we define

$$\begin{aligned}(r_1, s_1) + (r_2, s_2) &= (r_1 + r_2, s_1 + s_2) \\ (r_1, s_1) \cdot (r_2, s_2) &= (r_1 r_2, s_1 s_2).\end{aligned}$$

for all $r_1, r_2 \in R$, $s_1, s_2 \in S$. We have $0_{R \times S} = (0_R, 0_S)$ and $1_{R \times S} = (1_R, 1_S)$. Note that if K and L are fields then $K \times L$ is not a field, for instance $(0, 1)$ has no multiplicative inverse.

Definition 1.7. A subset $S \subseteq R$ of a ring R is called a *subring* if $(S, +)$ is a subgroup of $(R, +)$, $1_R \in S$ and S is closed under multiplication. Similarly, if K is a field then a subset $L \subseteq K$ is called a *subfield* if it is a subring of K and $r^{-1} \in L$ for all non-zero $r \in L$.

Example 1.8. Let $R = \mathbb{R}$ and $S = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$. Clearly $0 = 0 + \sqrt{5}, 1 = 1 + 0\sqrt{5} \in S$, so we will check that it is additively and multiplicatively closed. For all $a, b, c, d \in \mathbb{R}$, we have

$$(a + b\sqrt{5}) + (c + d\sqrt{5}) = (a + c) + (c + d)\sqrt{5} \in S,$$

$$\begin{aligned}(a + b\sqrt{5})(c + d\sqrt{5}) &= ac + ad\sqrt{5} + bc\sqrt{5} + 5bd \\ &= (ac + 5bd) + (ad + bc)\sqrt{5} \in S.\end{aligned}$$

Similarly if $R = \mathbb{C}$, then $S = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is a subring. Rings like these play an important role in areas of number theory.

Definition 1.9. Let R, S be rings. A *ring homomorphism* from R to S is a map $\varphi : R \to S$ such that for all $r_1, r_2 \in R$:

(i) $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$;

(ii) $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$;

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

If φ is bijective then we say φ is an *isomorphism*.

Exercise (Exercise sheet 0)**.** If $\varphi : R \to S$ is a ring isomorphism, prove that $\varphi^{-1} : S \to R$ is a ring homomorphism (and hence also an isomorphism).

Definition 1.10. Let $\varphi : R \to S$ be a ring homomorphism. The *kernel* of φ, denoted $\operatorname{Ker}\varphi$, is the set

$$\operatorname{Ker}\varphi = \{r \in R : \varphi(r) = 0_S\}.$$

The *image* of φ, denoted $\operatorname{Im}\varphi$, is the set

$$\operatorname{Im}\varphi = \{\varphi(r) : r \in R\}.$$

The proof of the following proposition is left as an easy exercise:

Proposition 1.11. *(i)* $\operatorname{Im}\varphi$ *is a subring of* S.

(ii) $\operatorname{Ker}\varphi$ *is not necessarily a subring of* R.

Proof. Exercise. □

2 Revision of ideals

That $\operatorname{Ker}\varphi$ is not a subring of R causes us problems if we wish to introduce quotient rings like we introduced quotient groups. Note that if H is a subgroup of G then G/H does not necessarily exist. Note also that dealing with commutative groups circumvents this problem, but that is not the case when dealing with rings. The "correct" notion of a substructure that allows us to take quotients is that of an ideal.

Definition 2.1. Let R be a ring. A subset $I \subseteq R$ is called an *ideal* if:

(i) $I \neq \emptyset$;

(ii) for all $x, y \in I$, $x - y \in I$;

(iii) for all $x \in I$ and $r \in R$, $rx \in I$.

We write $I \trianglelefteq R$ to mean I is an ideal of the ring R.
If $I \neq R$, then we say that I is a *proper ideal* of R.

Example 2.2. (i) Let R be a ring. Then $\{0_R\}$ and R are both ideals of R, usually referred to as trivial ideals.

(ii) For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

(iii) For a ring homomorphism $\varphi : R \to S$, $\operatorname{Ker}\varphi$ is an ideal of R. Indeed let $x, y \in \operatorname{Ker}\varphi$ and $r \in R$, then

$$\begin{aligned} \varphi(0) = 0 \text{ so } 0 \in \operatorname{Ker}\varphi \quad (\operatorname{Ker}\varphi \neq \emptyset), \\ \varphi(x+y) = \varphi(x) + \varphi(y) = 0 + 0 = 0 \text{ so } x + y \in \operatorname{Ker}\varphi, \\ \varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0 = 0 \text{ so } rx \in \operatorname{Ker}\varphi. \end{aligned}$$

(iv) A crucial example for algebraic geometry, and one we will encounter many times later in the course, is the following. Let K be a field (usually $\mathbb{R}$ or $\mathbb{C}$), $V \subseteq K^n$ be a set and $R = K[X_1, \dots, X_n]$. Then

$$I(V) = \{f \in R : f(v) = 0 \text{ for all } v \in V\}$$

is an ideal of R.

Definition 2.3. Let A be a non-empty subset of a ring R. The *ideal generated by* A, denoted $\langle A \rangle$, is the set of all elements

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} r_i a_i : n \in \mathbb{N},\ r_1, \ldots, r_n \in R,\ a_1, \ldots, a_n \in A \right\}.$$

We say an ideal I is *finitely generated* if there exists a finite subset $A \subseteq R$ such that $I = \langle A \rangle$. If $I = \langle a \rangle$ is generated by one element, then I is called a *principal ideal*.

Example 2.4. Let $R = K[x,y,z]$, and $I = \langle x,y,z \rangle$. Then I consists of all polynomials in $K[x,y,z]$ without constant term. One can show that $I = J$, where $J = \langle x+y, y+z^2, z \rangle$.

We can also perform operations on ideals as per the following proposition.

Proposition 2.5. *Let I, J be ideals of a ring R. The following are then also ideals of R:*

(i) $I \cap J = \{x : x \in I \text{ and } x \in J\}$, the intersection of I and J;

(ii) $IJ = \langle \{xy : x \in I, y \in J\} \rangle$, the product of I and J;

(iii) $I + J = \langle I \cup J \rangle$, the sum of I and J;

(iv) $(I : J) = \{r \in R : rJ \subseteq I\}$, *the* ideal quotient *of I and J.*

Proof. Exercise. See Exercise Sheet 1. □

In algebraic geometry the following type of ideals will play an important role:

Definition 2.6. Let $I \subseteq R$ be an ideal in a ring. Then

$$\sqrt{I} := \{x \in R : \text{there exists an } n \in \mathbb{N} \text{ such that } x^n \in I\}$$

is an ideal, called the *radical of I*. If $I = \sqrt{I}$, then I is called a *radical ideal*.

See exercise sheet 1 for a proof that $\sqrt{I}$ is an ideal in R.

Example 2.7. (1) Let $I = 288\mathbb{Z}$ in $\mathbb{Z}$. Then $\sqrt{I} = 6\mathbb{Z}$ (see this from $288 = 2^5 3^2$), and so I is not a radical ideal.
(2) Let $I = \langle x^2, y^2 \rangle$ in $K[x,y]$. It is clear that $\sqrt{I} \supseteq \langle x, y \rangle$. For the other inclusion note that a polynomial $P(x,y)$ is in $\sqrt{I}$ if and only if there exists an n, such that $P^n(x,y)$ is in I, that is P^n does not have a constant term. But $P(0,0)^n = 0$ if and only if $P(0,0) = 0$, thus P itself must be without nonconstant term, thus $P(x,y) \in I$.

We will now move on to quotient rings.

Definition 2.8. Let I be an ideal of a ring R. A *coset* of I in R is a set

$$r + I = \{r + x : x \in I\}$$

for some $r \in R$. This may also be denoted by $\bar{r}$, and we denote by R/I the set of cosets of I in R.

The following proposition is straightforward:

Proposition 2.9. *(i) Two cosets are either equal or disjoint, and the union of all cosets is R. We say that the cosets* partition *R.*

(ii) Cosets $r + I$ and $s + I$ are equal if and only if $r - s \in I$.

(iii) We can define multiplication and addition on R/I by setting $(r+I) + (s+I) = (r+s) + I$ and $(r+I)(s+I) = rs + I$.

(iv) The additive and multiplicative identities of R/I are $0 + I = I$ and $1 + I$ respectively.

This proposition shows that we have a ring structure on R/I, with much of the structure inherited from the ring structure on R.

Proposition 2.10. *Let I be an ideal of a ring R. Define $\varphi : R \to R/I$ by $\varphi(r) = r + I$. Then:*

(i) *φ is a ring homomorphism (called the* quotient homomorphism*);*

(ii) $\operatorname{Ker} \varphi = I$*;*

(iii) *there is a bijection between ideals of R/I and the ideals of R which contain I, given by*

$$J \subseteq R/I \longmapsto \varphi^{-1}(J) = \{r \in R : r + I \in J\}$$
$$I \subseteq K \subseteq R \longmapsto \varphi(K) = \{r + I : r \in K\}.$$

Proof. (i) See Exercise Sheet 1.

(ii) See Exercise Sheet 1.

(iii) For an ideal K such that $I \subseteq K \subseteq R$, we first show that $\varphi(K)$ is an ideal of R/I (note that this may not be true for any φ). Clearly $\varphi(K) \neq \emptyset$, as $\varphi(I) = I \in \varphi(K)$. For any two cosets $r + I, s + I \in \varphi(K)$ we have $r, s \in K$, and since K is an ideal then $r - s \in K$. Hence $(r + I) - (s + I) = (r - s) + I \in \varphi(K)$. If now we also choose any $t + I \in R/I$ then $(t + I)(r + I) = tr + I \in \varphi(K)$, since $tr \in K$ again due to K being an ideal of R.

We now show that the assignment $K \longmapsto \varphi(K)$ is injective. Suppose $K \neq K'$ are both ideals of R containing I, then without loss of generality there is some $r \in K$ such that $r \notin K'$. We clearly have $r + I \in \varphi(K)$. We will show that $r + I \notin \varphi(K')$, thus $\varphi(K) \neq \varphi(K')$. Assume for a contradiction that $r + I \in \varphi(K')$, then $r + I = s + I$ for some $s \in K'$. By the equality rule for cosets, we have $r - s \in I \subseteq K'$, and hence $(r - s) + s = r \in K'$, a contradiction.

Finally, we show the map $K \longmapsto \varphi(K)$ is surjective. Given an ideal $J \subseteq R/I$ we clearly have $\varphi(\varphi^{-1}(J)) = J$, so we must show that $\varphi^{-1}(J)$ is an ideal of R containing I. The containment is easy, since $I = \varphi^{-1}(0) \subseteq \varphi^{-1}(J)$. If now $r, s \in \varphi^{-1}(J)$, then $r + I, s + I \in J$ and hence $(r - s) + I \in J$. Therefore $r - s \in \varphi^{-1}(J)$. Similarly if $t \in R$ then $t + I \in R/I$ and $(t + I)(r + I) = tr + I \in J$, hence $tr \in \varphi^{-1}(J)$.

□

Theorem 2.11. *Let $\varphi : R \to S$ be a ring homomorphism. Then $\overline{\varphi} : R/\operatorname{Ker} \varphi \to \operatorname{Im} \varphi$ given by $\overline{\varphi}(r + \operatorname{Ker} \varphi) = \varphi(r)$ is an isomorphism.*

Proof. See Exercise Sheet 1 (remember to check that this is well defined!). □

3 Prime ideals

Definition 3.1. An ideal $\mathfrak{p}$ of R is called a *prime* ideal if;

(i) $\mathfrak{p} \neq R$;

(ii) $xy \in P \implies x \in \mathfrak{p}$ or $y \in P$.

The first example below explains the name of these ideals.

Example 3.2. (i) The ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is prime if and only if n is prime (Exercise).

(ii) The ideal $\langle f \rangle$ of $\mathbb{C}[x]$ is prime if and only if f is irreducible, i.e. f cannot be written as the product of two polynomials of positive degree.

Proposition 3.3. *Let $\varphi : R \to S$ be a ring homomorphism. If $\mp \subseteq S$ is a prime ideal, then $\varphi^{-1}(\mathfrak{p}) \subseteq R$ is a prime ideal.*

Proof. Let $x, y \in R$ be such that $xy \in \varphi^{-1}(\mathfrak{p})$, i.e. $\varphi(xy) \in \mathfrak{p}$. Now $\varphi(xy) = \varphi(x)\varphi(y)$, and since $\mathfrak{p}$ is prime we therefore have either $\varphi(x) \in \mathfrak{p}$ or $\varphi(y) \in \mathfrak{p}$. Hence either $x \in \varphi^{-1}(\mathfrak{p})$ or $y \in \varphi^{-1}(\mathfrak{p})$. $\square$

Proposition 3.4. *Let I be an ideal of a ring R. If $\mathfrak{p}$ is a prime ideal of R containing I, then the image of $\mathfrak{p}$ in R/I is also prime.*

Proof. Denote by $\overline{\mathfrak{p}}$ the image of $\mathfrak{p}$ in R/I. Suppose $x + I, y + I \in R/I$ are such that $(x + I)(y + I) \in \overline{\mathfrak{p}}$. Then $xy + I \in \overline{\mathfrak{p}}$, so there is some $p \in \mathfrak{p}$ such that $xy - p \in I \subseteq \mathfrak{p}$. Therefore $xy \in \mathfrak{p}$, so either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ as $\mathfrak{p}$ is prime, thus either $x + I \in \overline{\mathfrak{p}}$ or $y + I \in \overline{\mathfrak{p}}$. $\square$

Remark 3.5. These two propositions show that the bijection between ideals of R/I and ideals of R containing I restricts to a bijection between *prime* ideals of R/I and *prime* ideals of R containing I.

Definition 3.6. A ring R is an *integral domain* if:

(i) $R \neq \{0\}$;

(ii) for all $r, s \in R$, $rs = 0 \implies r = 0$ or $s = 0$, i.e. there are no non-zero zero divisors.

Example 3.7. (i) $\mathbb{Z}$ and $K[x]$ are integral domains.

(ii) $R = K[x]/\langle x^2 \rangle$ is not an integral domain, since $\overline{x} \neq \overline{0}$ in R but $\overline{x} \cdot \overline{x} = \overline{0}$.

(iii) $\mathbb{Z}_4$ is not an integral domain, as $(2 + 4\mathbb{Z})(2 + 4\mathbb{Z}) = 4 + 4\mathbb{Z} = 0$.

(iv) $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is an integral domain but $\mathbb{C}[x]/\langle x^2 + 1 \rangle$ is not. (Why?)

(v) $\mathbb{R}[x, y]/\langle x^2 - y^2 \rangle$ is not an integral domain. Geometrically, $V(\langle x^2 - y^2 \rangle)$ corresponds to two crossing lines in $\mathbb{R}^2$. The ring $\mathbb{R}[x, y]/\langle x^2 - y^2 \rangle$ is an integral domain. Geometrically, $V(\langle x^2 - y^2 \rangle)$ is a cusp in $\mathbb{R}^2$, an irreducible curve (see later about the connection between irreducible algebraic varieties and prime ideals).

Theorem 3.8. *Let $I \subsetneq R$ be an ideal. Then I is prime iff R/I is an integral domain.*

Proof. Suppose I is prime. Then since $I \neq R$ we have $R/I \neq \{0\}$. Now suppose $a + I$ is non-zero in R/I and there is some $b + I \in R/I$ such that $(a + I)(b + I) = I$. Then $ab + I = I$ and $ab \in I$. Since I is prime we have either $a \in I$ or $b \in I$, but since $a + I \neq I$ this forces $b \in I$. Hence $b + I = 0$ in R/I, and R/I is an integral domain.

Suppose now that R/I is an integral domain. Since $R/I \neq \{0\}$ we must have $I \neq R$. Now let $ab \in I$ for some $a, b \in R$, then $ab + I = (a + I)(b + I) = I$. Since R/I is an integral domain, we must have either $a + I = I$ or $b + I = I$, and hence either $a \in I$ or $b \in I$. Therefore I is prime. $\square$

Theorem 3.9. *Let R be a ring, $I_1, \ldots, I_n \subseteq R$ be ideals, and $\mathfrak{p} \subseteq R$ be a prime ideal. Then the following are equivalent:*

(i) $I_j \subseteq \mathfrak{p}$ *for some* $1 \leqslant j \leqslant n$*;*

(ii) $I_1 \cap \cdots \cap I_n \subseteq \mathfrak{p}$*;*

(iii) $I_1 \ldots I_n \subseteq \mathfrak{p}$.

Proof. $(i) \implies (ii) \implies (iii)$ are trivial.

$(iii) \implies (i)$: Assume that $I_1 \ldots I_n \subseteq \mathfrak{p}$ but for all $1 \leqslant j \leqslant n$ we can choose $a_j \in I_j \backslash \mathfrak{p}$. Then $a_1 \ldots a_n \in I_1 \ldots I_n \backslash \mathfrak{p}$ as $\mathfrak{p}$ is prime, a contradiction. $\square$

4 Maximal ideals

Definition 4.1. An ideal I of a ring R is called a *maximal* ideal if:

(i) $I \neq R$;

(ii) there is no ideal J of R such that $I \subsetneq J \subsetneq R$.

Example 4.2. (i) $p\mathbb{Z} \subseteq \mathbb{Z}$ is a maximal ideal for p prime (we will see a proof of this soon).

(ii) $\langle X \rangle \subseteq R[X, Y]$ is not maximal, as $\langle X \rangle \subsetneq \langle X, Y \rangle \subsetneq R[X, Y]$.

Theorem 4.3. *Maximal ideals are prime.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of a ring R and suppose $ab \in \mathfrak{m}$ for some $a, b \in R$. If neither a nor b are in $\mathfrak{m}$ then both $\langle a \rangle + \mathfrak{m}$ and $\langle b \rangle + \mathfrak{m}$ are strictly bigger than $\mathfrak{m}$. As $\mathfrak{m}$ is maximal, we must then have $\langle a \rangle + \mathfrak{m} = \langle b \rangle + \mathfrak{m} = R$. But now

$$\begin{aligned} R &= RR \\ &= (\langle a \rangle + \mathfrak{m})(\langle b \rangle + \mathfrak{m}) \\ &= \mathfrak{m}^2 + \langle a \rangle \mathfrak{m} + \langle b \rangle \mathfrak{m} + \langle ab \rangle \\ &\subseteq \mathfrak{m} \neq R, \end{aligned}$$

which is a contradiction. □

Proposition 4.4. *Let R be a ring. Then:*

(i) R is a field iff $\{0\}$ and R are the only ideals of R;

(ii) an ideal $I \subseteq R$ is maximal if and only if R/I is a field.

Proof. (i) Assume R is a field and let $I \subseteq R$ be a non-zero ideal. Choose $r \in I \backslash \{0\}$, then r has an inverse $r^{-1} \in R$. Hence $r^{-1}r = 1 \in I$, so $I = R$.

Conversely suppose $\{0\}$ and R are the only ideals of R, and choose $r \in R \backslash \{0\}$. Then $\langle r \rangle = R$ and so there exists some $s \in R$ such that $sr = 1$, i.e. r has an inverse $r^{-1} = s$. Therefore R is a field.

(ii) If I is maximal then by Proposition 2.10, R/I has no ideals other than $\{I\}$ and R/I. Therefore R/I is a field by (i).

If now R/I is a field then again by Proposition 2.10 and (i), any ideal of R which contains I must either be I or R, so I is maximal.

□

Remark. Let $\varphi : R \to S$ be a ring homomorphism. Unlike the situation with prime ideals, $\mathfrak{m} \subseteq S$ maximal does not imply that $\varphi^{-1}(\mathfrak{m})$ is maximal. For instance, let $\varphi : \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. Then $\{0_\mathbb{Q}\} \subseteq \mathbb{Q}$ is maximal as $\mathbb{Q}$ is a field, but $\varphi^{-1}(\{0_\mathbb{Q}\}) = \{0_\mathbb{Z}\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$, so $\varphi^{-1}(\{0_\mathbb{Q}\})$ is not maximal.

However we do have the following result which is analogous to Remark 3.5:

Proposition 4.5. *The bijection between ideals of R/I and ideals of R containing I restricts to a bijection between maximal ideals of R/I and maximal ideals of R containing I.*

Proof. Exercise. □

We will soon show that every proper ideal is contained in some maximal ideal. In order to prove this however, we must take a brief diversion into set theory.

A *partially ordered set* or *poset* $(\Sigma, \leqslant)$ is a set Σ and a binary relation $\leqslant \subseteq \Sigma \times \Sigma$ which is:

(i) reflexive, i.e. $x \leqslant x \ \forall x \in \Sigma$;

(ii) transitive, i.e. $x \leqslant y$ and $y \leqslant z \implies x \leqslant z \ \forall x, y, z \in \Sigma$;

(iii) antisymmetric, i.e. $x \leqslant y$ and $y \leqslant x \implies x = y \ \forall x, y \in \Sigma$.

A subset $S \subseteq \Sigma$ is *totally ordered* if for all $s, t \in S$ we have either $s \leqslant t$ or $t \leqslant s$ (or both).
Given a subset $S \subseteq \Sigma$, an element $u \in \Sigma$ is an *upper bound* for S if $s \leqslant u$ for all $s \in S$.
A *maximal element* of Σ is an element $m \in \Sigma$ such that there is no $s \in S$ with $m \leqslant s$ and $m \neq s$.

Example. A poset without a maximal element is the set $(\mathbb{Z}, \leqslant)$.

Theorem (Zorn's Lemma)**.** *Suppose that $(\Sigma, \leqslant)$ is a non-empty poset and that any totally ordered subset $S \subseteq \Sigma$ has an upper bound in Σ. Then Σ has a maximal element.*

This is equivalent to the Axiom of Choice, and we take it as an axiom in ZFC (where we generally do maths).

We can now prove the following:

Proposition 4.6. *Let R be a non-zero ring. Then every proper ideal I is contained in a maximal ideal.*

Proof. Let Σ be the set of ideals $J \subsetneq R$ containing I, ordered by inclusion $\subseteq$. Then $(\Sigma, \subseteq)$ is a non-empty poset, since $I \in \Sigma$. If $\{J_\lambda : \lambda \in \Lambda\}$ is a totally ordered subset of Σ then clearly $J^* = \cup_{\lambda \in \Lambda}$ is a proper ideal of R containing I, and moreover J^* is an upper bound for $\{J_\lambda : \lambda \in \Lambda\}$. By Zorn's Lemma, Σ then has a maximal element. But a maximal element of Σ is an ideal $\mathfrak{m} \neq R$ containing I with no proper ideals J containing it, so is a maximal ideal containing I. $\square$

This proposition shows that we usually have lots of maximal ideals, even if they can be hard to find.

Example 4.7. Let K be a field, $R = K[x_1, \ldots, x_n]$ and $a_1, \ldots, a_n \in K$. Then $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is a maximal ideal. If it wasn't, then there would exist a polynomial $f \in R$ such that $f \neq \mathfrak{m}$ and $\langle f \rangle + \mathfrak{m} \subsetneq R$. Applying the division algorithm n times gives

$$f = f_1(x_1 - a_1) + \cdots + f_n(x_n - a_n) + b,$$

where $f_i \in K[x_i, x_{i+1}, \ldots, x_n] \subseteq R$ for each $1 \leqslant i \leqslant n$ and $b \in K$. Since $f \notin \mathfrak{m}$, we must have $b \neq 0$ and so b has an inverse b^{-1}. Therefore $1 = b^{-1}\left(f - f_i(x_1 - a_1) - \cdots - f_n(x_n - a_n)\right) \in \langle f \rangle + \mathfrak{m}$ and so $\langle f \rangle + \mathfrak{m} = R$, a contradiction.

Are these the only maximal ideals of $K[x_1, \ldots, x_n]$? The answer is yes when K is algebraically closed, but we need a bit more theory in order to prove this.
In some cases, there are far fewer maximal ideals.

Definition 4.8. A ring R is called a *local ring* if it has precisely one maximal ideal $\mathfrak{m}$. We usually denote this ring by the pair $(R, \mathfrak{m})$.

Example 4.9. (1) If K is a field, then K is a local ring, with maximal ideal $\{0\}$.
(2) The formal power series ring $K[[x]]$ is local with maximal ideal $\langle x \rangle$ (Exercise!).

In order to talk about the prime and maximal ideals in a ring, we introduce the following notions, which will play a crucial role in algebraic geometry, since they allow to define the Zariski topology (see later!).

Definition 4.10. Let R be a ring, then

$$\operatorname{Spec}(R) = \{\mathfrak{p} \subseteq R : \mathfrak{p} \text{ is a prime ideal in } R\}$$

is called the *spectrum of* R. The set of all maximal ideals of R is called the *maximal spectrum of* R and denoted by $\operatorname{maxSpec}(R)$.

Example 4.11. Let $R = K[x]$ the polynomial ring in one variable over a field K. Then R is a principal ideal ring, and an ideal $I \subseteq R$ is maximal if and only if I is prime if and only if I is generated by an irreducible polynomial $P(x)$. Thus we have

$$\operatorname{Spec}(R) = \operatorname{maxSpec}(R) = \{\langle P(x)\rangle \subseteq K[x] : P(x) \text{ is irreducible } \}\,.$$

If K is algebraically closed, then $P(x) \in K[x]$ is irreducible if and only if $\deg(P(x)) = 1$, that is, $P(x)$ can be written as $P(x) = x - \lambda$, where $\lambda \in K$. Thus we get

$$\operatorname{Spec}(R) = \{\langle x - \lambda\rangle : \lambda \in K\}\,.$$

This means that elements in $\operatorname{Spec}(R)$ are in bijection with elements of K, or said differently, with points in $\mathbb{A}^1_K$, the affine line.
More generally, one can show that elements of $\operatorname{maxSpec}(K[x_1,\ldots,x_n])$ for K algebraically closed are in bijection with points in $\mathbb{A}^n_K = K^n$. (cf. example 4.7)

5 Polynomial ring $K[x_1,\ldots,x_n]$

We have already defined the polynomial ring in n variables over a field K via: $K[x_1,\ldots,x_n] = (K[x_1,\ldots,x_{n-1}])[x_n]$. In the following we study some properties of these rings and in particular define monomial orderings, that will be useful when dealing with the question on defining a division algorithm on $K[x_1,\ldots,x_n]$.
First note that the elements of $K[x_1,\ldots,x_n]$ are finite sums of the form $P(x_1,\ldots,x_n) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha \underline{x}^\alpha$. (We sometimes write short $K[\underline{x}]$ for $K[x_1,\ldots,x_n]$ and $\underline{x}^\alpha$ for $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$). An element $\underline{x}^\alpha$ of $K[\underline{x}]$ is called a *monomial*. The a_α in $P(\underline{x}) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha \underline{x}^\alpha$ are called *coefficients of* P.

One can distinguish between polynomials $P(\underline{x})$ as elements of the polynomial ring $K[\underline{x}]$ or as *polynomial maps*, that is, any P gives a map

$$P : K^n \to K, (a_1,\ldots,a_n) \mapsto P(a_1,\ldots,a_n)\,.$$

Given polynomials $P_1(\underline{x}),\ldots,P_m(\underline{x}) \in K[\underline{x}]$ one defines

$$V(P_1,\ldots,P_m) = \{(a_1,\ldots,a_n) \in K^n : P_i(a_1,\ldots,a_n) = 0 \text{ for all } i = 1,\ldots,m\}\,,$$

the *vanishing set (or zero-set) of* $P_1,\ldots,P_m$ in K^n. One writes $\mathbb{A}^n_K := K^n = \{(a_1,\ldots,a_n) \in K^n\}$ for the *affine n-space over* K. If $X \subseteq \mathbb{A}^n_K$ is of the form $X = V(P_1,\ldots,P_m)$, then X is called an *algebraic set* and the $P_1,\ldots,P_m$ *define* X. If $X \subseteq \mathbb{A}^n_K$ is an algebraic set, then

$$I(X) = \{P(\underline{x}) \in K[x_1,\ldots,x_n] : P(a_1,\ldots,a_n) = 0 \text{ for all } (a_1,\ldots,a_n) \in X\}$$

is an ideal in $K[x_1,\ldots,x_n]$, the *defining ideal of* X. Later we will study the relation between ideals in $K[x_1,\ldots,x_n]$ and algebraic sets in $\mathbb{A}^n_K$.

Example 5.1. (1) $X = V(x^3 - y^2) \subseteq \mathbb{A}^2_{\mathbb{R}}$ defines a *cusp*. This is an irreducible curve in the real plane.
(2) $X = V(x^2 + y^2) \subseteq \mathbb{A}^2_{\mathbb{R}}$ is the point $\{(0,0)\}$. However, $V(x^2 + y^2) \subseteq \mathbb{A}^2_{\mathbb{C}}$ consists of the two lines $\{x + iy = 0\}$ and $\{x - iy = 0\}$.
(3) Consider $J = \langle x^3, xy, y^2, z\rangle \subseteq K[x,y,z]$. Then one can see that $V(J) = \{(0,0,0)\}$, but $I(V(J)) = \langle x,y,z\rangle \supsetneq J$.

Consider the polynomial ring $K[x_1, \ldots, x_n]$. We define the *(total) degree* of a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ as $|\alpha| = \alpha_1 + \cdots \alpha_n$. Consequently, the *degree* of a polynomial $P(x_1, \ldots, x_n) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \underline{x}^\alpha$ is $\deg(P) = \max\{|\alpha| : a_\alpha \neq 0\}$. The *order* of P is $\mathrm{ord}(P) = \min\{|\alpha| : a_\alpha \neq 0\}$.
We can write $P(\underline{x}) = \sum_d P^{(d)}$, where $P^{(d)}$ is the sum of all monomials in $P(\underline{x})$ with $\deg(\underline{x}^\alpha) = d$. If $P \neq 0$, then we say that $P(\underline{x})$ is *homogeneous of degree d* if $P(\underline{x}) = P^{(d)}$.

Example 5.2. (1) $P : \mathbb{R}^3 \to \mathbb{R} : (x, y, z) \mapsto x^2y + xyz + x^2y^2 - \sqrt{2}z^3$ corresponds to the polynomial $P \in \mathbb{R}[x, y, z]$ with $\deg(P) = 4$, $\mathrm{ord}(P) = 3$ and $P = P^{(3)} + P^{(4)}$, with $P^{(3)} = x^2y + xyz - \sqrt{2}z^3$ and $P^{(4)} = x^2y^2$.
(2) $P(x, y, z) = x^3yz - xy^4$ is homogeneous of degree 4.

Remark 5.3. We can decompose $K[\underline{x}]$ into graded components, where each graded component is a finite-dimensional K-vector space:

$$K[x_1, \ldots, x_n] = \bigoplus_{d=0}^{\infty} K[x_1, \ldots, x_n]_d \ ,$$

where $K[x_1, \ldots, x_n]_d := \{$ homogeneous polynomials of degree $d\}$. Each $K[x_1, \ldots, x_n]_d$ is a finite dimensional K-vector space with basis all monomials of degree d (What is its dimension?). For example, for $n = 2$ we have $K[x, y]_0 = K$, $K[x, y]_1 = Kx \oplus Ky \cong K^2$, $K[x, y]_2 = Kx^2 \oplus Kxy \oplus Ky^2 \cong K^3, \ldots$.

Next we consider ring homomorphisms from $K[\underline{x}]$. In particular important are *evaluation homomorphisms*: Let $a \in K^n$, and define

$$\varepsilon_a : K[x_1, \ldots, x_n] \to K : P \mapsto P(a_1, \ldots, a_n) \ .$$

ε_a is a ring homomorphism and in particular, if $a = (0, \ldots, 0)$, then $\varepsilon_0(P) = P(0)$ yields the constant term of P.
More generally, define *substitution homomorphisms*: let $f \in K[x_1, \ldots, x_n]$ and $g_1, \ldots g_n \in K[y_1, \ldots, y_m]$. Then $f(g_1, \ldots, g_n)$ is an element of $K[y_1, \ldots, y_m]$. This can be described by the homomorphism

$$g^* : K[x_1, \ldots x_n] \to K[y_1, \ldots, y_m] : f \mapsto g^*(f) = f(g_1, \ldots, g_n) \ .$$

The evaluation homomorphism ε_a is a special case, that is, set $g_i = a_i$ in K, then $g^* = \varepsilon_a$.

Monomial orderings of $K[\underline{x}]$

If $n = 1$, then the degree gives a total order on the set of monomials in $K[x]$: $x^\alpha < x^\beta$ if and only if $\alpha < \beta$. However, if $n \geqslant 2$, the degree only yields a partial order on the set of monomials, e.g., for $n = 2$, both monomials x_1x_2 and x_1^2 have the same degree. In order to get a total order on monomials, we introduce the following:

Definition 5.4. A *monomial ordering* $>_\varepsilon$ on $K[x_1, \ldots, x_n]$ (or, equivalently, on $\mathbb{N}^n$) is a total order on the set of monomials $\underline{x}^\alpha$, $\alpha \in \mathbb{N}^n$ of $K[x_1, \ldots, x_n]$ (that is, either $\underline{x}^\alpha >_\varepsilon \underline{x}^\beta$, $\underline{x}^\alpha = \underline{x}^\beta$, or $\underline{x}^\alpha <_\varepsilon \underline{x}^\beta$) such that
(i) If $\alpha >_\varepsilon \beta$ and $\gamma \in \mathbb{N}^n$, then $\alpha + \gamma >_\varepsilon \beta + \gamma$.
(ii) $>_\varepsilon$ is a well-ordering on $\mathbb{N}^n$ (this means that every non-empty subseteq of $\mathbb{N}^n$ has a smallest element with respect to $>_\varepsilon$).

We write $\alpha \geqslant_\varepsilon \beta$ if $\alpha >_\varepsilon \beta$ or $\alpha = \beta$.

Example 5.5. (1) The *lexicographic order* $>_{lex}$ is a monomial order (see homework for a proof!) defined (on $\mathbb{N}^n$) as follows: $\alpha >_{lex} \beta :\Leftrightarrow$ there exists a $j \leqslant n$ such that $\alpha_i = \beta_i$ for all $i < j$ and $\alpha_j > \beta_j$.
(2) The *degree lexicographic order* $>_{deglex}$ is defined as:

$$\alpha >_{deglex} \beta :\Leftrightarrow \begin{cases} |\alpha| > |\beta| \ ; \text{or} \\ |\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta \ . \end{cases}$$

(3) The *reverse lexicographic order* $>_{revlex}$: $\alpha >_{revlex} \beta :\Leftrightarrow$ there exists a $j \geqslant 1$ such that $\alpha_i = \beta_i$ for all $i > j$ and $\alpha_j > \beta_j$.

Example 5.6. More generally, one can define a *linear order* $>_\lambda$: Let $\lambda \in \mathbb{R}^n_+$ be a vector with $\mathbb{Q}$-linearly independent components. Then λ induces a linear map $\lambda : \mathbb{N}^n \to \mathbb{R}_{\geqslant 0}$, $\alpha \mapsto \langle \alpha, \lambda \rangle = \sum_{i=1}^n \alpha_i \lambda_i$. Then $\alpha >_\lambda \beta :\Leftrightarrow \langle \alpha, \lambda \rangle > \langle \beta, \lambda \rangle$.

Example 5.7. For $n = 2$, consider $>_{lex}$: Then $x_1^2 x_2^3 >_{lex} x_1^2 x_2$, because $(2,3)$ is greater than $(2,1)$ in the lexicographic order. Also $x_1^2 >_{lex} x_2^3$.
For $>_{deglex}$ we similarly compute $x_1^2 x_2^3 >_{lex} x_1^2 x_2$ but $x_1^2 <_{deglex} x_2^3$

Definition 5.8. Let $f(\underline{x}) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \underline{x}^\alpha \in K[x_1, \dots, x_n]$ and let $>_\varepsilon$ be a monomial order. Then $\deg_\varepsilon(f) = \max_{>_\varepsilon}(\alpha \in \mathbb{N}^n : a_\alpha \neq 0)$ is called the $>_\varepsilon$*-degree* of f. The *leading coefficient* $lc_\varepsilon(f)$ is $a_{\deg_\varepsilon(f)} \in K$. The *leading monomial* of f is $lm(f) = x^{\deg_\varepsilon(f)}$. The *leading term* of f is $lt_\varepsilon(f) = lc_\varepsilon(f) \cdot lm_\varepsilon(f)$.

Remark 5.9. This is already enough to define an Euclidean division on $K[x_1, \dots, x_n]$ (see later in the chapter on Gröbner bases).

6 Localisation

We can construct $\mathbb{Q}$ from $\mathbb{Z}$ by inverting all non-zero elements. Formally this is done by viewing $\mathbb{Q}$ as a set of equivalence classes in $\mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$ via the relation

$$(r, a) \sim (s, b) \iff as = br.$$

We then write $\frac{r}{a}$ for the equivalence class of (r, a). Addition and multiplication of equivalence classes is defined by

$$\frac{r}{a} + \frac{s}{b} = \frac{as + br}{ab} \text{ and } \frac{r}{a}\frac{s}{b} = \frac{rs}{ab}. \tag{$*$}$$

We also have $0_\mathbb{Q} = \frac{0}{1}$ and $1_\mathbb{Q} = \frac{1}{1}$. It is easy to check that provided $r \neq 0$, $\frac{a}{r}$ is a multiplicative inverse for $\frac{r}{a}$.

We wish to repeat the above for a general ring R. Notice from ($*$) that if we invert a and b then we have also inverted ab. This motivates the following.

Definition 6.1. Let R be a ring and $A \subseteq R$ be a subset. We say A is *multiplicatively closed* if:

(i) $1_R \in A$;

(ii) $a, b \in A \implies ab \in A$.

Example 6.2. (1) For any ring, R itself is multiplicatively closed. If $R = K$, then $K^* = K \backslash \{0\}$ is multiplicatively closed.
(2) If $f \in R = K[x_1, \dots, x_n]$ is a nonzero element, then $A = \{1, f, f^2, f^3, \dots\}$ is a multiplicatively closed set.

Definition 6.3. Let R be a ring and $A \subseteq R$ be multiplicatively closed. The *localisation of R at A*, denoted $A^{-1}R$ or $R[A^{-1}]$ or R_A, is the set of equivalence classes of $R \times A$ under the equivalence relation

$$(r, a) \sim (s, b) \iff \text{there exists a } c \in A \text{ such that } c(as - br) = 0\,.$$

We will again usually write the equivalence class of (r, a) as $\frac{r}{a}$, with addition and multiplication defined as in ($*$).

Lemma 6.4. *Let R be a ring and $A \subseteq R$ a multiplicatively closed subset. Then the localisation A^{-1} of R at A is also a ring via the sum and product (*), and $0_{A^{-1}R} = \frac{0_R}{1_R}$ and $1_{A^{-1}R} = \frac{1_R}{1_R}$. Moreover there is a ring homomorphism*

$$\begin{aligned} i : R &\to A^{-1}R \\ r &\mapsto \frac{r}{1}, \end{aligned}$$

with kernel $\operatorname{Ker} i = \{r \in R : ra = 0 \text{ for some } a \in A\}$.

In some cases, such as the construction of $\mathbb{Q}$ above, we wish to invert as many things as possible.

Definition 6.5. Let R be an integral domain. The *quotient field* or *field of fractions* of R, denoted $\operatorname{Quot}(R)$, is the localisation

$$\operatorname{Quot}(R) = (R \backslash \{0\})^{-1} R.$$

Example 6.6. In each of the following, A is a multiplicatively closed subset of a ring R.

(i) R_A is the zero ring if and only if $0 \in A$.

(ii) Let $a \in A$. We write R_a for the localisation of R at the set $\{a^n : n \geqslant 0\}$.

(iii) Let $\mathfrak{p}$ be a prime ideal of R. Then $A = R \backslash \mathfrak{p}$ is multiplicatively closed and we write $R_{\mathfrak{p}}$ for $A^{-1}R$. (Careful here! The "correct" way to write this would be $R_{R\backslash\mathfrak{p}}$).

(iv) Let $p \in \mathbb{Z}$ be prime. Then

$$\begin{aligned} \mathbb{Z}_p &= \left\{ \frac{a}{b} \in \mathbb{Q} : b \text{ is a power of } p \right\}, \\ \mathbb{Z}_{\langle p \rangle} &= \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}, \\ \operatorname{Quot}(\mathbb{Z}) &= \mathbb{Q}. \end{aligned}$$

Since $A^{-1}R$ is a ring, we can talk about its ideals and how they relate to the ideals of R.

Definition 6.7. Given an ideal I of R, we define the *localisation of the ideal I* to be the set

$$A^{-1}I = \left\{ \frac{x}{a} : x \in I, a \in A \right\}.$$

Proposition 6.8. *Let R be a ring, $A \subseteq R$ a multiplicatively closed subset, and $I \subseteq R$ an ideal.*

(i) $A^{-1}I$ is an ideal of $A^{-1}R$. Moreover, if I is generated by a set X, then $A^{-1}I$ is generated by $\{\frac{x}{1} : x \in X\}$.

(ii) We have $\frac{x}{a} \in A^{-1}I$ if and only if there is some $b \in A$ with $xb \in I$.

(iii) $A^{-1}I = A^{-1}R$ if and only if $I \cap A \neq \emptyset$.

(iv) The map $I \mapsto A^{-1}I$ commutes with forming finite sums, products and intersections, and quotients.

Proof. See Homework Sheet. □

This leads to a correspondence theorem for between ideals of R and ideals of $A^{-1}R$.

Theorem 6.9. *There is a bijection*

$$\{\text{ideals } J \subseteq A^{-1}R\} \leftrightarrow \{\text{ideals } I \subseteq R \text{ such that no element of } A \text{ is a zero divisor in } R/I\},$$

sending $J \mapsto i^{-1}(J)$ and $I \mapsto A^{-1}I$, where i^{-1} is the preimage of the homomorphism from Lemma 6.4.

Moreover, this restricts to a bijection

$$\{\text{prime ideals } Q \subseteq A^{-1}R\} \leftrightarrow \{\text{prime ideals } P \subseteq R \text{ with } P \cap A = \emptyset\}.$$

Proof. Suppose $J \subseteq A^{-1}R$ is an ideal. Then $i^{-1}(J)$ is an ideal, being the preimage of an ideal under a ring homomorphism. By definition we have

$$i^{-1}(J) = \left\{ x \in R : \frac{x}{1} \in J \right\},$$

and therefore $A^{-1}(i^{-1}(J)) \subseteq J$ (see Definition 6.7). Conversely if $\frac{x}{a} \in J$ then $\frac{x}{1} = \frac{a}{1}\frac{x}{a} \in J$, so $x \in i^{-1}(J)$. Thus $\frac{x}{a} \in A^{-1}(i^{-1}(J))$ hence $J \subseteq A^{-1}(i^{-1}(J))$, and therefore $J = A^{-1}(i^{-1}(J))$.

We have shown that the maps are inverses to one another, so we must determine the image of $J \mapsto i^{-1}(J)$. We claim that I is in the image if and only if $I = i^{-1}(A^{-1}I)$. Indeed, such an ideal is certainly in the image of i^{-1}, whereas if $I = i^{-1}(J)$ then $A^{-1}I = A^{-1}(i^{-1}(J)) = J$, and so $i^{-1}(A^{-1}I) = i^{-1}(J) = I$.

Now we always have $I \subseteq i^{-1}(A^{-1}I)$, so $I \neq i^{-1}(A^{-1}I)$ if and only if there is some $x \notin I$ such that $\frac{x}{1} \in A^{-1}I$. By Proposition 6.8(ii), this is equivalent to there being some $x \notin I$ and $b \in A$ with $xb \in I$. That is, there exists $b \in A$ and $x + I \neq I = 0_{R/I}$ in R/I with $(b+I)(x+I) = I = 0_{R/I}$, i.e. some element of A is a zero divisor in R/I.

For the second part, observe first that if $P \subseteq R$ is prime then R/P is an integral domain (Theorem 3.8), so A contains a zero divisor in R/P if and only if $A \cap P \neq \emptyset$. It is therefore enough to show that prime ideals always map to prime ideals. Recall from Proposition 3.3 that if $Q \subseteq A^{-1}R$ is prime, then $i^{-1}(Q) \subseteq R$ is prime. On the other hand if $P \subseteq R$ is prime and $P \cap A = \emptyset$, then R/P is an integral domain and $\overline{A} \subseteq R/P$ does not contain $0_{R/P}$, so by Proposition 6.8(iv) we have

$$A^{-1}R/A^{-1}P \cong \overline{A}^{-1}(R/P) \subseteq \mathrm{Quot}(R/P).$$

Since $\mathrm{Quot}(R/P)$ is a field, it contains no non-zero zero divisors. Therefore as a subring neither does $A^{-1}R/A^{-1}P$, i.e. it is an integral domain, and so $A^{-1}P \subseteq A^{-1}R$ is a prime ideal. □

The following corollary then gives an insight into the name "localisation".

Corollary 6.10. *Let $\mathfrak{p} \subseteq R$ be a prime ideal. Then the prime ideals of $R_\mathfrak{p}$ are in bijection with the prime ideals of R contained in $\mathfrak{p}$. In particular $R_\mathfrak{p}$ has a unique maximal ideal $P_\mathfrak{p}$, and hence $(R_\mathfrak{p}, \mathfrak{p}_\mathfrak{p})$ is a local ring.*

Proof. By Theorem 6.9, the prime ideals of $R_\mathfrak{p}$ are in bijection with the prime ideals $\mathfrak{p}'$ of R that do not intersect $R \backslash \mathfrak{p}$. But this is precisely the condition that $\mathfrak{p}' \subseteq \mathfrak{p}$.

The maximality and uniqueness of $P_\mathfrak{p}$ follows from the fact that the bijection is inclusion preserving. In particular if $Q_1 \subseteq Q_2$ are ideals of $R_\mathfrak{p}$ then $i^{-1}(Q_1) \subseteq i^{-1}(Q_2)$, and if $P_1 \subseteq P_2$ are ideals of R then $(P_1)_\mathfrak{p} \subseteq (P_2)_\mathfrak{p}$. The largest prime ideal of R contained in $\mathfrak{p}$ is $\mathfrak{p}$ itself, and this is the unique ideal with this property, therefore $\mathfrak{p}_\mathfrak{p}$ is the unique maximal ideal of $R_\mathfrak{p}$. □

Theorem 6.11 (Universal property of the localisation)**.** *Let R be a ring and $A \subseteq R$ be a multiplicatively closed set. Let $\varphi : R \to A^{-1}R, r \mapsto \frac{r}{1}$ the ring homomorphism from above (note here: $\varphi(A) \subseteq A^{-1}R$ is inveritble in the localisation $A^{-1}R$). Let $f : R \to B$ be a ring homomorphism such that $g(a)$ is a unit in B for all $a \in A$. Then there exists a unique ring homomorphism $h : A^{-1}R \to B$ such that $f = h \circ \varphi$:*

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[dr, "\varphi"'] & B \\ & A^{-1}R \arrow[u, dashed, "\exists ! h"'] \end{tikzcd}$$

Proof. (1) We show uniqueness first: If h satisfies the conditions of the theorem, then $h(\frac{r}{1}) = h \circ \varphi(r) = f(r)$ for all $r \in R$. For any $a \in A$ we have $h(\frac{1}{a}) = h((\frac{a}{1})^{-1}) = h(\frac{a}{1})^{-1}$ (check this!), and this is equal to $f(a)^{-1}$. Therefore $h(\frac{r}{a}) = h(\frac{r}{1} \cdot \frac{1}{a}) = h(\frac{r}{1})h(\frac{1}{a}) = f(r)f(s)^{-1}$. This means that h is uniquely determined by f.
(2) For the existence we first define $h(\frac{r}{a}) := f(r)f(a)^{-1}$. Then we have to show that h is a well-defined ring homomorphism: for the well-definedness, assume that $\frac{r}{a} = \frac{r'}{a'}$. Then there exists a

$c \in A$ such that $cra' = cr'a$. Thus $f(0) = f(cra' - cr'a) = f(c)\,(f(r)f(a') - f(r')f(a))$ since f is a ring homomorphism. Since $c \in A$, by assumption $f(c)$ is a unit in B, thus $f(r)f(a') = f(r')f(a)$ and this implies that

$$f(r)f(a)^{-1} = f(a')^{-1}f(r')$$

and the left hand side of this equation is equal to $h(\frac{r}{a})$, whereas the right hand side to $h(\frac{r'}{a'})$. Showing that h is a ring homomorphism is an exercise. □

Remark 6.12. This theorem shows that the localisation $A^{-1}R$ is uniquely determined by the following conditions: if $f : R \to B$ is any ring homomorphism such that
(i) $a \in A$ implies that $f(a)$ is a unit in B,
(ii) $f(r) = 0$ implies that $ra = 0$ for some $a \in A$,
(iii) every element of B is of the form $f(r)f(a)^{-1}$,
then there exists a unique ring homomorphism $h : A^{-1} \to B$ such that $f = h \circ \varphi$.

7 The radical, nilradical and Jacobson radical

Recall that an element x in a ring R is called *zero-divisor* if there exists a $y \neq 0$ in R such that $x \cdot y = 0$.

Example 7.1. (1) $0 \in R$ is always a zero-divisor.
(2) $\mathbb{Z}$, $K[x_1, \ldots, x_n]$, and more generally, any integral domain R does not have nonzero zero-divisors.
(3) In $K[x,y]/\langle xy \rangle$ every element contained in the maximal ideal $\langle \overline{x}, \overline{y} \rangle$ is a zero-divisor.

Definition 7.2. Let R be a ring. An element $r \in R$ is *nilpotent* if there exists an integer $n \geqslant 1$ such that $r^n = 0$.

Example 7.3. (1) In an integral domain R are no nonzero nilpotent elements.

(2) In the ring $K[x,y]/\langle xy \rangle$ there are no nonzero nilpotent elements.

(3) The ring $K[x]/\langle x \rangle \cong K$, so does not contain any nonzero nilpotent elements. But in $K[x]/\langle x^k \rangle$ for $k \geqslant 2$, ever x^i, $1 \leqslant i \leqslant k$ is nilpotent.

(4) A noncommutative example: In the ring $M_2(\mathbb{R})$ of 2×2 real matrices,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Definition 7.4. The *nilradical* of a ring R, denoted $\mathrm{nil}(R)$, is the set of all nilpotent elements of R.

Theorem 7.5. *Let R be a ring. Then* $\mathrm{nil}(R)$ *is an ideal of R, and moreover is the intersection of all prime ideals of R.*

Proof. If $r, s \in \mathrm{nil}(R)$ then there exist $n, m \in \mathbb{N}$ such that $r^n = s^m = 0$. By the binomial theorem we have

$$(r+s)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} r^i s^{n+m-i},$$

and for all $0 \leqslant i \leqslant n+m$ we have either $i \geqslant n$ or $n+m-i \geqslant m$, so either $r^i = 0$ or $s^{n+m-i} = 0$. Hence $(r+s)^{n+m} = 0$ and $r+s \in \mathrm{nil}(R)$. Now for $t \in R$, $(tr)^n = t^n r^n = 0$. Finally $0 \in \mathrm{nil}(R)$ so $\mathrm{nil}(R) \neq \emptyset$, and $\mathrm{nil}(R)$ is an ideal of R.

We now show that $\mathrm{nil}(R) \subseteq P$ for all prime ideals P, therefore giving containment one way. Indeed, let P be a prime ideal. Then for any $r \in \mathrm{nil}(R)$ there exists some $n \in \mathbb{N}$ such that $r^n = 0 \in P$, but since P is prime we must then have $r \in P$.

Finally, we show that the intersection of all prime ideals is contained in the nilradical. In fact, we will prove the contrapositive. Suppose r is not nilpotent. Then $0 \notin \{r^i : i \geqslant 1\}$ and the set

$$S = \{I \subseteq R : I \text{ is an ideal and } r^i \notin I \text{ for all } i \geqslant 1\}$$

is non-empty as $\{0\} \in S$. We turn S into a poset by inclusion, and then any totally ordered subset of S has an upper bound, namely the union of all its elements (cf. proof of Proposition 4.6). By Zorn's Lemma, there is a maximal element $J \in S$. That J is an ideal is immediate, so we now prove that it is prime. Suppose $ab \in J$ but $a \notin J$ and $b \notin J$. Then $\langle a \rangle + J$ and $\langle b \rangle + J$ are strictly greater than J, so $r^m \in \langle a \rangle + J$ and $r^n \in \langle b \rangle + J$ for some $m, n \in \mathbb{N}$. Thus $r^{n+m} \in (\langle a \rangle + J)(\langle b \rangle + J) \subseteq J$, contradicting the choice of J. Therefore J is a prime ideal and moreover $r \notin J$ (set $i = 1$ in the above), so $r \notin \bigcap_{P \text{ prime}} P$. □

Recall the notion of radical ideal: Let I be an ideal of a ring R. The *radical* of I, denoted $\sqrt{I}$, is the set $\{r \in R : r^n \in I \text{ for some } n \geqslant 1\}$. We have already shown (in the exercises) that $\sqrt{I}$ is an ideal in R.

Theorem 7.6. *Let I be an ideal of a ring R. Then $\sqrt{I}$ is an ideal of R, and moreover is the intersection of all prime ideals in R which contain I.*

Proof. Consider the quotient homomorphism $\varphi : R \to R/I$. Then $r \in \sqrt{I}$ if and only if $\varphi(r) \in \operatorname{nil}(R/I)$, thus $rad(I) = \varphi^{-1}(\operatorname{nil}(R/I))$ and hence is an ideal.

For the second statement we see that

$$\begin{aligned} \sqrt{I} &= \varphi^{-1}(\operatorname{nil}(R/I)) \\ &= \varphi^{-1}\left(\bigcap_{\overline{P} \subseteq R/I \text{ prime}} \overline{P} \right) \\ &= \bigcap_{\overline{P} \subseteq R/I \text{ prime}} \varphi^{-1}(\overline{P}) \\ &= \bigcap_{\substack{P \subseteq R \text{ prime} \\ I \subseteq P}} P, \end{aligned}$$

where we have again used Proposition 2.10 in the last step. □

Example 7.7. (i) Working in $\mathbb{Z}$, we have $\sqrt{4\mathbb{Z}} = 2\mathbb{Z}$ and $\sqrt{3\mathbb{Z}} = 3\mathbb{Z}$.

(ii) Again in $\mathbb{Z}$,

$$\sqrt{12\mathbb{Z}} = \bigcap_{\substack{P prime \\ 12\mathbb{Z} \subseteq P}} P.$$

The prime ideals in $\mathbb{Z}$ are $p\mathbb{Z}$, and those containing $12\mathbb{Z}$ are $2\mathbb{Z}$ and $3\mathbb{Z}$. Hence $\sqrt{12\mathbb{Z}} = 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$.

(iii) Let $I = \langle x + y, y^2 \rangle \subseteq \mathbb{R}[x, y]$. Then $y \in \sqrt{I}$, and $x^2 = y^2 + (x - y)(x + y) \in I$ so also $x \in \sqrt{I}$. Then $\sqrt{I} = \langle x, y \rangle$.

Definition 7.8. Let R be a ring. The *Jacobson radical*, denoted $J(R)$, is defined to be the set

$$J(R) = \bigcap_{\mathfrak{m} \subseteq R \text{ maximal}} \mathfrak{m}.$$

Remark. Note that in a local ring $(R, \mathfrak{m})$ (see Definition 4.8), the Jacobson radical is equal to the maximal ideal, i.e. $J(R) = \mathfrak{m}$.

Lemma 7.9. *Let R be a ring and $x \in R$. Then $x \in J(R)$ if and only if $1 + rx$ is invertible for all $r \in R$.*

Proof. See Exercise Sheet 1. $\square$

Example 7.10. Let $R = K[[x]]$. Then R is local with maximal ideal $\mathfrak{m} = \langle x \rangle$. Then by definition we have $J(R) = \mathfrak{m}$ but $\mathrm{nil}(R) = \langle 0 \rangle$, as R is a domain.

8 Modules

Definition 8.1. Let R be a ring. An abelian group $M = (M, +)$ (with identity 0) is an *R-module* (or just a module if it is clear from context) if there exists a multiplication map $\cdot : R \times M \to M$, $(r, m) \mapsto rm$ such that for all $r, s \in R$ and $m, n \in M$:

(i) $r(sm) = (rs)m$;

(ii) $r(m + n) = rm + rn$;

(iii) $(r + s)m = rm + sm$;

(iv) $1_R m = m$.

Example 8.2. (1) If R is a field then an R-module is simply a vector space. The axioms for a module are the same as a vector space except R is not necessarily a field.

(2) Ideals in a ring R are also R-modules. In general, an ideal is not isomorphic to R as an R-module. Take for example $I = \langle x^3 - yz, y^2 - xz, z^2 - x^2y \rangle \subseteq K[x, y, z]$. Then the three generators are not linearly independent over $K[x, y, z]$. One has the relations $y(x^3 - yz) + z(y^2 - xz) + x(z^2 - x^2y) = z(x^3 - yz) + x^2(y^2 - xz) + y(z^2 - x^2y) = 0$. But the three given polynomials are a minimal generating set for I. We see that a module does not need to have a basis (different as for vector spaces).

(3) For a ring R, the set R^n of n-tuples of elements of R is an R-module.

(4) $R[x]$ is an R-module: it is generated by $R \oplus Rx \oplus Rx^2 \oplus \cdots$.

(5) R is a module over itself.

(6) Any abelian group is a $\mathbb{Z}$-module (and vice versa!).

(7) If $S \subseteq R$ is a subring then R is an S-module.

Modules therefore generalise the idea of vector spaces to rings.

Definition 8.3. A map $\varphi : M \to N$ between R-modules M and N is an *R-module homomorphism* (or R-homomorphism) if φ is an R-linear map, i.e. $\varphi(rm + sn) = r\varphi(m) + s\varphi(n)$ for all $r, s \in R$ and $m, n \in M$. An *R-module isomorphism (monomorphism, epimorphism)* is a (injective, surjective) bijective R-homomorphism. The set of all R-homomorphisms from M to N is denoted $\mathrm{Hom}_R(M, N)$.

Proposition 8.4. *The set $\mathrm{Hom}_R(M, N)$ is an R-module, via the action $(r\varphi)(m) = r\varphi(m)$ for all $r \in R$, $\varphi \in \mathrm{Hom}_R(M, N)$ and $m \in M$.*

Proof. Exercise. $\square$

Example 8.5. If $\varphi : R \to S$ is a ring homomorphism, then it is also a morphism of R-modules. For this define the R-module structure on S via $r \cdot s := \varphi(r)s$. Then it is easy to see that φ is R-linear.

If R is a field, then R-module homomorphisms are simple linear maps between vector spaces.

Definition 8.6. A *submodule* U of an R-module M is a subgroup $(U, +)$ of $(M, +)$, closed under the restricted action of the multiplication, i.e. $ru \in U$ for all $r \in R$ and $u \in U$.

Note that the inclusion map $U \hookrightarrow M$ is an R-module homomorphism.

Example 8.7. (i) Let $I \subseteq R$ be an ideal and M an R-module. Then

$$IM = \left\{ \sum_{i=1}^{n} a_i m_i : n \geqslant 1,\ a_i \in I,\ m_i \in M \right\}$$

is a submodule of M.

(ii) If $U, V \subseteq M$ are submodules, then $U \cap V$ is a submodule of U, V and M.

The factor group M/U is also an R-module, via the action $r(m+U) = (rm) + U$. The quotient map $\varphi : M \to M/U$ is an R-homomorphism, and this allows us to talk about I/J for ideals I and J of a ring R.

Example 8.8. (1) The quotient group $\mathbb{Z}/6\mathbb{Z}$ is a $\mathbb{Z}$-module. Note that $2(3+6\mathbb{Z}) = 6+6\mathbb{Z} = 0$ in $\mathbb{Z}/6\mathbb{Z}$, hence multiplication of non-zero elements of a module by non-zero scalars may result in zero. This is in contrast to the situation in vector spaces.
(2) Let K be a field. Then K is a $K[x]$-module, via $\pi : K[x] \to K[x]/\langle x \rangle$, which sends $P(x)$ to $P(0)$. Then the multiplication $P(x) \cdot \alpha$ for $P(x) \in K[x]$ and $\alpha \in K$ is simply given by $P(0)\alpha \in K$.

For a general R-homomorphism $\varphi : M \to N$, we can define $\operatorname{Ker} \varphi$ and $\operatorname{Im} \varphi$ in the usual way, and these are submodules of M and N respectively.

Definition 8.9. The *cokernel* of an R-homomorphism $\varphi : M \to N$ is the set

$$\operatorname{Coker} \varphi = N/\operatorname{Im} \varphi.$$

Let U, V be submodules of an R-module M. Then the set

$$U + V = \{u + v : u \in U,\ v \in V\}$$

is also a submodule of M. This is used in the following theorem.

Theorem 8.10 (Isomorphism theorems)**.** *Let R be a ring and M, N be R-modules. We have the following:*

(i) if $\varphi : M \to N$ is an R-module homomorphism then

$$M/\operatorname{Ker} \varphi \cong \operatorname{Im} \varphi;$$

(ii) if $L \subseteq M \subseteq N$ are submodules then

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

via the map $(m+L) + M/L \mapsto m + M$;

(iii) if N is a module and L, M are submodules then

$$M/(M \cap L) \cong (M+L)/L,$$

via the map $m + M \cap L \mapsto m + L$.

These isomorphisms are canonical (i.e. require no choices in their definition).

Proof. Exercise Sheet. □

Definition 8.11. Let R be a ring and M an R-module. Let Γ be a subset of M. The *submodule of M generated by* Γ, denoted $\langle \Gamma \rangle$ or $\sum_{g \in \Gamma} Rg$, is the set

$$\langle \Gamma \rangle = \left\{ \sum_{i=1}^{n} r_i g_i : n \geqslant 1,\ r_i \in R,\ g_i \in \Gamma \right\}.$$

The module M is *finitely generated* if there exists a finite set $\Gamma \subseteq M$ such that $\langle \Gamma \rangle = M$.

Example 8.12. (1) Let R be a ring and $I \subseteq R$ an ideal, then the R-module R/I is finitely generated. In fact it is *cyclic*, i.e. generated by one element, namely $1 + I$.

(2) If R is an integral domain and $0 \neq f \in R$, then

$$R[\tfrac{1}{f}] = R + R\tfrac{1}{f} + R\tfrac{1}{f^2} + \dots$$

is usually not finitely generated as an R-module.

(3) Let $\Gamma = \{x, x^2, x^3, \dots,\} \subseteq K[x]$. Then $\langle \Gamma \rangle = \langle x \rangle$.

9 Nakayama's Lemma

Nakayama's lemma (also known as NAK, where the letters stand for Nakayama–Azumaya–Krull) is an important tool in algebraic geometry. In particular it gives a precise definition of what it means for a module to be minimally generated (over a local ring).

Definition 9.1. A *minimal generating set* for an R-module M is a subset $\Gamma \subseteq M$ such that Γ generates M but no proper subset of Γ generates M.

Example 9.2. Consider $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$, then $\{1 + 6\mathbb{Z}\}$ and $\{2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}\}$ are both minimal generating sets. Contrast this with vector spaces, where the number of elements in any two minimal generating sets of a given vector space are equal.

Theorem 9.3 (Nakayama's Lemma – NAK)**.** *Let M be a finitely generated R-module, and $I \subseteq J(R)$ an ideal of R. If $M = IM$, then $M = 0$.*

Proof. Suppose $M \neq 0$. Since M is finitely generated there exists a finite minimal generating set $\Gamma = \{g_1, \dots, g_n\}$ say. Now $M = IM \implies g_1 \in IM$, so there exists $a_1, \dots, a_n \in I$ such that

$$g_1 = \sum_{i=1}^{n} a_i g_i$$

and so

$$(1 - a_1) g_1 = \sum_{i=2}^{n} a_i g_i.$$

But $a_1 \in I \subseteq J(R)$, so by Lemma 7.9, $1 - a_1$ is a unit of R. Thus

$$g_1 = (1 - a_1)^{-1} \sum_{i=2}^{n} a_i g_i$$

and $\{g_2, \dots, g_n\}$ is a generating set for M strictly smaller than Γ, a contradiction. □

Corollary 9.4. *Let M be a finitely generated R-module and $N \subseteq M$ a submodule. Let also $I \subseteq J(R)$ be an ideal of R. Then $M = N + IM \implies M = N$.*

Proof. Take the equality $M = N + IM$ and quotient both sides by the submodule N to obtain $M/N = (N + IM)/N$. By Theorem 8.10, we have $(N + IM)/N \cong IM/(N \cap IM)$. Now the map

$$IM \to I(M/N)$$
$$\sum_{i=1}^{n} a_i m_i \mapsto \sum_{i=1}^{n} a_i (m_i + N)$$

is a surjective R-module homomorphism, and its kernel is $(IM) \cap N$. Therefore

$$I(M/N) \cong IM/(IM \cap N) \cong (N + IM)/N.$$

Therefore we have $M/N = I(M/N)$. Since M is finitely generated so too is M/N, and hence by Nakayama's Lemma we have $M/N = 0$, i.e. $M = N$. □

Example 9.5. Consider $K[x,y]$ for some field K and let $\mathfrak{m} = \langle x, y\rangle$. Let $R = K[x,y]_{\mathfrak{m}}$, the localisation at the ideal $\mathfrak{m}$. Then R is a local ring, with maximal ideal $\mathfrak{m}_{\mathfrak{m}}$. We will show that the ideal

$$I = \langle x + x^2y + 3y^2 + x^4, y + 2y^3 + y^4 + 4x^7\rangle_{\mathfrak{m}} \subseteq R$$

is equal to $\mathfrak{m}_{\mathfrak{m}}$. Note first that since R is local it has a unique maximal ideal, hence $J(R) = \mathfrak{m}_{\mathfrak{m}}$. Now

$$\begin{aligned} I + \mathfrak{m}_{\mathfrak{m}}\mathfrak{m}_{\mathfrak{m}} &= \langle x + x^2y + 3y^2 + x^4, y + 2y^3 + y^4 + 4x^7, x^2, xy, y^2\rangle_{\mathfrak{m}} \\ &= \langle x, y, x^2, xy, y^2\rangle_{\mathfrak{m}} \\ &= \langle x, y\rangle_{\mathfrak{m}} \\ &= \mathfrak{m}_{\mathfrak{m}}. \end{aligned}$$

So by Nakayama's Lemma, $I = \mathfrak{m}_{\mathfrak{m}}$.

Recall from earlier that we had an issue with minimal generating sets for modules, in that the number of elements in such a set is not well defined. Nakayama's Lemma allows us to fix this in certain cases.

Theorem 9.6. *Let $(R, \mathfrak{m})$ be a local ring and M a finitely generated R-module. If $\Gamma \subseteq M$ is a set of elements whose images in $M/\mathfrak{m}M$ form a basis of $M/\mathfrak{m}M$ as an $R/\mathfrak{m}$-vector space, then Γ is a minimal generating set of M as an R-module.*

Proof. As $M/\mathfrak{m}M$ is generated by the images of the elements of Γ, we have $M = \langle\Gamma\rangle + \mathfrak{m}M$. So by Corollary 9.4 to Nakayama's Lemma, we have $M = \langle\Gamma\rangle$. If $\Gamma' \subsetneq \Gamma$, then $\langle\Gamma'\rangle + \mathfrak{m}M \neq \langle\Gamma\rangle + \mathfrak{m}M = M$, and so Γ' is not a generating set. □

10 Exact sequences

Definition 10.1. A sequence of R-modules and R-module homomorphisms

$$\cdots \longrightarrow M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \longrightarrow \cdots \xrightarrow{f_n} M_n \longrightarrow \cdots$$

is called *exact at M_i* if $\operatorname{Ker} f_{i+1} = \operatorname{Im} f_i$. A sequence which is exact at M_i for all i is called an *exact sequence*.

Example 10.2. (i) The sequence $0 \longrightarrow L \xrightarrow{f} M$ is exact if and only if f is injective.

(ii) The sequence $M \xrightarrow{g} N \longrightarrow 0$ is exact if and only if g is surjective.

(iii) The sequence $0 \longrightarrow M \xrightarrow{g} N \longrightarrow 0$ is exact if and only if g is an isomorphism.

Definition 10.3. A *short exact sequence* is an exact sequence of the form

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0.$$

Remark. This is equivalent to insisting that f is injective, g is surjective and $\operatorname{Ker} g = \operatorname{Im} f$.

Short exact sequences appear in many different sub-branches of algebra, and are very powerful objects.

Example 10.4. (i) Let R be a ring, M an R-module and $N \subseteq M$ a submodule. Then

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0,$$

where i is the natural inclusion map and π is the canonical quotient map, is a short exact sequence.

(ii) Any long exact sequence can be split into short exact sequences. Let

$$\cdots \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$$

be an exact sequence, that is $\mathrm{Im}\,(f_i) = \mathrm{Ker}\,(f_{i+1})$ for all i. Then

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

is a short exact sequence.

(iii) Let K be a field and

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

be a short exact sequence of K-modules. Then each module is a K-vector space, and using facts from linear algebra we have

$$\begin{aligned}\dim_K M &= \dim_K \mathrm{Ker}\, g + \dim_K \mathrm{Im}\, g \\ &= \dim_K \mathrm{Im}\, f + \dim_K N \\ &= \dim_K L + \dim_K N.\end{aligned}$$

More generally, if

$$0 \longrightarrow M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \longrightarrow \cdots \xrightarrow{f_n} M_n \longrightarrow 0$$

is an exact sequence of K-vector spaces, then $\sum_{i=0}^{n}(-1)^i \dim_K M_i = 0$.

Remark 10.5. One can also consider (exact) sequences of other objects, sequences $\cdots \to A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \cdots$ of abelian groups, where the f_i are group homomorphisms.

Definition 10.6. Let A, B, C, D be R-modules and let $\alpha, \beta, \gamma, \delta$ be R-module homomorphisms. Then the *diagram*

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\gamma"'] & B \arrow[d, "\beta"] \\ C \arrow[r, "\delta"] & D \end{tikzcd}$$

is *commutative* (or: the diagram commutes) if $\beta \circ \alpha = \delta \circ \gamma$.

The following lemma is a typical example for statements in homological algebra. We will prove it with *diagram chasing.*

Theorem 10.7 (Snake Lemma)**.** *Suppose the following commutative diagram of R-modules and R-module homomorphisms*

$$\begin{tikzcd} & L \arrow[r, "f"] \arrow[d, "\alpha"] & M \arrow[r, "g"] \arrow[d, "\beta"] & N \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & L' \arrow[r, "f'"] & M' \arrow[r, "g'"] & N' & \end{tikzcd}$$

has exact rows. Then there exists a homomorphism $\delta : \mathrm{Ker}\,\gamma \to \mathrm{Coker}\,\alpha$ *such that*

$$\mathrm{Ker}\,\alpha \longrightarrow \mathrm{Ker}\,\beta \longrightarrow \mathrm{Ker}\,\gamma \xrightarrow{\delta} \mathrm{Coker}\,\alpha \longrightarrow \mathrm{Coker}\,\beta \longrightarrow \mathrm{Coker}\,\gamma$$

is exact.

Furthermore, if f is injective then so too is $\mathrm{Ker}\,\alpha \to \mathrm{Ker}\,\beta$*, and if g' is surjective then so too is* $\mathrm{Coker}\,\beta \to \mathrm{Coker}\,\gamma$*.*

The name of this theorem comes from the following diagram:

$$\begin{tikzcd}
 & \operatorname{Ker}\alpha \arrow[d] & \operatorname{Ker}\beta \arrow[d] & \operatorname{Ker}\gamma \arrow[d] \arrow[dddll, "\delta", red] & \\
 & L \arrow[r, "f"] \arrow[d, "\alpha"] & M \arrow[r, "g"] \arrow[d, "\beta"] & N \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & L' \arrow[r, "f'"] \arrow[d] & M' \arrow[r, "g'"] \arrow[d] & N' \arrow[d] & \\
 & \operatorname{Coker}\alpha & \operatorname{Coker}\beta & \operatorname{Coker}\gamma &
\end{tikzcd}$$

Proof. We will first define all of the necessary maps, then prove exactness at each site.

The map $f|_{\operatorname{Ker}\alpha} : \operatorname{Ker}\alpha \to \operatorname{Ker}\beta$ is given by the restriction of f to $\operatorname{Ker}\alpha$. Note that if $\ell \in \operatorname{Ker}\alpha$ then $\beta(f(\ell)) = f'(\alpha(\ell)) = 0$ by the commutativity of the diagram. Therefore $f(\operatorname{Ker}\alpha) \subseteq \operatorname{Ker}\beta$. That this is a R-homomorphism follows from the fact that f itself is. Similarly the map $g|_{\operatorname{Ker}\beta} :$ $\operatorname{Ker}\beta \to \operatorname{Ker}\gamma$ is given by the restriction of g to $\operatorname{Ker}\beta$.

The map $\overline{f} : \operatorname{Coker}\alpha \to \operatorname{Coker}\beta$ is induced from f', by setting $\overline{f}(\ell' + \operatorname{Im}\alpha) = f'(\ell') + \operatorname{Im}\beta$. This is well defined, as if $\ell_1' + \operatorname{Im}\alpha = \ell_2' + \operatorname{Im}\alpha$ then $\ell_1' - \ell_2' \in \operatorname{Im}\alpha$, so $\ell_1' - \ell_2' = \alpha(\ell)$ for some $\ell \in L$. Then

$$\begin{aligned}
f'(\ell_1') - f'(\ell_2') &= f'(\ell_1' - \ell_2') \\
&= f'(\alpha(\ell)) \\
&= \beta(f(\ell)) \\
&\in \operatorname{Im}\beta,
\end{aligned}$$

so $f'(\ell_1') + \operatorname{Im}\beta = f'(\ell_2') + \operatorname{Im}\beta$. That $\overline{f}$ is a homomorphism follows from the fact that f' is. We similarly define $\overline{g} : \operatorname{Coker}\beta \to \operatorname{Coker}\gamma$.

We now construct the connecting homomorphism $\delta : \operatorname{Ker}\gamma \to \operatorname{Coker}\alpha$ by a process known as "diagram chasing". Take $n \in \operatorname{Ker}\gamma \subseteq N$. Since g is surjective, there exists some $m \in M$ such that $n = g(m)$. Then

$$\begin{aligned}
0 &= \gamma(n) \\
&= \gamma(g(m)) \\
&= g'(\beta(m))
\end{aligned}$$

by the commutativity of the diagram, so $\beta(m) \in \operatorname{Ker} g'$. By the exactness of rows, $\operatorname{Ker} g' = \operatorname{Im} f'$, so $\beta(m) = f'(\ell')$ for some $\ell' \in L'$. We then define

$$\delta(n) = \ell' + \operatorname{Im}\alpha \in \operatorname{Coker}\alpha.$$

We must show that this is well defined. Since f' is injective, the only ambiguity in our process lies in our choice of m. Suppose then that $g(m_1) = g(m_2) = n$, and $\ell_1', \ell_2' \in L'$ are the unique elements such that $\beta(m_1) = f'(\ell_1')$ and $\beta(m_2) = f'(\ell_2')$. We must show that $\ell_1' - \ell_2' \in \operatorname{Im}\alpha$. Note then that $m_1 - m_2 \in \operatorname{Ker} g$, and so by exactness of rows is equal to $f(\ell)$ for some $\ell \in L$. Therefore $\beta(m_1 - m_2) = \beta(f(\ell)) = f'(\alpha(\ell))$. By the injectivity of f', we then see that $\alpha(\ell) = \ell_1' - \ell_2'$. That δ is a homomorphism is left as an easy exercise.

We now prove exactness at each site.

The composition $g|_{\operatorname{Ker}\beta} \circ f|_{\operatorname{Ker}\alpha} = 0$ follows from the fact that $\operatorname{Im} f = \operatorname{Ker} g$, therefore $\operatorname{Im} f|_{\operatorname{Ker}\alpha} \subseteq \operatorname{Ker} g|_{\operatorname{Ker}\beta}$. Suppose now that $m \in \operatorname{Ker}\beta$ with $g|_{\operatorname{Ker}\beta}(m) = 0$. Then $g(m) = 0$ so $m \in \operatorname{Ker} g = \operatorname{Im} f$, say $m = f(\ell)$, and it remains to show that $\ell \in \operatorname{Ker}\alpha$. But

$$\begin{aligned} f'(\alpha(\ell)) &= \beta(f(\ell)) \\ &= \beta(m) \\ &= 0 \end{aligned}$$

as $m \in \operatorname{Ker}\beta$, and since f' is injective we must have $\alpha(\ell) = 0$.

For exactness at $\operatorname{Ker}\gamma$, we first calculate $\delta(g|_{\operatorname{Ker}\beta}(m))$ for $m \in \operatorname{Ker}\beta$. Following our construction of δ above, we have $g_{\operatorname{Ker}\beta}(m) = g(m)$, and so ℓ' is chosen so that $\beta(m) = f'(\ell')$. But $\beta(m) = 0$, so by the injectivity of f' we also have $\delta(g|_{\operatorname{Ker}\beta}(m)) = 0$ and hence $\operatorname{Im} g|_{\operatorname{Ker}\beta} \subseteq \operatorname{Ker}\delta$. Conversely if $n \in \operatorname{Ker}\gamma$ is such that $\delta(n) = 0$, then the corresponding ℓ' is in $\operatorname{Im}\alpha$, say $\ell' = \alpha(\ell)$. Therefore if m is such that $n = g(m)$, we have $\beta(m) = f'(\alpha(\ell')) = \beta(f(\ell))$, and hence $m - f(\ell) \in \operatorname{Ker}\beta$. Then $g|_{\operatorname{Ker}\beta}(m - f(\ell)) = g(m) - g(f(\ell)) = n$.

For exactness at $\operatorname{Coker}\alpha$, note that $\overline{f}(\delta(n)) = f'(\ell') + \operatorname{Im}\beta = \beta(m) + \operatorname{Im}\beta = 0$ in $\operatorname{Coker}\beta$. Therefore $\operatorname{Im}\delta \subseteq \operatorname{Ker}\overline{f}$. Conversely if $l' + \operatorname{Im}\alpha \in \operatorname{Coker}\alpha$ is such that $\overline{f}(l' + \operatorname{Im}\alpha) = 0$, then $f'(\ell') \in \operatorname{Im}\beta$, say $f'(\ell') = \beta(m)$. But then $\delta(g(m)) = \ell' + \operatorname{Im}\alpha$.

Finally, for exactness at $\operatorname{Coker}\beta$ we see first that $\overline{g}(\overline{f}(\ell' + \operatorname{Im}\alpha)) = \overline{g}(f'(\ell') + \operatorname{Im}\beta) = g'(f'(\ell')) + \operatorname{Im}\gamma = 0$ since $g' \circ f' = 0$. Therefore $\operatorname{Im}\overline{f} \subseteq \operatorname{Ker}\overline{g}$. Conversely, if $m' + \operatorname{Im}\beta \in \operatorname{Coker}\beta$ is such that $\overline{g}(m' + \operatorname{Im}\beta) = 0$, then $g'(m') \in \operatorname{Im}\gamma$, say $g'(m') = \gamma(n)$. Since g is surjective, there is some $m \in M$ such that $g(m) = n$, so $g'(m') = \gamma(g(m))$. Commutativity of the diagram then gives $g'(m') = g'(\beta(m))$, so $m' - \beta(m) \in \operatorname{Ker} g' = \operatorname{Im} f'$, say $m' - \beta(m) = f'(\ell')$. But now $\overline{f}(\ell' + \operatorname{Im}\alpha) = f'(\ell') + \operatorname{Im}\beta = m' - \beta(m) + \operatorname{Im}\beta = m' + \operatorname{Im}\beta$.

We leave the last statement as an exercise. $\square$

Example 10.8. We reprove part (ii) of Theorem 8.10. Let $L \subseteq M \subseteq N$ be a sequence of submodules and consider the following diagram:

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "\alpha"] & N \arrow[r, "g"] \arrow[d, "\beta"] & N/M \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & M/L \arrow[r, "f'"] & N/L \arrow[r, "g'"] & (N/L)/(M/L) \arrow[r] & 0 \end{tikzcd}$$

The maps f, g and f', g' are pairs of inclusion and quotient maps, so the rows are short exact sequences. We have $\alpha : M \to M/L$ and $\beta : N \to N/L$ also quotient homomorphisms, and for all $m \in M$

$$\begin{aligned} \beta(f(m)) &= \beta(m) \\ &= m + L \\ &= f'(m + L) \text{ since } m \in M \\ &= f'(\alpha(m)), \end{aligned}$$

so the first square commutes. Now define $\gamma : N/M \to (N/L)/(M/L)$ by $\gamma(n + M) = (n + L) + M/L$. This is well defined since if $n + M = n' + M$ then $n - n' \in M$ so

$$\begin{aligned} \gamma(n) - \gamma(n') &= ((n + L) + M/L) - ((n' + L) + M/L) \\ &= (n - n' + L) + M/L \\ &= M/L = 0_{(N/L)/(M/L)} \text{ since } n - n' \in M. \end{aligned}$$

It is also a homomorphism (easy check since it is the composition of two quotient maps). Finally we check that the diagram commutes: for all $n \in N$ we have

$$\begin{aligned}\gamma(g(n)) &= \gamma(n+M) \\ &= (n+L)+M/L, \text{ and} \\ g'(\beta(n)) &= g'(n+L) \\ &= (n+L)+M/L.\end{aligned}$$

By the Snake Lemma, we therefore have an exact sequence

$$0 \to \operatorname{Ker}\alpha \to \operatorname{Ker}\beta \to \operatorname{Ker}\gamma \to \operatorname{Coker}\alpha \to \operatorname{Coker}\beta \to \operatorname{Coker}\gamma \to 0.$$

Clearly $\operatorname{Ker}\alpha = \operatorname{Ker}\beta = L$ and $\operatorname{Coker}\alpha = \operatorname{Coker}\beta = 0$. Therefore our exact sequence is equal to

$$0 \to L \to L \to \operatorname{Ker}\gamma \to 0 \to 0 \to \operatorname{Coker}\gamma \to 0.$$

By exactness we immediately see that $\operatorname{Ker}\gamma = \operatorname{Coker}\gamma = 0$. Thus γ is both injective and surjective, so is an isomorphism between N/M and $(N/L)/(M/L)$.

11 Free modules

Let R be a ring, Λ a set and M_λ an R-module for each $\lambda \in \Lambda$.

Definition 11.1. The *direct product* of $\{M_\lambda\}_{\lambda\in\Lambda}$, denoted $\prod\limits_{\lambda\in\Lambda} M_\lambda$, consists of all sequences $(m_\lambda)_{\lambda\in\Lambda}$ with $m_\lambda \in M_\lambda$ for each $\lambda \in \Lambda$. This is a module, with addition

$$(m_\lambda)_{\lambda\in\Lambda} + (n_\lambda)_{\lambda\in\Lambda} = (m_\lambda + n_\lambda)_{\lambda\in\Lambda}$$

and for any $r \in R$,

$$r(m_\lambda)_{\lambda\in\Lambda} = (rm_\lambda)_{\lambda\in\Lambda}.$$

The *direct sum* of $\{M_\lambda\}_{\lambda\in\Lambda}$, denoted $\bigoplus\limits_{\lambda\in\Lambda} M_\lambda$, consists of all sequences $(m_\lambda)_{\lambda\in\Lambda}$ with $m_\lambda \in M_\lambda$ for each $\lambda \in \Lambda$, and all but finitely many of the m_λ are zero. This is again a module, with addition and scalar multiplication as before.

Note that if Λ is finite then $\prod_{\lambda\in\Lambda} M_\lambda = \bigoplus_{\lambda\in\Lambda} M_\lambda$. For instance, $\mathbb{R} \oplus \mathbb{R} \cong \mathbb{R}^2$.

Remark 11.2. The direct sum/product can be defined categorically and are given by universal properties.

Proposition 11.3. *If U, V are submodules of M, then $M = U \oplus V \iff M = U + V$ and $U \cap V = \{0\}$.*

Proof. Exercise. $\square$

Remark. Care needs to be taken when dealing with direct products. For instance, for rings R and S their direct product $R \times S$ has identity $(1,1)$. Then the natural map $\varphi : R \to R \times S$ given by $\varphi(r) = (r, 0)$ is not a ring homomorphism, since $\varphi(1) = (1,0) \neq (1,1)$.

Definition 11.4. An R-module is called *free* if it is isomorphic to $\bigoplus_{\lambda\in\Lambda} R$ for some set Λ. We adopt the convention the the zero module is free, with index set $\Lambda = \emptyset$.

Example 11.5. (i) $R^n = R \oplus R \oplus \cdots \oplus R$ is clearly free.

(ii) The ring of $m \times n$ matrices over a ring R is free and isomorphic to R^{mn}.

(iii) The polynomial ring $R[X]$ is free, as $R[X] \cong R \oplus RX \oplus RX^2 \oplus \ldots$.

Recall that in contrast to vector spaces, not every module has a basis. However free modules do.

Proposition 11.6. *An R-module is free if and only if there exists a set of generators $\{m_\lambda\}_{\lambda\in\Lambda}$ of M such that whenever $r_1 m_{\lambda_1} + \dots r_n m_{\lambda_n} = 0$ with $r_i \in R$ and $\lambda_i \in \Lambda$ for all i, we have $r_1 = \dots = r_n = 0$.*

Proof. The "only if" direction is clear.

Conversely, assume we have a set of generators as above and define a map

$$\begin{aligned} \varphi : \bigoplus_{\lambda\in\Lambda} R &\to M \\ (r_\lambda)_{\lambda\in\Lambda} &\mapsto \sum_{\lambda\in\Lambda} r_\lambda m_\lambda. \end{aligned}$$

It is then straightforward to check that this is an isomorphism of R-modules. □

Definition 11.7. A set of generators as in Proposition 11.6 is called a *free basis*, or just a basis. The *rank* of a free module is the cardinality of Λ, equivalently the number of basis elements.

Example 11.8. (i) $1, X, X^2, \dots$ is a basis of $R[X]$.

(ii) The rank of R^n is n.

(iii) A K-vector space has a basis and so is a free K-module.

(iv) Consider the maximal ideal $\mathfrak{m} = \langle x, y\rangle$ of $R = K[x,y]$. This is generated by two elements but is not free, for instance as $-yx + xy = 0$ is a non-trivial dependence relation. However, the module of relations of $\mathfrak{m}$ is freely generated by one element, $(-y, x)$. Thus we get an exact sequence of R-modules

$$0 \longrightarrow R \longrightarrow R^2 \longrightarrow \mathfrak{m} \longrightarrow 0 \ .$$

This exact sequence can be completed to the Koszul complex of K:

$$0 \longrightarrow R \longrightarrow R^2 \longrightarrow R \longrightarrow K \longrightarrow 0 \ .$$

This is what is called a *free resolution* of the R-module K. In order to understand the structure of non-free modules M, one can study resolutions of M by free modules.

(v) $\mathbb{Z}_2$ is not free as a $\mathbb{Z}$-module, since it is generated by $1 + 2\mathbb{Z}$ but $2(1 + 2\mathbb{Z}) = 2 + 2\mathbb{Z} = 0_{\mathbb{Z}_2}$, so this is a non-trivial dependence relation.

Proposition 11.9. *Let R be a ring and M an R-module. Then there exists a free module F and a surjective homomorphism of R modules $\varphi : F \to M$. Furthermore if M is finitely generated then F can be chosen to have finite rank.*

Proof. Any R-module can be written as $\langle\Gamma\rangle$ for some $\Gamma \subseteq M$, for instance by setting $\Gamma = M$. Then let F be the free module with basis Γ. Now define

$$\begin{aligned} \varphi : F &\to M \\ (r_g)_{g\in\Gamma} &\mapsto \sum_{g\in\Gamma} r_g g. \end{aligned}$$

Note that this sum is finite since F is a direct sum of copies of R. It is an easy exercise to see that this is a surjective R-module homomorphism.

If M is finitely generated, say by $\{m_g\}_{g\in\Gamma}$ then we similarly define F to be the free module with finite basis Γ, and $\varphi : F \to M$ by $\varphi((r_g)_{g\in\Gamma}) = \sum_{g\in\Gamma} r_g m_g$. It is again easy to check that this is a surjective homomorphism. □

Example 11.10. Let $M_1, \dots, M_n$ be R-modules. Then the sequence

$$0 \longrightarrow M_1 \longrightarrow M_1 \oplus \cdots \oplus M_n \longrightarrow M_2 \oplus M_3 \oplus \cdots \oplus M_n \longrightarrow 0$$

is exact.

Proposition 11.11. *Let L, M, N be R-modules and let*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

be a short exact sequence. Then the following are equivalent:

(i) There exists an isomorphism $M \cong L \oplus N$ under which α is given by $l \mapsto (l, 0)$ and β as $(l, n) \mapsto n$.

(ii) There exists a section of β, that is, a map $s : N \to M$ such that $\beta s = \mathrm{Id}_N$.

(iii) There exists a retraction for α, that is, a map $r : M \to L$ such that $r\alpha = \mathrm{Id}_L$.

Definition 11.12. If any of the three equivalent condition of the above proposition is satisfied, then the short exact sequence

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

is called a *split exact sequence.*

Proof. Exercise. □

Example 11.13. (1) For finite dimensional K-vector spaces, every short exact sequence is split.

(2) The short exact sequence

$$0 \to \langle x \rangle \xrightarrow{incl} K[x] \xrightarrow{\pi} K \to 0$$

is nonsplit as a sequence of $K[x]$-modules. (See this by trying to construct a section $K \to K[x]$!)

12 Noetherian rings and modules

Being finitely generated is obviously a good property for a module to have. But if M is a finitely generated R-module then there is no guarantee that its submodules will be.

Example 12.1. Let $R = K[x_1, x_2, x_3, \dots]$. Then R is an R-module and is finitely generated by $\{1\}$. However the submodule $\langle x_1, x_2, x_3 \dots \rangle$ is not.

This motivates the following:

Definition 12.2. A module M is called a *Noetherian*[1] *module* if every submodule of M is finitely generated. A ring R is called a *Noetherian ring* if it is a Noetherian module over itself (i.e. all ideals are finitely generated).

Examples are hard to give without a bit of extra theory, so we present this first.

Theorem 12.3. *Let M be an R-module. Then the following are equivalent:*

(i) all submodules of M are finitely generated;

(ii) M satisfies the ascending chain condition (ACC), i.e. every chain of submodules

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

of M is stationary, that is there exists some N with $M_n = M_N$ for all $n \geqslant N$;

[1] Named after Emmy Noether (1882–1935),

(iii) every non-empty set of submodules of M has a maximal element.

Proof. $(i) \implies (ii)$: The union $\bigcup_i M_i$ is a submodule of M, so is finitely generated by assumption. Each of these generators must lie in some M_j, and taking N to be the maximum of these j we have $\bigcup_i M_i = M_N$. Hence $M_n = M_N$ for all $n \geqslant N$.

$(ii) \implies (iii)$: Let S be a non-empty set of submodules of M and suppose S has no maximal element. Since S is non-empty we can take some $M_1 \in S$. Since M_1 is not maximal we can find some $M_2 \in S$ with $M_1 \subsetneq M_2$. Repeating this argument we can construct inductively a non-stationary ascending chain of submodules of M, contradicting (ii).

$(iii) \implies (i)$: Let U be a submodule of M and S the set of finitely generated submodules of U. This is non-empty as it contains the zero module, so has a maximal element $U' = \langle u_1, \ldots, u_n \rangle$. Now take any $v \in U$, then $U' + \langle v \rangle = \langle u_1, \ldots, u_n, v \rangle$ is a finitely generated submodule of U, so by maximality must equal U'. Hence $U = U'$ is finitely generated. $\square$

We can now give some examples of Noetherian rings and modules.

Example 12.4. (i) Let R be a field, then the only ideals of R are R and $\{0\}$ which are finitely generated. Therefore R is a Noetherian ring.

(ii) Modules and rings with a finite number of elements are Noetherian.

(iii) Any principal ideal domain is a Noetherian ring. Therefore $\mathbb{Z}$, $\mathbb{Z}[i]$ and $K[x]$ (K a field) are Noetherian rings (as they are Euclidean domains).

(iv) Finite dimensional K-vector spaces are Noetherian K-modules, since any subspace (submodule) has a finite basis.

Theorem 12.5. *Let* $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ *be an exact sequence of R-modules. Then M is Noetherian if and only if both L and N are Noetherian.*

Proof. Note that the property of being Noetherian is preserved by isomorphisms, thus it is sufficient to prove the theorem in the case $L \subseteq M$ and $N = M/L$. [One can prove this using the snake lemma. Look at the diagram of short exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "\alpha"] \arrow[d, "="] & M \arrow[r, "\beta"] \arrow[d, "="] & N \arrow[r] \arrow[d, dashed, "\gamma"] & 0 \\
0 \arrow[r] & \alpha(L) \arrow[r, hook, "i"] & M \arrow[r, "\pi"] & M/\alpha(L) \arrow[r] & 0
\end{tikzcd},$$

where $\gamma : N \to M/\alpha(L)$ is defined via: since β is surjective, for any $n \in N$ there exists an $m \in M$ such that $\beta(m) = n$. Then set $\gamma(n) = m + \alpha(L)$. This is well-defined, since for any $m' \in M$ with $\beta(m') = n$, one has that $m - m' \in \operatorname{Ker}(\beta)$, which is equal to $\operatorname{Im}(\alpha)$, since the top sequence is exact. But this means that $m - m' \in \alpha(L)$ and thus the cosets $m + \alpha(L) = m' + \alpha(L)$ in $M/\alpha(L)$. For the bottom row note that $\alpha(L) \cong L$, since α is injective. The bottom row is exact by construction. It is easy to see that the diagram commutes, and then an application of the snake lemma yields the result.]

Suppose first that M is Noetherian and let L' be a submodule of L. Then L' is a submodule of M so is finitely generated, and hence L is Noetherian. Next, any submodule N' of M/L is of the form M'/L for some submodule M' of M. Therefore M' is finitely generated, and reduction of these generators modulo L shows that N' is also finitely generated.

Conversely suppose that both L and N are Noetherian and consider a submodule $M' \subseteq M$. Then the submodules $M' \cap L \subseteq L$ and $M'/L \subseteq N$ are both finitely generated, say by $x_1, \ldots, x_n$ and $y_1 + L, \ldots, y_m + L$ respectively. Now for any $m \in M'$ we have $m + L = (b_1 y_1 + \cdots + b_m y_m) + L$ for some $b_i \in R$, thus $m - (b_1 y_1 + \cdots + b_m y_m) \in L$. But also $m, y_1, \ldots, y_m \in M'$, so $m - (b_1 y_1 + \cdots + b_m y_m) = a_1 x_1 + \cdots + a_n x_n$ for some $a_i \in R$. Hence $m = a_1 x_1 + \cdots + a_n x_n + b_1 y_1 + \cdots + b_m y_m$, and so M' is finitely generated. Therefore M is Noetherian. $\square$

Proposition 12.6. *Let R be a Noetherian ring and M an R-module. Then M is Noetherian if and only if M is finitely generated.*

Proof. The "only if" direction is by definition.

Suppose M is finitely generated, then there is a surjection $\varphi : R^n \to M$ for some $n \geqslant 0$. The sequence $0 \longrightarrow \operatorname{Ker}\varphi \longrightarrow R^n \longrightarrow M \longrightarrow 0$ is then exact, and since R^n is Noetherian then so too is M by Theorem 12.5. □

Proposition 12.7. *Let R be a Noetherian ring.*

(i) Let $I \subseteq R$ be an ideal. Then R/I is a Noetherian ring.

(ii) Let $A \subseteq R$ be a multiplicatively closed subset. Then $A^{-1}R$ is a Noetherian ring.

Proof. (i) Let J be an ideal or R/I. Its preimage under the canonical quotient map is finitely generated, therefore so too is J.

(ii) Similarly for an ideal J of $A^{-1}R$, its preimage under the natural map $R \to A^{-1}R$ is finitely generated. Therefore so too is J.

□

Remark 12.8. One can also define Noetherian spaces: Let X be a topological space. Then X is called *noetherian* if every descending chain of closed subsets becomes stationary. In particular $X = \mathbb{A}^n_K$ is a noetherian space, where one takes the closed subsets to be $V(I)$, where $I \subseteq K[x_1, \ldots, x_n]$ is an ideal. This topology is called *Zariski topology*. Since for ideal $I \subseteq J$ in $K[x_1, \ldots, x_n]$, one has $V(J) \subseteq V(I)$ (see part about algebraic geometry), one can show that a descending chain of closed subsets in X corresponds to an ascending chain of ideals in $K[x_1, \ldots, x_n]$.

Remark 12.9. If an R-module M satisfies the *descending chain condition*, that is, every descending chain of submodules $M_1 \supseteq M_2 \supseteq \cdots$ becomes stationary, then M is called *Artinian module*. A ring R is called *Artinian* if it is Artinian as a module over itself. This condition is much rarer than noetherian: if R is Artinian, then it is also Noetherian. An example of an Artinian ring is $R = K[x]/\langle x^n \rangle$ for $n \geqslant 1$.
But on the other hand, take for example the polynomial ring $K[x]$: here $\langle x \rangle \supsetneq \langle x^2 \rangle \supsetneq \langle x^3 \rangle \supsetneq \cdots$ is a strictly decreasing chain of ideals that never becomes stationary.

13 Hilbert's Basis Theorem

This theorem was proved by David Hilbert in 1890. It is fundamental for algebraic geometry and also important for practical computations, in particular, Gröbner basis calculations.

Theorem 13.1. *If R is Noetherian, then the polynomial ring $R[x]$ is Noetherian.*

Remark 13.2. In the lecture I did a different proof, following Atiyah–Macdonald [1, p.81f]. The idea of both proofs is the same: take an ideal I in $R[x]$ and look at the ideal generated by all the leading coefficients of polynomials in I. The leading coefficients are in R, so this ideal $lc(I)$ has to be finitely generated. Then look at the corresponding ideal $I' \subseteq R[x]$ generated by all the polynomials, whose leading coefficient generate $lc(I)$. Show with a "division algorithm" that any element in I belongs to a finitely generated module (namely I' and the "remainders").

Proof. Suppose there exists an ideal $I \subseteq R[x]$ which is not finitely generated. Choose a sequence $f_1, f_2, f_3, \ldots$ of polynomials in $R[x]$ such that

$$\begin{aligned} &f_1 \in I, \\ &f_2 \in I \backslash \langle f_1 \rangle, \\ &f_3 \in I \backslash \langle f_1, f_2 \rangle, \ldots \end{aligned}$$

of minimal possible degree. If $d_i = \deg(f_i)$, say $f_i = a_i x^{d_i} +$ lower terms, then $d_1 \leqslant d_2 \leqslant d_3 \leqslant \dots$ and

$$\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \langle a_1, a_2, a_3 \rangle \subseteq \dots$$

is an ascending chain of ideals in R. Since R is Noetherian this chain is stationary, i.e. there is some N such that $\langle a_1, \dots, a_N \rangle = \langle a_1, \dots, a_{N+1} \rangle$. Hence $a_{N+1} = \sum_{i=1}^{N} b_i a_i$ for some suitable $b_i \in R$. Now consider

$$\begin{aligned} g &= f_{N+1} - \sum_{i=1}^{N} b_i x^{d_{N+1} - d_i} f_i \\ &= a_{N+1} x^{d_{N+1}} - \left(\sum_{i=1}^{N} b_i a_i \right) x^{d_{N+1}} + \textit{lower terms}. \end{aligned}$$

Since $f_{N+1} \in I \backslash \langle f_1, \dots, f_N \rangle$, it follows that $g \in I \backslash \langle f_1, \dots, f_N \rangle$ is a polynomial of degree smaller than d_{N+1}, a contradiction to the choice of f_{N+1}. □

Corollary 13.3. *If R is Noetherian, then $R[x_1, \dots, x_n]$ is Noetherian. In particular, if K is a field then $K[x_1, \dots, x_n]$ is Noetherian.*

Proof. Exercise (easy induction). □

Corollary 13.4. *If R is Noetherian and $\varphi : R \to B$ is a ring homomorphism, such that B is a finitely generated extension ring of* $\operatorname{Im}(\varphi)$ *(i.e., $B \cong R[x_1, \dots, x_n]/I$), then B is noetherian.*

Proof. See p.55 of [2]. □

Example 13.5. Similarly one can show that $K[[x]]$, the power series ring over K, is Noetherian.

14 Primary decomposition

This is sometimes also called *Lasker–Noether decomposition* and an analogue of decomposition of an integer into prime factors for more general rings. It also has a geometric content: we will see that the (isolated) components of a minimal primary decomposition of an ideal $I \subseteq K[x_1, \dots, x_n]$ correspond to the irreducible components of the algebraic set $V(I) \subseteq \mathbb{A}^n_K$.

Motivation: Consider $R = \mathbb{Z}$. Then every $z \in \mathbb{Z}$ may be written as $z = p_1^{k_1} \cdots p_n^{k_n}$. One can express this in ideal notation:

$$\langle z \rangle = \langle p_1^{k_1} \rangle \cap \cdots \langle p_n^{k_n} \rangle .$$

Here one sees that the ideals on the right hand side are just powers of prime ideals. It is not so clear how to generalize this to Noetherian rings.

Example 14.1. Let $I = \langle x^3, x^2y, x^2z, xy^2, xz^2, xyz, y^3, y^2z, yz^2, z^3 \rangle \subseteq K[x, y, z]$. Then I may be written as intersection of ideals

$$I = \langle x, y \rangle \cap \langle x, z \rangle \cap \langle y, z \rangle \cap \langle x, y^2, z^2 \rangle \cap \langle x^2, y, z^2 \rangle \cap \langle x^2, y^2, z \rangle .$$

Not all of the ideals on the right hand side are powers of primes! For example, set $\mathfrak{m} = \langle x, y, z \rangle$. Then $\mathfrak{m} \supsetneq \langle x, y^2, z^2 \rangle \supsetneq \mathfrak{m}^3$. Taking the radicals of all three ideals and noting that if $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$, it follows that $\sqrt{\langle x, y^2, z^2 \rangle} = \mathfrak{m}$. Since $\langle x, y^2, z^2 \rangle$ is not equal to $\mathfrak{m}^2$, it cannot be a power of a prime ideal.

To get a bit more flexibility one makes the following

Definition 14.2. A proper ideal $\mathfrak{q} \subseteq R$ is called *primary* if $xy \in \mathfrak{q} \implies$ either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n \geqslant 1$. Equivalently, $\mathfrak{q}$ is primary if and only if $R/\mathfrak{q} \neq 0$ and every zero-divisor in $R/\mathfrak{q}$ is nilpotent.

Remark 14.3. A prime ideal is a generalisation of a prime number. In turn, a primary ideal is a generalisation of the power of a prime number. This will allow us to talk about "unique factorisation" of ideals in much the same way we do for integers or polynomials say.

Example 14.4. (i) If I is prime, then I is primary.

(ii) The ideal $I = \langle x, y^2, z^2 \rangle$ is primary in $R = K[x,y,z]$. To see this, look at the quotient $R/I \neq\cong K[y,z]/\langle y^2, z^2\rangle \neq 0$. If $\overline{f} \neq \overline{0}$ in R/I is a zero-divisor, then it is easy to see that $\overline{f} \in \langle \overline{y}, \overline{z} \rangle$ and that $\overline{f}^3 = \overline{0}$ in R/I.

(iii) On the other hand, if $\mathfrak{p}$ is prime, then $\mathfrak{p}^n$ is not necessarily primary: let $R = K[x,y,z]/\langle xy - z^2 \rangle$. Then $I = \langle \overline{x}, \overline{z} \rangle$ is prime (since $R/I \cong K[y]$ is an integral domain). Calculate $I^2 = \langle \overline{x}^2, \overline{xz}, \overline{z}^2 \rangle$. Here $\overline{z}^2 = \overline{xy} \in I^2$. But neither $\overline{x}$, nor $\overline{y}$ are contained in $I = \sqrt{I}$ (direct calculation), so no power of them is in I. But this means that I^2 violates the condition of being a primary ideal.

(iv) $\{0\}$ and $\langle p^n \rangle$ for p a prime, $n \geqslant 1$ are the primary ideals in $\mathbb{Z}$. These are the only ideals with prime radical, and it is then clear that they are primary.

Proposition 14.5. *(1) Let $I \subseteq R$ be a primary ideal, then $\sqrt{I}$ is a prime ideal.*
(2) If $\sqrt{I} = \mathfrak{m}$ is maximal, then I is primary.

Proof. Exercise. □

Proof. Exercise. □

Definition 14.6. Let R be a ring and let $\mathfrak{p} \subseteq R$ be a prime ideal. We say that an ideal $I \subseteq R$ is $\mathfrak{p}$-*primary* if I is primary and $\sqrt{I} = \mathfrak{p}$. If I is primary, then $\mathfrak{p}$ is called the *associated prime ideal*.

Theorem 14.7. *Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ be $\mathfrak{p}$-primary ideals in R. Then $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ is $\mathfrak{p}$-primary.*

Proof. As $\sqrt{\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_n} = \mathfrak{p}$, we need only check that $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ is primary. Assume $x, y \in R$ are such that $xy \in \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$. If $x \notin \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ then $x \notin \mathfrak{q}_j$ for some $1 \leqslant j \leqslant n$. Now $xy \in \mathfrak{q}_j$ and since $\mathfrak{q}_j$ is primary we have $y^m \in \mathfrak{q}_j$ for some $m \geqslant 1$, i.e. $y \in \sqrt{\mathfrak{q}_j} = P = \sqrt{\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n}$, and the result follows. □

Definition 14.8. A *primary decomposition* of an ideal I in a ring R is an expression of I as a finite intersection of primary ideals

$$I = \bigcap_{i=1}^{n} \mathfrak{q}_i.$$

The decomposition is *minimal* (sometimes: *irredundant* or *reduced*) if:

(i) $\sqrt{\mathfrak{q}_i}$ are distinct for all i;

(ii) $\displaystyle\bigcap_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$ for all $1 \leqslant i \leqslant n$.

Remark 14.9. One can always obtain a minimal primary decomposition from a given one: if $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$ is an intersection of primary ideals, then if $\mathfrak{q}_{i_1}, \ldots, \mathfrak{q}_{i_k}$ have the same associated prime $\mathfrak{p}_i$, we collect them together as $\mathfrak{q}_i' := \mathfrak{q}_{i_1} \cap \ldots \cap \mathfrak{q}_{i_k}$ (which is $\mathfrak{p}_i$-primary by Thm. 14.7). If $\bigcap_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \mathfrak{q}_j \subseteq \mathfrak{q}_i$, then omit $\mathfrak{q}_i$.

Theorem 14.10 (Lasker–Noether)**.** *Let R be a Noetherian ring, $I \subseteq R$ an ideal. Then I has a minimal primary decomposition*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n\ .$$

Moreover, for any two minimal primary decompositions

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_m$$

we have $n = m$ and (possibly after reordering) $\sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}'_i}$ for all $1 \leqslant i \leqslant n$. The set $\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$ is equal to the set of prime ideals of R of the form $\sqrt{(I : \langle x \rangle)}$ for some $x \in R$.
In particular, if $I = \sqrt{I} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ then the primary decomposition is unique and all $\mathfrak{q}_i$ are prime.

Example 14.11. (i) Let I be the ideal from example 14.1: $I = \langle x, y\rangle \cap \langle x, z\rangle \cap \langle y, z\rangle \cap \langle x, y^2, z^2\rangle \cap \langle x^2, y, z^2\rangle \cap \langle x^2, y^2, z\rangle$. Then we have seen this is a primary decomposition of I. However, this decomposistion is not minimal, since $\sqrt{\langle x, y^2, z^2\rangle} = \sqrt{\langle x^2, y, z^2\rangle} = \sqrt{\langle x^2, y^2, z\rangle} = \langle x, y, z\rangle$. Use the remark above and set

$$\mathfrak{q}' = \langle x, y^2, z^2\rangle \cap \langle x^2, y, z^2\rangle \cap \langle x^2, y^2, z\rangle = \langle x^2, y^2, z^2, xyz\rangle \, .$$

It is now easy to see that replacing the three ideals with $\mathfrak{q}'$ yields a minimal primary decomposition of I.

(ii) Suppose $I = \langle f\rangle \subseteq K[x_1, \ldots, x_n]$, and $f = f_1^{n_1} \ldots f_r^{n_r}$ is the factorisation into irreducibles over K. Then $I = \langle f_1^{n_1}\rangle \cap \cdots \cap \langle f_r^{n_r}\rangle$ is a minimal primary decomposition, with associated primes $\{\langle f_1\rangle, \ldots, \langle f_r\rangle\}$.

Now we come to the proof of the primary decomposition theorem: it mainly consists of two parts - existence and uniqueness. For the existence one introduces the notion of irreducible ideals, and first shows that any ideal in a Noetherian ring can be written as an intersection of irreducible ideals, and finally that any irreducible ideal is primary.

Definition 14.12. We call an ideal $I \subseteq R$ *irreducible* if it cannot be written as $I_1 \cap I_2$, where I_1 and I_2 are proper ideals of R which strictly contain I.

Example 14.13. (i) $\langle x^2 + 1\rangle \subseteq \mathbb{R}[x]$ is irreducible.

(ii) $\langle (y - x^2)(y^2 - x^3)\rangle = \langle y - x^2\rangle \cap \langle y^2 - x^3\rangle \subseteq R[x, y]$ is reducible.

Proposition 14.14. *Every proper ideal of a Noetherian ring R is the intersection of finitely many irreducible ideals.*

Proof. Let S be the set of all ideals which are not the intersection of finitely many irreducible ideals. If $S \neq \emptyset$ then by Theorem 12.3(iii) it has a maximal element, J say. Now J is not irreducible, so $J = J_1 \cap J_2$ for some ideals $J_1, J_2 \supsetneq J$. By the maximality of J, it must be possible to write J_1 and J_2 as the intersection of finitely many irreducible ideals, and therefore we can also write J as such. This is a contradiction, so $S = \emptyset$ and the result follows. □

For the next proposition we need to recall the quotient ideal

$$(I : J) = \{r \in R : rJ \subseteq I\}$$

for ideals $I, J \subseteq R$ from Proposition 2.5. It is an easy exercise to show that $(I : J_1 + J_2) = (I : J_1) \cap (I : J_2)$ and $(I_1 \cap I_2 : J) = (I_1 : J) \cap (I_2 : J)$, which allows us to prove:

Proposition 14.15. *Irreducible ideals in Noetherian rings are primary.*

Proof. Let R be Noetherian. We first show that if the zero ideal is irreducible then it is primary. Let $xy = 0$ with $y \neq 0$ and consider the chain

$$(0 : \langle x\rangle) \subseteq (0 : \langle x\rangle) \subseteq (0 : \langle x\rangle) \subseteq \ldots .$$

By ACC this is stationary, i.e. $(0 : \langle x^n\rangle) = (0 : \langle x^{n+1}\rangle) = \ldots$ for some $n \geqslant 1$. It follows that $\langle x^n\rangle \cap \langle y\rangle = \{0\}$, for if $a \in \langle y\rangle$ then $ax = 0$ so if also $a \in \langle x^n\rangle$ then $a = bx^n$ and $ax = bx^{n+1} = 0$.

Hence $b \in (0 : \langle x^{n+1} \rangle) = (0 : \langle x^n \rangle)$, so $bx^n = a = 0$. Since $\{0\}$ is irreducible and $\langle y \rangle \neq 0$ we must therefore have $x^n = 0$, i.e. $\{0\}$ is primary.

Now let $I \subseteq R$ be irreducible. Then R/I is Noetherian by Theorem 12.5 and the zero ideal $\{0 + I\} \subseteq R/I$ is irreducible by Proposition 2.10. Therefore $\{0 + I\}$ is primary, so for any $x, y \in R$ we have $xy \in I$ implies that $(x + I)(y + I) \in \{0 + I\}$, thus either $x + I = 0 + I$ or $y^n + I = 0 + I$ for some n. But this is equivalent to having either $x \in I$ or $y^n \in I$, hence I is primary. □

Corollary 14.16. *Every proper ideal of a Noetherian ring can be written as an intersection of finitely many primary ideals.*

Proof. Exercise, use Propositions 14.14 and 14.15. □

For the proof of uniqueness in the Lasker–Noether theorem and also for practical computations, one needs the following

Lemma 14.17. *Let $\mathfrak{q}$ be a primary ideal in R. Then for any $x \in R$*

$$\sqrt{(\mathfrak{q} : \langle x \rangle)} = \begin{cases} R & \text{if } x \in \mathfrak{q}, \\ \sqrt{\mathfrak{q}} & \text{if } x \notin \mathfrak{q}. \end{cases}$$

Proof. Exercise. □

Proof of Thm. 14.10. Corollary 14.16 tells us that primary decompositions always exist, and now Theorem 14.7 allows us to reduce this to a minimal decomposition.

Suppose first that $\sqrt{(I : \langle x \rangle)}$ is prime for some $x \in R$. Then we have

$$\begin{aligned} \sqrt{(I : \langle x \rangle)} &= \sqrt{(\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n : \langle x \rangle)} \\ &= \sqrt{(\mathfrak{q}_1 : \langle x \rangle)} \cap \cdots \cap \sqrt{(\mathfrak{q}_n : \langle x \rangle)}. \end{aligned}$$

Recall from Theorem 3.9 that $I_1 \cap \cdots \cap I_n \subseteq P \iff I_j \subseteq P$ for some j, where I_i are ideals and P is prime. It is an easy exercise to show that in the "only if" direction, the subsets can be replaced by equalities, and hence $\sqrt{(I : \langle x \rangle)} = \sqrt{(\mathfrak{q}_j : \langle x \rangle)}$ for some j. Since $\sqrt{(I : \langle x \rangle)} \neq R$ we must have $\sqrt{(I : \langle x \rangle)} = \sqrt{(\mathfrak{q}_j : \langle x \rangle)} = \sqrt{\mathfrak{q}_j}$ by Lemma 14.17. Therefore the set of prime ideals of the form $\sqrt{(I : \langle x \rangle)}$ is a subset of $\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$.

Now consider $\sqrt{\mathfrak{q}_i}$. By minimality of the primary decomposition we can choose $x \in \mathfrak{q}_j$ for all $j \neq i$ but $x \notin \mathfrak{q}_i$. But then we have

$$\begin{aligned} \sqrt{(I : \langle x \rangle)} &= \sqrt{(\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n : \langle x \rangle)} \\ &= \sqrt{(\mathfrak{q}_1 : \langle x \rangle)} \cap \cdots \cap \sqrt{(\mathfrak{q}_n : \langle x \rangle)} \\ &= \sqrt{\mathfrak{q}_i}. \end{aligned}$$

Thus $\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$ is a subset of the set of prime ideals of the form $\sqrt{(I : \langle x \rangle)}$, and the equality is established. The final statement follows immediately, since the set of primes of the form $\sqrt{(I : \langle x \rangle)}$ is independent of any choice of primary decomposition. □

Definition 14.18. For any ideal I of a Noetherian ring R, the *associated primes* of I is the set

$$\operatorname{Ass}(I) = \{\sqrt{\mathfrak{q}_i} : 1 \leqslant i \leqslant n,\ I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \text{ is a minimal primary decomposition}\}.$$

A minimal element in $\operatorname{Ass}(I)$ (w.r.t. inclusion) is called an *isolated* or *minimal* prime ideal. A non-isolated prime ideal is called *embedded*. The $\mathfrak{q}_i$ are called the *(isolated or embedded) primary components of I*.

If $\sqrt{I} = I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, then the primary components are the $\sqrt{\mathfrak{q}_i} = \mathfrak{q}_i = \mathfrak{p}_i$ and all $\mathfrak{p}_i$ are isolated.

Example 14.19. An ideal I is primary if and only if $\mathrm{Ass}(I)$ consists of one element.
An ideal I is prime if and only if $\mathrm{Ass}(I) = I$.

Proposition 14.20. *For any ideal I of a Noetherian ring R, the set*

$$\{x + I : x \in P \text{ for some } P \in \mathrm{Ass}(I)\}$$

is precisely the set of zero divisors of R/I.

Proof. Exercise. □

Example 14.21. (i) $R = \mathbb{Z}$, $I = \langle 12 \rangle = \langle 3 \rangle \cap \langle 4 \rangle$. Then $\mathfrak{q}_1 = \langle 4 \rangle$, $\mathfrak{q}_2 = \langle 3 \rangle$ which have radicals $\langle 2 \rangle$ and $\langle 3 \rangle$ respectively. Therefore $\mathrm{Ass}(\langle 12 \rangle) = \{\langle 2 \rangle, \langle 3 \rangle\}$.

(ii) Consider $I = \langle x, y^2 \rangle \cap \langle y \rangle \subseteq K[x, y]$. Then $\mathfrak{q}_1 = \langle x, y^2 \rangle$, $\mathfrak{q}_2 = \langle y \rangle$ have radicals $\langle x, y \rangle$ and $\langle y \rangle$ respectively, so $\mathrm{Ass}(I) = \{\langle x, y \rangle, \langle y \rangle\}$. Here $\langle y \rangle$ is an embedded component and $\langle x, y \rangle$ is an isolated component.
But I also has the minimal primary decomposition $I = \langle y \rangle \cap \langle x^2, xy, y^2 \rangle$ which have the same radicals as q_1 and q_2.

15 Noether normalisation and Hilbert's Nullstellensatz

Both of these classical theorems have a geometric background. We will only sketch this in the case of Noether normalisation, the geometric meaning of the Nullstellensatz is part of the next chapter.
For the Noether normalisation let $X = V(I) \subseteq \mathbb{A}^n_K$ be an algebraic set, where $I \subseteq K[x_1, \ldots, x_n]$ is an ideal. The normalisation theorem says that there exists a (linear) surjective and finite morphism $\pi : X \to \mathbb{A}^d_K$ onto the linear space $\mathbb{A}^d_K$. *Finite* is an algebraic condition and means that $K[x_1, \ldots, x_n]/I$ is a finitely generated $K[x_1, \ldots, x_d]$-module under the map $\pi^* : K[x_1, \ldots, x_d] \to K[x_1, \ldots, x_n]/I$, $f \mapsto \pi^*(f) = f \circ \pi$. In particular, if π is finite, then it has *finite fibers*, that is, for any $b \in \mathbb{A}^d_K$ the set $\pi^{-1}(b)$ consists of a finite number of points.

Example 15.1. (i) Let $X = V(y - x^2) \subseteq \mathbb{A}^2_{\mathbb{R}}$. We can project X onto each of the two coordinate axes: $\pi_x : X \to \mathbb{A}^1_{\mathbb{R}} : (x, y) \mapsto x$ and $\pi_y : X \to \mathbb{A}^1_{\mathbb{R}} : (x, y) \mapsto y$. The first projection π_x is even bijective, for π_y the fibers $\pi_y^{-1}(b)$, $b \in \mathbb{A}^1_{\mathbb{R}}$, consist of either 1 or 2 points.
Algebraically for π_x^* we have $\pi_x^* : \mathbb{R}[x] \to \mathbb{R}[x, y]/\langle y - x^2 \rangle \cong \mathbb{R}[x, x^2]$. Clearly, $\mathbb{R}[x, x^2] = \mathbb{R}[x]$ is finitely generated as an $\mathbb{R}[x]$-module here!

(ii) Consider the cross $V(xy) \subseteq \mathbb{A}^2_{\mathbb{R}}$ and take again the projections π_x and π_y onto the two coordinate axes. Here neither of the two projections is finite, since $\pi_x^{-1}(0)$ is the whole y-axis, and $\pi_y^{-1}(0)$ is the x-axis. Algebraically, one sees for example that for $\pi_x^* : \mathbb{R}[x] \to \mathbb{R}[x, y]/\langle xy \rangle$ the module $\mathbb{R}[x, y]/\langle xy \rangle$ is not finitely generated over $\mathbb{R}[x]$: it is the infinite direct sum $\mathbb{R}[x] \oplus y\mathbb{R}[x] \oplus y^2\mathbb{R}[x] \oplus \cdots$.

In the second example above, the (proof of the) Noether normalisation theorem will tell us how to modify X to obtain a finite projection onto a linear space. For this first recall the following

Definition 15.2. Let R be a ring. An *R-algebra* is a ring S with an R-homomorphism $\varphi : R \to S$. We say S is a *finite* R-algebra if it is finitely generated as an R-module, i.e. there exist $x_1, \ldots, x_n \in S$ such that

$$S = Rx_1 + \cdots + Rx_n.$$

If also R is a field then we say S is a *finite dimensional* R-algebra.
We say S is a *finitely generated* R-algebra if there exist $x_1, \ldots, x_n \in S$ such that $S = R[x_1, \ldots, x_n]$.

Example 15.3. (i) $R[x]$ is an R-algebra via the natural inclusion map. It is not finite, but it is finitely generated.

(ii) $\mathbb{Q}[\sqrt{2}]$ is finitely generated over $\mathbb{Q}$ and also finite, since $\mathbb{Q}[\sqrt{2}] = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2}$ as $\mathbb{Q}$-vector space.

(iii) $K[t]$ is a finitely generated $R = K[t^2, t^3]$-algebra: $K[t] = R[t]$ as algebras and $K[t] = R + Rt$ as R-module.

(iv) Any finitely generated K-algebra is of the form $K[x_1, \dots, x_n]/I$, where I is an ideal in $K[x_1, \dots, x_n]$: Let $S = K[a_1, \dots, a_n]$ be a finitely generated K-algebra, with $a_i \in S$. We have an algebra homomorphism (this is a ring homomorphism that is also a K-module homomorphism) $\varphi : K[x_1, \dots, x_n] \to S$, $x_i \mapsto a_i$. Then by construction φ is surjective, and by the homomorphism theorem $S \cong K[x_1, \dots, x_n]/\operatorname{Ker}(\varphi)$.

The homomorphism φ turns S into an R-module, where multiplication is defined by $r \cdot s = \varphi(r)s$ for all $r \in R, s \in S$.

When $R \subseteq S$, we call S an *extension ring* of R. If in addition R and S are fields, then we call S an *extension field* of R.

Definition 15.4. Let S be an R-algebra. An element $s \in S$ is *integral over R* if there exists a monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 \in R[x]$$

such that $f(s) = 0$.

We say S is integral over R if every $s \in S$ is integral over R. If also $R \subseteq S$, then we call S an *integral extension*.

Example 15.5. (i) The integral elements of $\mathbb{Q}$ over $\mathbb{Z}$ are the integers.

(ii) $K[x^2] \subseteq K[x]$ is an integral extension.

Proposition 15.6. *(i) Let $R \subseteq S \subseteq T$ be rings. If S is a finite R-algebra and T is a finite S-algebra, then T is a finite R-algebra.*

(ii) If $R \subseteq S$ is a finite R-algebra and $t \in S$, then t satisfies a monic polynomial over R.

(iii) If S is an R-algebra and $t \in S$ is integral over R, then $R[t]$ is a finite R-algebra.

Proof. (i) Exercise.

(ii) Suppose $S = \sum_{i=1}^n Rs_i$. Then for each i, $ts_i \in S$ so there exist $r_{ij} \in R$ such that

$$ts_i = \sum_{j=1}^n r_{ij}s_j \implies \sum_{j=1}^n (t\delta_{ij} - r_{ij})s_j = 0,$$

where δ_{ij} is the Kronecker Delta, taking value 1 if $i = j$ and 0 otherwise. Now let A be the matrix with $A_{ij} = t\delta_{ij} - r_{ij}$, and set $\Delta = \det A$ and $\underline{s} = (s_1, \dots, s_n)^\intercal$. Then $A\underline{s} = 0$, hence $0 = (A^{\mathrm{adj}})A\underline{s} = \Delta\underline{s}$ where A^{adj} is the adjoint matrix. Therefore $\Delta s_i = 0$ for all i. But $1 \in S$ is a linear combination of the s_i, so in particular we have $\Delta = \Delta \cdot 1 =$. Therefore the monic polynomial $\det(x\delta_{ij} - r_{ij})$ over R is satisfied by t.

(iii) Exercise.

□

Corollary 15.7. *Let S be a field and R a subring of S such that S is a finite R-algebra. Then R is a field.*

Proof. For any $0 \neq r \in R$, the inverse r^{-1} exists in S, so we must show $r^{-1} \in R$. Now by Proposition 15.6(ii), r^{-1} satisfies a monic polynomial over R, say

$$r^{-n} + a_{n-1}r^{-n+1} + \cdots + a_1 r^{-1} + a_0 = 0$$

for some $a_i \in R$. Then multiply by r^{n-1} to get

$$r^{-1} = -(a_{n-1} + a_{n-2}r + \cdots + a_0 r^{n-1}) \in R,$$

so R is a field. $\square$

We will prove the normalisation theorem for infinite fields K, and for this the following lemma is crucial:

Lemma 15.8. *Let K be an infinite field and $f \in K[x_1, \ldots, x_n]$ be a non-zero polynomial. Then there exist $\alpha_1, \ldots, \alpha_n \in K$ such that $f(\alpha_1, \ldots, \alpha_n) \neq 0$.*

Proof. We prove this by induction on n, with the case $n = 0$ being trivial. If now $n = 1$ then any non-zero $f \in K[x_1]$ has at most $\deg(f)$ roots. Since K is infinite, we can choose α_1 not equal to any of these roots and thus $f(\alpha_1) \neq 0$.

Assume now that $n > 1$ and the result holds for $n - 1$. Let $f \in K[x_1, \ldots, x_n]$ be non-zero. If $f \in K[x_1, \ldots, x_{n-1}]$ then we are done, so assume this is not the case. Then we can write

$$f = g_r x_n^r + \cdots + g_1 x_n + g_0$$

for some $g_i \in K[x_1, \ldots, x_{n-1}]$ with $g_r \neq 0$. Now by induction, there exist $\alpha_1, \ldots, \alpha_{n-1} \in K$ such that $g_r(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. Therefore $f(\alpha_1, \ldots, \alpha_{n-1}, x_n) \in K[x_n]$ is a non-zero polynomial, so by the $n = 1$ case above we see that there exists $\alpha_n \in K$ with $f(\alpha_1, \ldots, \alpha_n) \neq 0$. $\square$

Theorem 15.9 (Noether Normalisation)**.** *Let K be an infinite field and S a finitely generated K-algebra. Then there exist $z_1, \ldots, z_m \in S$ such that:*

(i) $z_1, \ldots, z_m$ are algebraically independent over K, i.e. there is no non-zero polynomial $f \in K[x_1, \ldots, x_m]$ such that $f(z_1, \ldots, z_m) = 0$;

(ii) S is finite over $R = K[z_1, \ldots, z_m]$.

Proof. Suppose $S = K[y_1, \ldots, y_n]$ and $f \in K[x_1, \ldots, x_n]$ is such that $f(y_1, \ldots, y_n) = 0$, i.e. $y_1, \ldots, y_n$ are algebraically dependent over K. Then choose $\alpha_1, \ldots, \alpha_{n-1} \in K$ and set $z_i = y_i - \alpha_i y_n$ for $1 \leqslant i \leqslant n - 1$. Now let $g \in K[x_1, \ldots, x_n]$ be such that

$$g(z_1, \ldots, z_{n-1}, y_n) = f(z_1 + \alpha_1 y_n, \ldots, z_{n-1} + \alpha_{n-1} y_n, y_n) = 0.$$

If f has degree d then let f_d be the sum of all monomials of f of degree d (the homogeneous piece of f of degree d). Then

$$\begin{aligned} f_d(z_1 + \alpha_1 y_n, \ldots, z_{n-1} + \alpha_{n-1} y_n, y_n) &= f_d(\alpha_1 y_n, \ldots, \alpha_{n-1} y_n, y_n) + \textit{lower order terms in } y_n \\ &= f_d(\alpha_1, \ldots, \alpha_{n-1}, 1) y_n^d + \textit{lower order terms in } y_n. \end{aligned}$$

Therefore considering g as a polynomial in y_n over $K[z_1, \ldots, z_{n-1}]$ we have

$$g(z_1, \ldots, z_{n-1}, y_n) = f_d(\alpha_1, \ldots, \alpha_{n-1}, 1) y_n^d + \textit{lower order terms in } y_n,$$

Since $f_d \neq 0$ (as $\deg(f) = d$), we have by Lemma 15.8 that there exist $\alpha_1, \ldots, \alpha_{n-1}$ such that $f_d(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0$. For this choice we have

$$f_d(\alpha_1, \ldots, \alpha_{n-1}, 1)^{-1} g(z_1, \ldots, z_{n-1}, y_n) = 0,$$

a monic polynomial over $K[z_1, \ldots, z_{n-1}]$ satisfied by y_n. Therefore y_n is integral over $K[z_1, \ldots, z_{n-1}]$.

The proof of the theorem is now by induction on the number n of generators of S. Suppose $S = k[y_1, \dots, y_n]$ is such that $y_1, \dots, y_n$ are algebraically independent, then we are done. Otherwise there exists some $f \in K[x_1, \dots, x_n]$ such that $f(y_1, \dots, y_n) = 0$. Then by the above we can choose $z_1, \dots, z_{n-1} \in S$ such that y_n is integral over $S^* = K[z_1, \dots, z_{n-1}]$ and $S = S^*[y_n]$. By the induction hypothesis applied to S^* there exist elements $w_1, \dots, w_m \in S^*$ that are algebraically independent over K with S^* finite dimensional over $R = K[w_1, \dots, w_m]$. Now since y_n is integral over S^* it follows by Proposition 15.6(iii) that $S^*[y_n]$ is a finite S^*-algebra. Since both extensions $R \subseteq S^*$ and $S^* \subseteq S$ are finite, it follows by Proposition 15.6(i) that the extension $R \subseteq S$ is finite as required. $\square$

Remark. (i) In fact Theorem 15.9 does hold for finite fields, but an alternative proof is needed (for instance, see [2] or [1]). In the following we will assume the normalisation theorem for any field.

(ii) Theorem 15.9 shows that any finitely generated extension $K \subseteq S$ can be written as a composite

$$K \subseteq K[z_1, \dots, z_m] \subseteq S,$$

where the first extension is polynomial and the second is finite.

Example 15.10. Let again $S = K[x, y]/\langle xy\rangle = K[\overline{x}, \overline{y}]$. We want to show that S is finite over some $K[z]$. As in the proof of the theorem, $f(\overline{x}, \overline{y}) = \overline{x} \cdot \overline{y} = \overline{0}$ in S. Thus we have $d = \deg f = 2$. Now we find an $\alpha_1 \in K$ such that $f(\alpha_1, 1) \neq \overline{0}$, e.g., $\alpha_1 = 1$. Then set $z := \overline{x} - 1 \cdot \overline{y}$ and get $g(z, \overline{y}) = f(z + \overline{y}, \overline{y}) = (z + \overline{y})\overline{y} = z\overline{y} + \overline{y}^2$. One has $g(z, \overline{y}) = \overline{0}$ and thus $S = K[z, y]/\langle yz + y^2\rangle$ is finite over $R = K[z]$.

Theorem 15.11 (Weak Nullstellensatz)**.** *Let K be a field and S a finitely generated K-algebra. If S is also a field, then S is finitely generated as a K-module.*

In particular, if K is algebraically closed then every maximal ideal of $K[x_1, \dots, x_n]$ is of the form $\langle x_1 - a_1, \dots, x_n - a_n\rangle$ for some $a_1, \dots, a_n \in K$.

Proof. Using Theorem 15.9 (Noether Normalisation) there exists a polynomial subalgebra $R = K[x_1, \dots, x_r]$ of S, over which S is a finite algebra. If S is a field then so is R by Corollary 15.7. If $r \geqslant 1$ then $\langle x_1\rangle$ is a proper ideal in R, a contradiction. Therefore S is finitely generated as an R-module.

For the second part, suppose $R = K[x_1, \dots, x_n]$ and $\mathfrak{m} \subseteq R$ is a maximal ideal. Then by the first part of the theorem we have that $R/\mathfrak{m}$ is a finite dimensional K-algebra. So given $\alpha \in R/\mathfrak{m}$ we have $m(\alpha) = 0$ for some monic polynomial $m \in K[t]$ of degree r by Proposition 15.6(ii). Since K is algebraically closed, we can write $m = (t - \alpha_r) \dots (t - \alpha_r)$ for some $\alpha_1, \dots, \alpha_r \in K$. As $R/\mathfrak{m}$ is a field and $m(\alpha) = 0$ we have $\alpha = \alpha_i$ for some i. Therefore $\alpha \in K$ and so $R/\mathfrak{m} = K$. Thus $x_i + \mathfrak{m} = a_i + \mathfrak{m}$ for some $a_i \in K$, and so $\langle x_1 - a_1, \dots, x_n - a_n\rangle \subseteq \mathfrak{m}$. Since both sides are maximal ideals, this is an equality. $\square$

Bibliography

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802]. 29, 37

[2] Miles Reid. *Undergraduate commutative algebra*, volume 29 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1995. 30, 37