Rings and Modules Notes

Francesco Chotuck

Abstract

This is KCL undergraduate module 6CCM350A, instructed by Dr. Peter Jossen. The formal name for this class is “Rings and Modules”.

Contents

1 Ring theory

1.1 Definitions

Definition 1.1. A **ring** is a tuple $(R, 0_R, 1_R, +, \cdot)$ consisting of a set R with two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ (called addition and multiplication) satisfying the following axioms:

1. $(R, +)$ is an abelian group with a neutral element 0_R, which we call the **zero element** of the ring;

2. The operation $\cdot$ is associative and 1_R is a neutral element for it, which we call the **unit element** of the ring;

3. The distributivity laws hold in R i.e.: for all $x, y, a, v \in R$ we have

$$(x + y) \cdot (a + b) = (x \cdot a) + (x \cdot b) + (y \cdot a) + (y \cdot b);$$

4. For all $x \in R$ we have $x \cdot 0_R = 0_R \cdot x = 0_R$.

Definition 1.2. A ring is called **commutative** if its multiplication operation is commutative.

Remark 1.3. For ease of notation: when talking about a ring R we suppose the data $0_R, 1_R, +$ and $\cdot$ is given, without incorporating it in the notation. If possible we will refer to the zero and unit element by 0 and 1, if no confusion is possible. We will also write multiplication in R by xy rather than $x \cdot y$. The additive inverse of $x \in R$ is denoted by $-x$, and instead of writing $x + (-y)$ we will write $x - y$. Furthermore, given an integer $n \geq 1$ and an element $x \in R$, we can write

$$nx = \underbrace{x + x + \cdots + x}_{n \text{ times}} \quad \text{and} \quad x^n = \underbrace{x \times x \times \cdots x}_{n \text{ times}},$$

and abbreviate $n \cdot 1_R$ as n_R or just n (if possible). As such we have that $(n+m)_R = n_R + m_R$ and $n_R x = nx$ in R. Lastly, we set $(-n)_R = -(n_R)$ so that n_R and nx are defined for all $n \in \mathbb{Z}$.

Note 1.4. The condition that a ring R has a unit element and the distributivity laws hold forces the commutativity of addition. To see this, compute the product $(1 + 1)(a + b)$ in two different ways, using the distributivity laws (but not assuming that addition is commutative). One obtains

$$(1 + 1)(a + b) = 1(a + b) + 1(a + b) = 1a + 1b + 1a + 1b = a + b + a + b$$

and

$$(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = 1a + 1a + 1b + 1b = a + a + b + b.$$

Since R is a group under addition, this implies $b + a = a + b$.

Proposition 1.5. Let R be a ring. Then for all $x, y \in R$ we have

- $0x = x0 = 0$;

- $(-x)y = x(-y) = -(xy)$;
- $(-x)(-y) = xy$;
- $(nx)y = x(ny) = n(xy)$ for any $n \in \mathbb{Z}$.

Definition 1.6. The **characteristic** of a ring R is defined as the smallest positive integer n such that $n \cdot 1_R = 0$, where 1_R is the multiplicative identity in R. If no such n exists, the characteristic is said to be zero, indicating that multiplying 1_R by any integer yields a non-zero result.

1.1.1 Special elements in a ring

Definition 1.7. A **unit** in a ring is an element which has a multiplicative inverse.

Proposition 1.8. The units of a non-trivial ring R form a group with respect to multiplication, and $R^\times$ is called the group of units of R.

Definition 1.9. Let R be ring.

- A non-zero element $x \in R$ is element is a **left zero divisor** if there exists a non-zero $y \in R$ such that $xy = 0$.
- A non-zero element $y \in R$ is a **right zero divisor** if there exists a non-zero $x \in R$ such that $xy = 0$.

> **Remark 1.10.** A *zero divisor can never be a unit.*
>
> *Proof.* Suppose that $x \in R$ is a unit and that $xy = 0$ for some non-zero $y \in R$. Then $ux = 1$ for some $u \in R$ so, $y = 1y = (ux)y = u(xy) = u0 = 0$, a contradiction. □

Definition 1.11. Let R be a non-commutative ring and $ab = x$.

- We say that a is a **left divisor** and b a **right divisor** of x.
- We say that x is a **right multiple** of a and a **left multiple** of b.

1.1.2 Special kind of rings

Definition 1.12. A non-trivial ring R is called an **integral domain**

- if it is commutative and,
- if $x \cdot y = 0$ implies $x = 0$ or $y = 0$ for all $x, y \in R$.

> **Remark 1.13.** An integral domain is a non-trivial commutative ring with **NO** zero divisors.

Example 1.14. The ring $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, since $[2]_4 \cdot [2]_4 = [0]_4$; but $\mathbb{Z}$ is an integral domain.

Proposition 1.15 (Canellation law in integral domains)
In an integral domain for any non-zero element $x \in R$ if

$$xu = xv \Rightarrow u = v$$

holds for all $u, v \in R$.

Proof. If $xu = xv$ then $x(u-v) = 0$ so, either $x = 0$ or $u - v = 0$. Since $x \neq 0$ we have that $u = v$. □

Definition 1.16. A non-trivial ring R is called a **division ring/algebra** (or **skew field**) if every non-zero element $x \in R$ has a multiplicative inverse.

Definition 1.17. A **field** is a commutative ring R such that for all non-zero elements $x \in R$ has a multiplicative inverse.

Note 1.18. Equivalently, a field is a commutative division ring.

Example 1.19. Some common examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}/p\mathbb{Z}$ where p is a prime. However, $\mathbb{Z}$ is not a field.

Theorem 1.20. A finite integral domain is a field.

Proof. Let $R = \{r_1, r_2, \ldots, r_l\}$ be a finite integral domain. For any $r_i \neq 0$ and $j \neq k$ we have $r_i(r_j - r_k) \neq 0$, since $r_j \neq r_k$ and there are no zero-divisors. Thus,

$$\{r_i r_1, r_i r_2, \ldots, r_i r_l\} = R$$

and in particular one of these is $r_i r_j = 1$. □

Definition 1.21. Let $(R, 0_R, 1_R, +, \cdot)$ be a ring. The **opposite ring** is the ring R^{op} given by the same set R, the same zero 0_R and one 1_R, carrying the same addition as R but whose multiplication $*$ is defined by

$$x * y = y \cdot x$$

for all $x, y \in R$.

1.1.3 Subrings

Definition 1.22. If R is a ring, and S is a subset of R we say that S is a **subring** of R if

- $(S, +)$ is a subgroup of R,
- S is closed under multiplication, and
- $1_R \in S$.

Theorem 1.23 (Subring test)**.** For any ring R, a subset S of R is a subring if and only if

1. $S \neq \varnothing$;
2. $\forall x, y \in S : x + (-y) \in S$ and
3. $\forall x, y \in S : xy \in S$.

Proof. We split the proof into parts:

- Proof of ($\Rightarrow$):
  Suppose S is a subring of R then, S is a subgroup of R with respect to addition thus, $y \in S \Rightarrow -y \in S$. We have that S is closed under multiplication and addition so,
  $$x, y \in S \Rightarrow x, -y \in S \Rightarrow x + (-y) = x - y \in S.$$
- Proof of ($\Leftarrow$):
  From the non-empty condition we have that $x \in S \Rightarrow x - x = 0 \in S$. Now, $0, x \in S \Rightarrow 0 - x = -x \in S$ i.e. each element has an additive inverse. Next, let $x, y, -y \in S$ then, from the first condition
  $$0, -y \in S \Rightarrow x - (-y) = (x + y) \in S$$
  i.e. S is closed under multiplication.

□

1.1.4 Polynomial rings

Definition 1.24. Let R be a ring. A **polynomial** in intermediate x, with coefficients in R, is a formal expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{with} \quad a_i \in R.$$

We write $R[X]$ for the set of all such polynomials.

Remark 1.25. We say $f(x) = g(x)$ if the coefficients a_i agree for all i.

Note 1.26. This construction is called **adjoining** an element: start with a ring R, and add a new element x. This x could be a “formal variable”, or it could be a known element of some other ring containing R. We build $R[X]$, which contains all elements of R as well as the new element x. Since we allow addition and multiplication we must also include x^k, rx^k where $r \in R$, and sums.

Proposition 1.27. The set $R[X]$ is a ring with the obvious choice of addition, multiplication, zero and identity elements.

Proposition 1.28. If the ring R has zero divisor then so does $R[X]$.

Proof. $R \subset R[X]$. □

Proposition 1.29

Let R be an integral domain. Then,

- the units of $R[X]$ are just the units of R,
- $R[X]$ is an integral domain.

Definition 1.30. Define $R[X, Y] = (R[X])\,[Y]$ and so on.

Definition 1.31. Let R be a ring. The **degree** of a non-zero polynomial $f(x) = \sum_{i=0}^{d} a_i x^i \in R[X]$ is the integer

$$\deg(f) = \max\{i : a_i \neq 0\}.$$

We denote $\deg(0) = -\infty$.

Proposition 1.32. The following two inequality hold for all non-zero polynomials $f, g \in R[X]$

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\} \quad \text{and} \quad \deg(fg) \leq \deg(f) + \deg(g).$$

If $R[X]$ is an integral domain the second inequality is an equality for all f and g.

Proposition 1.33 (Euclidean algorithm for polynomials)

Let F be a field and $f, g \in F[X]$. Then there is some $q, r \in F[X]$ such that

$$f = gq + r \quad \text{with} \quad \deg(r) < \deg(g).$$

Corollary 1.34. Division with remainder can be done whenever the leading coefficient of f is a unit.

Corollary 1.35. Let $g(x) \in R[X]$, and let $\alpha \in R$. The remainder of division of $g(x)$ by $x - \alpha$ is $g(\alpha)$.

1.2 Ring homomorphisms and isomorphisms

Definition 1.36. Let R and K be rings. A **ring homomorphism** from R to K is a map $f : R \to K$ satisfying

- $f(0_R) = 0_K$,
- $f(1_R) = 1_K$,

$$f(x +_R y) = f(x) +_K f(y) \quad \text{and} \quad f(x \cdot_R y) = f(x) \cdot_K f(y)$$

for all elements $x, y \in R$.

Definition 1.37. The set for all homomorphism from R to K denoted by $\mathrm{Hom}(R, K)$.

Definition 1.38. Let R be a ring. A ring homomorphism $f : R \to R$ is called a **ring endomorphism**. If f is bijective it is a **ring automorphism**.

Definition 1.39. If for a ring homomorphism $f : R \to K$ there is also a ring homomorphism $g : K \to R$ such that $g \circ f = 1_R$ and $f \circ g = 1_K$ then f is a **ring isomorphism**.

Note 1.40. This is equivalent to saying that f is a bijective map. However, sometimes it is too difficult to prove bijectivity thus, finding the inverse map is more convenient (and often simpler).

Example 1.41

Some important examples of ring homomorphisms. Let R be a ring.

- There is a ring homomorphism $f : \mathbb{Z} \to R$ defined by $f(n) = n_R$, and this is in fact the only ring homomorphism from $\mathbb{Z}$ to R. We call this the **canonical homomorphism**.
- The evaluation homomorphism which evaluates polynomials for a given value: $R[X] \to R$ with $p(x) \mapsto p(a)$.

Definition 1.42. The **kernel** of a ring homomorphism $f : R \to K$ is the set

$$\ker(f) := \{r \in R : f(r) = 0_K\}.$$

Example 1.43. The map $f : Z \to \mathbb{Z}/m\mathbb{Z}$ given by $n \mapsto [n]_m$ is a ring homomorphism, and $\ker(f) = m\mathbb{Z}$.

Definition 1.44. The **image** of a ring homomorphism $f : R \to K$ is the set

$$\operatorname{Im}(f) = \{k \in K : k = f(r) \text{ for some } r \in R\}.$$

Proposition 1.45. Let R and K be rings and let $f : R \to K$ be a ring homomorphism. Then,

- f is injective if and only if $\ker(f) = \{0_R\}$;
- f is surjective if and only if $\operatorname{Im}(f) = K$;
- the image of f is a subring of K;
- If $\alpha \in \ker(f)$ then $r\alpha, \alpha r \in \ker(f)$ for every $r \in R$, i.e. the kernel is closed under multiplication by elements from R.

Remark 1.46. The kernel is generally NOT a subring.

1.2.1 R-algebra

Definition 1.47. Let R be a ring. An R-**algebra** is a ring A together with a ring homomorphism $f : R \to A$. The homomorphism f is referred to as the **structural map**.

Note 1.48. A R-algebra is a ring with 'scalar multiplication' where the scalars come from R.

Example 1.49

Some examples of R-algebras.

- Every ring R is a $\mathbb{Z}$-algebra. We can choose the structural map to be $f : \mathbb{Z} \to R$ with $n \mapsto n_R$. However, this map is not injective! For example, take $R = \mathbb{Z}/10\mathbb{Z}$.
- Every ring R is an R-algebra.

Definition 1.50. Let R be a ring and let A and B be R-algebras. An R**-algebra homomorphism** $f : A \to B$ is a ring homomorphism satisfying $f(xa) = xf(a)$ for all $x \in R$ and all $a \in A$.

1.3 Ideals and quotient rings

In this section we deal with non-commutative rings in general. As such many definitions will have a *left* and *right* versions. When working in a commutative ring, the difference between left and right vanishes.

1.3.1 Definitions

Definition 1.51. Let R be a ring, a subset $I \subseteq R$

- is called a **left ideal** of R if
  - $(I, +)$ is a subgroup of $(R, +)$, and
  - for every $r \in R$ and every $i \in I$ we have $ri \in I$.
- is called a **right ideal** in R 'idem' with $ir \in I$;
- we say that I is a **two-sided ideal** if both $ri, ir \in I$ for every element $i \in I$ and every $r \in R$.

Note 1.52. We can interpret the multiplication condition for left ideals as for all $r \in R$ we have $rI \subseteq I$.

Example 1.53

The subsets $\{0\}$ and R are two-sided ideals.

Definition 1.54. A **proper ideal** of a ring R is an ideal which is different from R.

Lemma 1.55

Let I be an ideal of R. We have that I contains a unit if and only if $I = R$.

> **Remark 1.56.** By the definition of a ring and subring in this course an ideal is not a subring, unless the ideal is the ring itself.

Proof. We split the proof in two parts.

- Proof of ($\Rightarrow$).
  If $I = R$ then I contains the unit 1.

- Proof of ($\Leftarrow$).
  If x is a unit in I with inverse y, then for any $r \in R$
  $$r = r \cdot 1 = r(yx) = (ry)x \in I$$
  hence $R = I$.

□

Proposition 1.57. If $f : R \to K$ is a ring homomorphism then, $\ker(f)$ is a two-sided ideal of R.

Proof. For any $r \in R$ we have $f(\alpha) = f(r)f(\alpha) = f(r) \cdot 0 = 0$ and also $f(\alpha r) = f(\alpha)f(r) = 0 \cdot f(r) = 0$ so, $r\alpha, \alpha r \in \ker(f)$. □

Definition 1.58. Let R be a ring and let $I \subseteq R$ be a left ideal. We say that I is a **principal left ideal** if there exists an element $a \in I$ such that
$$I = Ra = \{r \cdot a : r \in R\}$$
holds. We call $a \in I$ a **generator** of I.

Definition 1.59. Let X be any subset of the ring R. The **left ideal generated** by X is the subset
$$\langle X \rangle = \{r_1x_1 + \cdots + r_nx_n \mid r_1, \ldots, r_n \in R, x_1, \ldots, x_n \in X\}$$
of R. An ideal $I \subseteq R$ is called **finitely generated** if there exists a finite set $X \subseteq R$ such that $I = \langle X \rangle$.

Definition 1.60. An ideal I is **principal** if $I = \langle a \rangle$ for some $a \in R$.

Example 1.61. All ideals of $\mathbb{Z}$ are principal because they all take the form $m\mathbb{Z}$ for $m \in \mathbb{Z}$.

Proposition 1.62

A non-trivial commutative ring R is a field if and only if its only ideals are $\{0\}$ and R.

Proof. We prove each direction in turn.

- Proof of ($\Rightarrow$).
  Let $I \subseteq R$ be and ideal and R be a field. Suppose $x \neq 0 \in I$. Then as x is a unit we have $I = R$.

- Proof of ($\Leftarrow$).
  Suppose $x \neq 0 \in R$. Then $\langle x \rangle$ is an ideal of R. It is not $\{0\}$ since it contains x so, $\langle x \rangle = R$. That is, $1 \in \langle x \rangle$ but, we defined $\langle x \rangle = \{x \cdot y : y \in R\}$. Therefore, there exists some $u \in R$ such that $x \cdot u = 1$ hence, x is a unit. Since the choice of x was arbitrary we have that R is a field.

□

1.3.2 Quotient rings

Definition 1.63. Let $I \subseteq R$ be a left ideal. The **quotient ring** R/I consists of the (additive) cosets $r + I$ with

- the zero element as $0_R + I$ and,
- unit element ad $1_R + I$.

It has the following operations:

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$$
$$(r_1 + I) \cdot (r_2 + I) = r_1 r_2 + I.$$

Remark 1.64. Equivalently,R/I is the quotient of R modulo the equivalence relation $\sim$ defined by

$$x \sim y \iff x - y \in I$$

for all $x, y \in R$. We will denote the equivalence classes by $[x]$ that is, the coset $x + I$.

Proposition 1.65. Let R be a ring and let $I \subseteq R$ be a two-sided ideal. Denote the quotient map by $\pi : R \to R/I$, we have that the maps

$$J \mapsto \pi(J) = J/I \quad \text{and} \quad K \mapsto \pi^{-1}(K) = \{r \in R : \pi(r) \in K\}$$

- are bijective;
- are inverse maps to each other;
- respect inclusion i.e. given two left ideals J_1 and J_2 in R containing I such that $J_1 \subseteq J_2$, then their images under the quotient map will also have the inclusion $J_1/I \subseteq J_2/I$ in R/I.

Note 1.66. This theorem is saying that the ideals of R/I ar ein bijection with ideals of R which contain I.

Theorem 1.67 (Ring isomorphism theorem)
Let R be a ring. If $f : R \to K$ is a ring homomorphism then $R/\ker(f) \cong f(R)$.

1.3.3 Ideal arithmetic

Definition 1.68. Let R be a commutative ring and let $I, J \subseteq R$ be ideals. We can construct the following sets:

1. The **sum** $I + J = \{i + j : i \in I, j \in J\}$.
2. The **intersection** $I \cap J$.
3. The **product** $I \cdot J = \{i_1 j_1 + \cdots + i_n j_n : i \in I, j \in J\}$.
4. The **quotient** $(I : J) = \{r \in R : rJ \subseteq I\}$.

Proposition 1.69

All the sets above are ideals of R.

Example 1.70. Let $I = \langle x^2, y\rangle$ and $J = \langle x, y^2\rangle$ in $\mathbb{C}[X, Y]$. Then, $I + J = \langle x, y\rangle$ and $I \cap J = \langle x^2, xy, y^2\rangle$.

Example 1.71

In the ring of integers, all the ideals take the form of $m\mathbb{Z}$ for $m \in \mathbb{Z}$ thus, the sum and intersection of ideals are

$$m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z} \quad \text{and} \quad m\mathbb{Z} \cap n\mathbb{Z} = \operatorname{lcm}(m, n)\mathbb{Z}.$$

Remark 1.72. Some formulas to know:

- $\gcd(a, b)\operatorname{lcm}(a, b) = |ab|$;
- $\gcd(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$;
- $\operatorname{lcm}(a, b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$.

Definition 1.73. Let R be a commutative ring and let $I, J \subseteq R$ be ideals. We say

- I **divides** J if $J \subseteq I$ and,
- we say I and J **coprime** if $I + J = R$.

Proposition 1.74

Let R be a commutative ring and let $I, J \subseteq R$ be ideals. The inclusion $I \cdot J \subseteq I \cap J$ <u>holds</u>, and it is an equality if I and J are coprime.

Proof. The inclusions $I \cdot J \subset I$ and $I \cdot J \subset J$ are trivial since both I and J are ideals, so it follows from the definition. Next, suppose that I and J are coprime. There exists $a_0 \in I$ and $b_0 \in J$ such that $1 = a_0 + b_0$. For every element x of $I \cap J$ we find $x = a_0x + xb_0 \in I \cdot J$. □

1.3.4 Prime ideals and maximal ideals

Definition 1.75. Let R be a ring. A proper ideal $I \subsetneq R$ is called a **prime ideal** if

$$\forall x, y \in R \text{ we have } xy \in I \Rightarrow x \in I \text{ or } y \in I.$$

Example 1.76. The ideal $m\mathbb{Z} \subset \mathbb{Z}$ is a prime ideal if and only if $m = 0$ or m is prime;

Definition 1.77. An ideal I of a ring R is **maximal** if $I \neq R$ and for any ideal J with $I \subseteq J \subseteq R$ either $J = I$ or $J = R$.

Proposition 1.78. Let R be a commutative ring, and let $I \subseteq R$ be a proper ideal. The following statements are equivalent:

1. the ideal I is prime.

2. If I divides a product of ideals $J \cdot K$ then I divides J or K.

Proof. We split the proof into parts.

- Proof of (1) $\Rightarrow$ (2).
  Let $I \subseteq R$ be a prime ideal and let J, K be ideals of R such that $J \cdot K \subseteq I$. We must show that $J \subseteq I$ or $K \subseteq I$ holds. If this was not the case then, there would exist an element $j \in J$ and $k \in K$ none of which belong to I. However, $jk \in I$, contradicting the assumption that I is prime.

- Proof of (2) $\Leftarrow$ (1).
  Let $I \subseteq R$ be an ideal satisfying (2) and let $a, b \in R$ be elements such that $ab \in I$. We must show that $a \in I$ or $b \in I$. Setting $J = aR$ and $K = bR$ we find that $J \cdot K = abR \subseteq I$. Hence, by the hypothesis $aR \subseteq I$ or $bR \subseteq I$.

□

Proposition 1.79

Let R be a commutative ring and let $I \subsetneq R$ be a proper ideal. Then

1. The ideal I is prime $\iff$ R/I is an integral domain.

2. The ideal I is maximal $\iff$ R/I is a field.

Proof. We prove each bullet point and direction in turn.

1. - Proof of ($\Rightarrow$).
     Suppose I is a prime ideal and let $[x], [y] \in R/I$ such that $[x][y] = [xy] = [0]$ i.e. $xy \in I$. Since I is prime we deduce that $x \in I$ or $y \in I$ hence, $[x] = 0$ or $[y] = 0$. The definition for R/I to be an integral domain.
   - Proof of ($\Leftarrow$).
     Suppose R/I is an integral domain, and let $x, y \in R$ such that $xy \in I$. Therefore, $[x][y] = [xy] = [0]$, and since R/I is an integral domain we have $[x] = [0]$ or $[y] = 0$ i.e. $x \in I$ or $y \in I$.

2. - Proof of ($\Rightarrow$).
     Suppose I is a maximal ideal, and let $x \in R$ be any element such that $[x]$ is non-zero in R/I. We must show that there exists an element $y \in R$ such that $[x][y] = [1]$. To say that $[x]$ is non-zero in R/I is to say that $x \notin I$. The subset

     $$J = \{u + xy \mid u \in I, y \in R\}$$

     is an ideal, and it contains I strictly because $x \in J$ and $x \notin I$. Since I is a maximal ideal, we conclude $J = R$, and hence in particular $1 \in J$. That means that there exist elements $u \in I$ and $y \in R$ such that $1 = u + xy$. Modulo I, this relation reads $[1] = [0] + [xy] = [x][y]$, hence $[y]$ is the multiplicative inverse to $[x]$.

- Proof of ($\Leftarrow$).
  Suppose R/I is a field, and let J be an ideal of R containing I strictly. We need to show that $J = R$. Let x be any element of J which is not in I. Then the element $[x]$ is non-zero in the field R/I, hence it has a multiplicative inverse. In other words, there exists $y \in R$ such that $[x][y] = [1]$. We can rewrite this as $[xy] - [1] = [0]$ or as $xy - 1 \in I$. Since $x \in J$ we have $xy \in J$ and since $I \subseteq J$ we have $(xy - 1) \in J$, hence we deduce that
  $$1 = xy - (xy - 1)$$
  belongs to J. But then, $z = 1z$ belongs to J for all $z \in R$, hence $J = R$ as claimed.

□

Corollary 1.80

Every maximal ideal is a prime ideal.

Proof. If the ideal $I \subseteq R$ is maximal then R/I is a field which also implies R/I is an integral domain hence, by the proposition above, I is prime. □

Example 1.81

Some examples of this property.

- In $\mathbb{Z}$ and $\mathbb{R}[X]$ every non-zero prime ideal is maximal.
- In $\mathbb{R}[X, Y]$ the ideal $\langle x, y\rangle$ is maximal, $\langle x\rangle$ is prime but not maximal, $\langle x^2\rangle$ is neither prime nor maximal.
- In $\mathbb{C}[X, Y]$ any ideal of the form $\langle x - a, y - b\rangle$ for $a, b \in \mathbb{C}$ is maximal.
- In $\mathbb{Z}[X]$, the ideal $\langle 2\rangle$ is prime but not maximal and, $\langle 2, x\rangle$ is maximal.

Proposition 1.82. Let R be a commutative ring. Every proper ideal $I \subseteq R$ is contained in a maximal ideal of R.

Proof. Let X be a set of all proper ideals of R. We have that $\{0\} \in X$ thus, X is non-empty. Let $\mathcal{C} \subseteq X$ be a chain of ideals of R containing I i.e. $\mathcal{C}$“=”$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$. The union
$$J = \bigcup_{\mathcal{I} \in \mathcal{C}} \mathcal{I}$$
is a proper ideal of R containing I. Therefore, $J \in X$ and it is an upper bound for $\mathcal{C}$ since $\mathcal{I} \subseteq J$ for all $\mathcal{I} \in \mathcal{C}$. The conditions for Zorn's lemma are satisfied, by applying it there exists a maximal ideal of R. □

1.3.5 Jacobson radical

Definition 1.83. Let R be a commutative ring. The **Jacobson radical** of R is the intersection of all maximal ideals of R.

Proposition 1.84

Let R be a commutative ring, and let $J \subseteq R$ be its Jacobson radical. An element $x \in R$ belongs to J if and only if $1 + xy$ is a unit for all $y \in R$.

Proof. We prove each direction in turn.

- Proof of ($\Rightarrow$).
  Let $x \in J$ and let $y \in R$. If $1 + xy$ is not a unit, then $1 + xy$ generates a proper ideal of R hence, it belongs to some maximal ideal, say $I_{\text{max}} \subseteq R$ by the proposition above. However, $x \in I_{\text{max}}$ thus $xy \in I$. As such, we have $1 = (1 + xy) - xy \in I$ contradicting the fact that I_{max} is a proper ideal of R.

- Proof of ($\Leftarrow$).
  Let $x \in R$ be an element such that $1 + xy$ is a unit for all $y \in R$ and let $I_{\text{max}} \subsetneq R$ be a maximal ideal. We show that $x \in I_{\text{max}}$. If $x \in I_{\text{max}}$, then $R = I_{\text{max}} + xR$ hence, there exists some $a \in I_{\text{max}}$ and $y \in R$ such that $1 = a + xy$. But, $a = 1 - xy$ is a unit contained in I_{max} contradicting the fact that I_{max} is a proper ideal of R.

□

1.4 Types of rings

1.4.1 Principal ideal domains

Definition 1.85. An integral domain R is called a **principal ideal domain** (PID) if every ideal of R is principal (i.e. every ideal is generated by a single element).

Proposition 1.86

Let R be a PID. Every non-zero prime ideal of R is maximal.

Proof. Let $I \subsetneq R$ be a non-zero prime ideal. Let $J \subseteq R$ be an ideal with $I \subseteq J \subseteq R$. We need to show that $I = J$ or $J = R$. Since R is a PID we must have that I and J are principal ideals so, let i and j be generators of the ideals I and J respectively. Since $I \subseteq J$ we have $i \in J$ hence, $i = jx$ for some $x \in R$. Since I is prime and $i = jx \in I$ we have $j \in I$ or $x \in I$. We have two cases.

- If $j \in I$ then $j = iy$ for some $y \in R$ thus, $i = iyx$ which implies that $xy = 1$ (we have applied the cancellation law since R is an integral domain). Therefore, x and y must be units so, $I = iR = jxyR = jR = J$.

- If $x \in I$ then $x = it$ for some $t \in R$ so, $i = jx = jit$ (commutativity applied) which implies $jt = 1$. We have that j and t are units so, $J = jR = R$ since j is a unit.

□

Theorem 1.87. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. Let $I \subset \mathbb{Z}$ be an ideal. If $I = \{0\}$ then I is principal, and we are done. If $I \neq \{0\}$ let $n \in I$ be the smallest positive element, and we claim that $I = n\mathbb{Z}$ holds. Since $n \in I$ the inclusion $n\mathbb{Z} \subseteq I$ holds. On the other hand, let $x \in I$, and we show that x is an integer multiple of n. Without loss of generality suppose $x > 0$. Division of x by n yields

$$x = nk + r$$

for some $k, r \in \mathbb{Z}$ satisfying $k \geq 0$ and $0 \leq r < n$. Since, $x \in I$ and $nk \in I$ we must have $r \in I$. However, n was chosen to be the smallest positive element of I and yet $r < n$. Therefore, the only possibility is $r = 0$ and hence, x is a multiple of n, showing $I \subseteq n\mathbb{Z}$. □

Theorem 1.88

Let K be a field. The ring of polynomials $K[X]$ is a principal ideal domain.

Proof. Let $I \subseteq K[X]$ be an ideal. If $I = \{0\}$ then I is principal, and we are done. If $I \neq \{0\}$ then let $f \in I$ be a non-zero polynomial with the smallest possible degree. Since $f \in I$ the inclusion $\langle f \rangle \subseteq I$ holds, and we claim that this is an equality. To verify this, let $g \in I$ be an arbitrary element. Long polynomial division of g by f yields

$$g = hf + r$$

for some $h, r \in K[X]$ with $\deg(r) \leq \deg(f)$. Since both g and hf belong to I also r belongs to I. However, f was chosen to be of minimal degree among non-zero elements of I and yet $\deg(r) \leq \deg(f)$. Therefore, the only possibility is $r = 0$ and hence, $g = hf$ is indeed a multiple of f, showing $\langle f \rangle = I$. □

1.4.2 Euclidean rings

Definition 1.89. Let R be an integral domain. A function

$$\sigma : R \backslash \{0\} \to \mathbb{Z}_{\geq 0}$$

is called a **Euclidean function** on R if for all $a, b \in R$ where $b \neq 0$ there exists $x, r \in R$ such that

$$a = bx + r \quad \text{and} \quad r = 0 \text{ or } \sigma(r) < \sigma(b).$$

If such function exists we say that R is a **Euclidean ring** with respect to σ.

Example 1.90. Take $R = \mathbb{Z}[i]$ then we can construct a Euclidean function σ such that $a + bi \mapsto a^2 + b^2$ or $z \mapsto |z|^2$.

Theorem 1.91

Every Euclidean ring is a PID.

Proof. Let R be a Euclidean ring with Euclidean function $\sigma : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. Let $I \subsetneq R$ be a non-zero ideal and let $b \in I \setminus \{0\}$ be an element with $\sigma(b)$ minimal. Then, for any $a \in I$ we write

$$a = bx + r \quad \text{with} \quad r = 0 \text{ or } \sigma(r) < \sigma(b).$$

However, any such r must be in I since $r = a - bx \in I$ and so, we cannot have $\sigma(r) < \sigma(b)$ hence, $r = 0$. We have that $a = bx$ so, $a \in \langle b \rangle$; since this is true for all $a \in I$ we must have $I \subseteq \langle b \rangle$. However, since $b \in I$ we must also have $\langle b \rangle \in I$ therefore, $I = \langle b \rangle$. □

1.4.3 Noetherian rings

Definition 1.92. A ring R is called **Noetherian** if every ideal of R is finitely generated.

Example 1.93

PID are Noetherian rings. The opposite is not true.

Proposition 1.94 (Characterisation of Noetherian rings)

Let R be a ring. The following statements are equivalent:

1. Every ideal of R is finitely generated.
2. Every ascending chain of ideals $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ of R is stationary, i.e. $\exists n \geq 0$ such that $I_n = I_{n+1} = I_{n+2} = \cdots$
3. Every non-empty set of ideals of R contains a maximal element with respect to inclusion i.e. let $\mathcal{I}$ be a non-empty set of ideals of a ring R there exists an ideal $M \in \mathcal{I}$ such that for every ideal $N \in \mathcal{I}$, if $M \subseteq N$, then $M = N$.

Proof. We prove each statement in turn.

1. Proof of (1) ⇒ (2).
   Let $I_0 \subseteq I_1 \subseteq \cdots$ be a chain of ideals of R. Let $J = \bigcup_{k=0}^{\infty} I_k$, this is an ideal of R, which is finitely generated by assumption. Let $x_1, \ldots, x_n$ be the finite set of generators of J. Each generator x_i belongs to one of the ideals I_k. Since these ideals form an ascending chain, there exists $k \geq 0$ such that I_k contains all generators $x_1, \ldots, x_n$. This implies $I_k = J$ and hence $I_k = I_m$ for all $m \geq k$, that is the chain of ideals is stationary.

2. Proof of (2) ⇒ (3).
   We use Zorn's lemma to prove this statement. Thus, we must show that the conditions for it are satisfied. Let S be a non-empty set of ideals in R and let $\mathcal{C} \subseteq S$ be a chain of ideals and pick $I_0 \in \mathcal{C}$. If $\mathcal{C}$ does not contain a maximal element, we may choose an element $I_1 \in \mathcal{C}$ containing I_0 strictly, then an element $I_2 \in \mathcal{C}$ containing I_1 strictly and so on. These choices produce an ascending chain of ideals $I_0 \subseteq I_1 \subseteq \cdots$ in S which is not stationary hence, contradicting the assumption (2). We conclude $\mathcal{C}$ contains a maximal element which is an upper bound in S.

3. Proof of (3) $\Rightarrow$ (1).
   Let I be an ideal of R and let S be the set of all finitely generated ideals of R which are contained in I. By assumption S has a maximal element which we denote by $I_{\max}$. Let $x \in I$ then $I_{\max} + \langle x \rangle \subseteq I$ is finitely generated and contains $I_{\max}$. However, we assumed $I_{\max}$ to be the maximal element so, $I_{\max} = I_{\max} + \langle x \rangle$ hence, $x \in I_{\max}$. In conclusion, $I_{\max} = I$.

□

Theorem 1.95 (Hilbert's basis theroem)**.** Let R be a Noetherian ring. Then $R[X]$ is also a Noetherian ring.

> **Note 1.96.** We can iterate this theorem and obtain that if R is Noetherian then $R[X_1, \dots, X_n]$ is also Noetherian.

Proof. Let J be an ideal of $R[X]$, and let us show that J is finitely generated. Given $f \in R[X]$ and $d \geq 0$, let us denote by $c_d(f)$ the coefficient of X^d in the polynomial f. Routine checking shows that the subsets $I_d \subseteq R$ defined by

$$I_d = \{c_d(f) \mid f \in J \text{ and } \deg f \leq d\}.$$

form a chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ of ideals in R. Since R is Noetherian, this chain is stationary, so there exists $n \geq 0$ such that $I_d = I_n$ for all $d \geq n$. Again because R is Noetherian, the ideals $I_0, \dots, I_n$ are finitely generated. Choose generators $a_{d,1}, \dots, a_{d,r_d}$ of I_d, and for each of these generators choose a polynomial $f_{d,k} \in I$ of degree $\leq d$ with $c_d(f_{d,k}) = a_{d,k}$. We claim that the finite set of polynomials

$$F = \{f_{d,k} \mid 0 \leq d \leq n, 1 \leq k \leq r_d\}$$

generate the ideal I. Let $g \in J$ be an element of J. We prove by induction on the degree of g that g belongs to the ideal $\langle F \rangle$. Suppose first that g is of degree zero, so a non-zero constant polynomial given by $a \in R$. Then an $a \in I_0$ can be written as

$$a = \sum_{i=1}^{r_0} x_i a_{0,i} = \sum_{i=1}^{r_0} x_i f_{0,i}$$

for some $x_i \in R$, hence $g \in \langle F \rangle$. Next, suppose that g is of degree $d > 0$ but $d \leq n$, and that every element of J of degree $< d$ belongs to $\langle F \rangle$. The coefficient $a = c_d(g)$ of g belongs to I_d, and it can therefore be written as

$$a = \sum_{i=1}^{r_d} x_i a_{d,i}$$

for some $x_i \in R$. Define a polynomial f belonging to $\langle F \rangle$ by

$$f = \sum_{i=1}^{r_d} x_i f_{d,i}.$$

The polynomial $h = g - f$ belongs to J and is of degree $< d$ since the leading coefficients of g and f are equal and cancel each other out. Hence, h belongs to $\langle F \rangle$ by induction hypothesis, and hence so does $g = h + f$. Finally, suppose g is of degree $d > n$, and that every element of J of degree $< d$ belongs to $\langle F \rangle$. The coefficient $a = c_d(g)$ of g belongs to I_n, hence can be written in the form (1.4). Define f again by (1.5) and note this time that $h = g - X^n f$ belongs to J and is of degree $< d$, hence belongs to $\langle F \rangle$ by induction. As before we conclude that $g \in \langle F \rangle$ and are done. □

Definition 1.97. Let R be a commutative ring, and let A be an R-algebra. We say that A is **finitely generated** if there exists $a_1, \dots, a_n$ such that every $a \in A$ can be written as a polynomial expression in $a_1, \dots a_n$ and elements of R i.e.

$$a = \sum_{i=0}^{n} r_i a_1^{n_{i,1}} a_2^{n_{i,2}} \cdots a_n^{n_{i,n}}.$$

Corollary 1.98 (Noetherian R-algebras)**.** Let R be a Noetherian ring. Then every finitely generated R-algebra is Noetherian.

Proof. Let A be a finitely generated R-algebra where $a_1, \dots a_n \in A$ are the generators. This means that the ring homomorphism

$$\begin{aligned} \phi : R[X_1, \dots, X_n] &\to A \\ x_i &\mapsto a_i \end{aligned}$$

is surjective. Let $I \subseteq A$ be an ideal then $\phi^{-1}(I) \subseteq R[X_1, \dots, X_n]$ is a finitely generated ideal, say generated by $f_1, \dots, f_p$/ Then $\phi(f_1), \dots, \phi(f_p)$ generate the ideal $\phi(\phi^{-1}(I)) = I$. □

1.4.4 Unique factorisation domains

Note 1.99. A unique factorisation domain (UFD) is an integral domain in which an analogue of the fundamental theorem of arithmetic holds: Every element can be factorised into a product of primes, and this factorisation is essentially unique.

Remark 1.100. All rings in this section are assumed commutative.

Definition 1.101. Let R be a ring. A non-zero element $r \in R$ is called **irreducible** if it is not a unit and if $r = ab$ implies that a or b is a unit.

Definition 1.102. Let R be a ring. For elements $x, y \in R$, we say x **divides** y, written $x \mid y$, if there exists $q \in R$ such that $y = qx$.

Definition 1.103. Let R be a ring. We say a non-zero element $r \in R$ is **prime** r is not a unit and whenever $r \mid xy$ either $r \mid x$ or $r \mid y$.

Example 1.104. In the ring of integers $\mathbb{Z}$, an element $m \in \mathbb{Z}$ is irreducible if and only if it is prime.

Example 1.105

In a general ring, prime elements and irreducible elements are not the same. In an integral domain however, prime elements are irreducible.

Definition 1.106. An integral domain R is said to be a **unique factorisation domain** if every non-zero element $x \in R$ can be written as

$$x = uy_1y_2 \cdots y_n$$

for some unit $u \in R^{\times}$ and irreducible elements $y_1, \dots, y_n \in R$ in an essentially unique way. By essentially unique we mean that the factorisation can be reordered, and the result would not change. That is, any two factorisation $x = ua_1 \cdots a_k = vb_1 \cdots b_m$, k and m must be the same.

Lemma 1.107. Let R be an integral domain and let $r \in R$ be non-zero element which is not a unit. If r is prime, then it is irreducible.

Proof. Let $r \in R$ be prime, and suppose $r = ab$. Since $r \mid r = ab$, and r is prime, we must have $r \mid a$ or $r \mid b$. Without loss of generality, assume $r \mid a$ so, $a = rc$ for $c \in R$. We can write $r = ab = rcb$, since R is an integral domain we must have $1 = cb$ hence, b is a unit. □

Lemma 1.108. Let R be a Noetherian integral domain, and let $x \in R$ be a non-zero element which is not a unit. There exists an irreducible element $y_1 \in R$ which divides x.

Proof. Let S be the set of all proper ideals of R of them form $\langle y \rangle$ where y is not a unit and is a divisor of x i.e. $x = yz$ for some $z \in R$. The set S contains $\langle x \rangle$ thus, is non-empty. By Proposition 1.94, the set S contains a maximal element, say $\langle y_1 \rangle$. We how that the divisor y_1 of x is irreducible. Let $y_1 = uv$ by any factorisation of y_1. Since y_1 is not a unit, one of the factors, say u, is also not a unit. Since u divides x, the ideal $\langle u \rangle$ belongs in S, and since u divides y_1 we have the inclusion $\langle y_1 \rangle \subseteq \langle u \rangle$. However, $\langle y_1 \rangle \in S$ was chosen to be the maximal element hence $\langle y_1 \rangle = \langle u \rangle$. We can write $u = wy_1 = wuv$ which implies $1 = wv$ so, v is a unit. Hence, y_1 is irreducible. □

Proposition 1.109

Let R be a Noetherian integral domain.

1. Every non-zero element of R is a product of irreducible elements.
2. The ring R is a UFD if and only if every irreducible element of R is prime.

Proof. We prove each statement in turn.

1. Let $x \in R$ be a non-zero element and define

   $$S = \{\langle z \rangle : x = y_1 \cdots y_n z \text{ where } y_i \text{ is irreducible}\}.$$

   The set S is non-empty as it contains $\langle x \rangle$, hence the set S contains a maximal element by Proposition 1.94, say $\langle u \rangle$ with

   $$x = y_1y_2 \cdots y_n u$$

   for some irreducible $y_1, \dots, y_n$. If $\langle u \rangle = R$ then u is a unit, and we are done. If not, the lemma above guarantees the existence of an irreducible element y_{n+1} dividing u, so $u = y_{n+1}v$ for some $v \in R$. As $x = y_1y_2 \cdots y_{n+1}v$ we find $\langle v \rangle \subseteq \langle u \rangle$ and $\langle u \rangle \subseteq \langle v \rangle$. But $\langle u \rangle$ was already chosen to be maximal, hence $\langle u \rangle = \langle v \rangle$. But this in turn implies that y_{n+1} is a unit, contradicting that y_{n+1} is an irreducible element, hence the only possibility is that u is in fact a unit.

2. We prove each direction in turn.

   - Proof of ($\Rightarrow$).
     Let $x \in R$ be an irreducible element, and let us show that x is prime. Let $y, z \in R$ such that $x = yz$. Since R is a UFD, we may factorise y and z into products of irreducibles. But x is already its own factorisation into irreducibles, hence we deduce from the uniqueness of the number of irreducible factors in any factorisation that either y is a unit and x divides z, or z is a unit and x divides y. In other words, x is prime.
   - Proof of ($\Leftarrow$).
     We have shown in part that every non-zero element of R admits a factorisation into a unit and a finite product of irreducible elements. It remains to show that this factorisation is essentially unique, given that every irreducible element of R is prime. Consider two factorisations of some non-zero element of R, that is, an equality of the form

     $$uy_1y_2 \cdots y_n = vz_1z_2 \cdots z_m$$

     with units u and v and irreducible elements $y_1, \dots, y_n, z_1, \dots, z_m$ in R, say with $n \leq m$. We need to show that these two factorisations are essentially the same in the sense of the definition of a UFD. If $n = 0$, then the left-hand side is the unit u, hence $m = 0$ as well, and we are done. Suppose now $n \geq 1$. Since y_n is irreducible, hence prime, y_n divides at least one of the irreducible elements $z_1, \dots, z_m$, say without loss of generality z_m, hence $z_m = y_nw$ for some $w \in R$. Since z_m is irreducible and y_n is not a unit, w must be a unit. Simplifying the equality by the common factor y_n yields an equality

     $$uy_1 \cdots y_{n-1} = vwz_1 \cdots z_{m-1}$$

     of factorisations with fewer factors. Arguing by induction on n finishes the proof.

□

Proposition 1.110

Every PID is a UFD.

Proof. PID are in particular Noetherian rings hence, using the proposition above it suffices to show that every irreducible element of R is prime. Let $x \in R$ be an irreducible, and suppose x divides a product uv. We must show that x divides u or v.

We claim that the ideal $\langle x \rangle$ is maximal. To prove this: let I be an ideal of R with $\langle x \rangle \subseteq I$. As R is a PID, the ideal I is generated by a single element say y. Therefore, $x = yz$ for some $z \in R$. Since x is irreducible, one of y or z is a unit. If z is a unit, then $I = \langle x \rangle$, and if y is a unit, then $I = R$.

Since $\langle x \rangle$ is maximal it means that it is also a prime ideal. As x divides uv the product $uv \in \langle x \rangle$ hence, either u or v belong to $\langle x \rangle$. Hence, x divides u or v. □

Corollary 1.111

Let R be a PID then, irreducible elements generate maximal ideals.

Proof. Let R be a PID and let $a \in R$ be an irreducible. Suppose that J is an ideal of R such that $(a) \subseteq J$. Since R is a PID, we have $J = (b)$ for some $b \in R$. The inclusion $(a) \subseteq (b)$ means that there exists $c \in R$ such that $a = bc$ and so, as a is irreducible, either b is a unit or c is a unit. In the first case, it follows that $(b) = R$ whereas, in the second case, it follows that $(c) = R$. Hence (a) is a maximal ideal of R. □

Example 1.112 (Counterexample)

Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

By definition, it is a subring of a field. So it is an integral domain. What are the units of the ring? There is a nice trick we can use, when things are lying inside $\mathbb{C}$. Consider the function

$$N : R \to \mathbb{Z}_{\geq 0}$$

given by

$$N(a + b\sqrt{-5}) \mapsto a^2 + 5b^2.$$

It is convenient to think of this as $z \mapsto zz^* = |z|^2$. This satisfies $N(z \cdot w) = N(z)N(w)$. This is a desirable thing to have for a ring, since it immediately implies all units have norm 1 — if $r \cdot s = 1$, then $1 = N(1) = N(r \cdot s) = N(r)N(s)$. So $N(r) = N(s) = 1$.

So to find the units, we need to solve $a^2 + 5b^2 = 1$, for a and b units. The only solutions are ± 1. So only ± 1 in R can be units, and these obviously are units. Hence, $R^\times = \{\pm 1\}$.

Next, we claim 2 in R is irreducible. We again use the norm. Suppose $2 = ab$. Then $4 = N(2) = N(a)N(b)$. Now note that nothing has norm 2. $a^2 + 5b^2$ can never be 2 for integers a, b in $\mathbb{Z}$. So we must have, without loss of generality, $N(a) = 4, N(b) = 1$. So b must be a unit. Similarly, we see that $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible (since there is also no element of norm 3).

We have four irreducible elements in this ring. We claim that they are not prime. Note that

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3.$$

We now claim 2 does not divide $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$. So 2 is not prime.

To show this, suppose $2 \mid 1 + \sqrt{-5}$. Then $N(2) \mid N(1 + \sqrt{-5})$. But $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$, and $4 \nmid 6$. Similarly, $N(1 - \sqrt{-5}) = 6$ as well. So $2 \nmid 1 + \sqrt{-5}$.

There are several things to be learnt here. First is that primes and irreducibles are not the same thing in general. The second is that factorisation into irreducibles is not necessarily unique, since $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two factorisations into irreducibles.

However, there is one situation when unique factorisations holds. This is when we have a Euclidean algorithm available.

Definition 1.113. Let R be a UFD. Two elements x and y are **similar** if there exists a unit $u \in R^{\times}$ such that $x = uy$.

Proposition 1.114. Being similar defines an equivalence relation on the set of all irreducible elements of R.

Definition 1.115. Pick one element from each equivalence class, and name it the **distinguished** irreducible element.

Proposition 1.116. We can factorise every non-zero element $x \in R$ as

$$x = uy_1y_2 \cdots y_n$$

where u is a unit and y_i are distinguished irreducible elements. This factorisation is unique up to reordering of the factors.

Proposition 1.117. Another way of representing $x \in R$ as a product

$$x = u \prod_y y^{e(y)}$$

ranging over all distinguished irreducible elements of R where u is a unit and $e(y) \geq 0$ is an integer for each distinguished irreducible element y. All but finitely many of the integers $e(y)$ are zero, so that the product is one of finitely many factors.

Definition 1.118. Let R be a UFD. Given two non-zero elements $x_1, x_2 \in R$ with factorisation

$$x_1 = u_1 \prod_y y^{e_1(y)} \quad \text{and} x_2 = u_2 \prod_y y^{e_2(y)}$$

we define

$$\gcd(x_1, x_2) = \prod_y y^{\min\{e_1(y), e_2(y)\}} \quad \text{and} \quad \operatorname{lcm}(x_1, x_2) = \prod_y y^{\max\{e_1(y), e_2(y)\}}$$

disregarding the units u_1 and u_2.

Proposition 1.119. The gcd and lcm depend on the choice of distinguished irreducible elements. However, any choice of these lead to similar elements.

> **Note 1.120.** We can think of gcd and lcm as elements of R which are well-defined up to a unit factor.

1.4.5 Fraction field

Definition 1.121. Let R be an integral domain. Let N be the subset of $R \times R$ such that the second entry is non-zero. Define the following equivalence relation $\sim$ on N:

$$(a, b) \sim (c, d) \iff ad = bc.$$

Proof. We prove the axioms for $\sim$ to be an equivalence relation.

- Suppose that $(a, b) \in \mathbb{N}$. Then
$$a \cdot b = a \cdot b$$
so that $(a, b) \sim (a, b)$. Hence, $\sim$ is reflexive.

- Now suppose that $(a, b), (c, d) \in \mathbb{N}$ and that $(a, b) \sim (c, d)$. Then
$$ad = bc. \quad \text{But then } cb = da, \text{ as } R \text{ is commutative, and so } (c, d) = (a, b).$$
Hence, $\sim$ is symmetric.

- Finally, suppose that $(a, b), (c, d)$ and $(e, f) \in R$ and that $(a, b) \sim (c, d), (c, d) \sim (e, f)$. Then $ad = bc$ and $cf = de$. Then
$$\begin{aligned}(af)d &= (ad)f \\ &= (bc)f \\ &= b(cf) \\ &= (be)d.\end{aligned}$$
As $(c, d) \in \mathbb{N}$, we have $d \neq 0$. Cancelling d, we get $af = be$. Thus, $(a, b) \sim (e, f)$. Hence, $\sim$ is transitive.

□

Definition 1.122. The **fraction field** of R, denoted K is the set of equivalence classes, under the equivalence relation defined above.

Definition 1.123. We denote the equivalence class of the pairs (a, b) by $\frac{a}{b}$. Elements of K are all equivalence classes
$$K = \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\}.$$
Set
$$0_K = \frac{0}{1} \quad \text{and} \quad 1_K = \frac{1}{1}$$
and define an addition and multiplication by
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$
for all $\frac{a}{b}, \frac{c}{d} \in K$.

Note 1.124. The equivalence class of (a, b) is $[a, b] = \frac{a}{b}$.

Proposition 1.125

The fraction field of R, which we denote K, is a field. Moreover, the map
$$\begin{aligned}\phi : R &\to K \\ x &\mapsto \frac{x}{1}\end{aligned}$$
is an injective ring homomorphism.

Note 1.126. This is map is an inclusion i.e. $\phi : R \hookrightarrow K$.

1.4.6 Chain of implication

We have now completed the first major goal of this course, namely to establish the following chain of implications:

$$(\mathbb{Z}) \Rightarrow \text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD} \Rightarrow \text{ID} \Rightarrow \text{Commutative Ring} \Rightarrow \text{Ring}$$

where $(\mathbb{Z})$ just denotes the property of being isomorphic to $\mathbb{Z}$. For each ring R, we can classify how similar it is to $\mathbb{Z}$ by seeing how many properties it satisfies, i.e. how far left it sits in the chain of implications. To show that these all make sense as separate definitions, we also need to find examples showing that each implication cannot be reversed:

$$(\mathbb{Z}) \underbrace{\not\Leftarrow}_{\mathbb{Q},\mathbb{Z}[i]} \text{ED} \quad \underbrace{\not\Leftarrow}_{\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]} \quad \text{PID} \underbrace{\not\Leftarrow}_{\mathbb{Z}[X]} \text{UFD} \quad \underbrace{\not\Leftarrow}_{\mathbb{Z}[\sqrt{-5}]} \quad \text{ID} \underbrace{\not\Leftarrow}_{\mathbb{Z}/6\mathbb{Z}} \text{Commutative Ring} \underbrace{\not\Leftarrow}_{M_2(\mathbb{Z})} \text{Ring.}$$

1.4.7 Factorisation in polynomial rings

Proposition 1.127. Let R be an integral domain, let $f \in R[X]$ be a non-zero polynomial, and let $a_1, \dots, a_n \in R$ be distinct elements such that

$$f(a_1) = f(a_2) = \cdots = f(a_n) = 0.$$

Then $\deg(f) \geq n$.

Proof. Let K denote the fraction field of R and identify $R[X]$ with a subring of $K[X]$. Using long division in the euclidean ring $K[X]$ we may write $f \in K[X]$ as

$$f(X) = g(X)(X - a_i) + r_i$$

for some $r_i \in K$. Evaluating at a_i yields $0 = r_i$, hence $(X - a_i)$ divides f in the ring $K[X]$ for $i = 1, 2, \dots, n$. The polynomials $(X - a_1), \dots, (X - a_n)$ are irreducible and pairwise coprime, hence their product $g(X) = (X - a_1) \cdots (X - a_n)$ divides f, hence $\deg(f) \geq \deg(g) = n$ as claimed. □

Corollary 1.128

Let R be an integral domain. Every finite subgroup of $R^\times$ is cyclic.

Proof. Let $G \subseteq R^\times$ be a finite subgroup, and let $e \geq 0$ be the smallest integer such that $g^e = 1$ for all $g \in G$. We need to show that $e = |G|$. Consider the polynomial $X^e - 1 \in R[X]$, every element of G is a roof of this polynomial thus, $e \geq |G|$ which implies e divide $|G|$ hence, $e = |G|$. □

Corollary 1.129

Let p be a prime number. The finite field with p elements $\mathbb{F}_p$ contains an element x with $x^2 = -1$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. We prove by case.

- For $p = 2$ we have $1^2 = 1 = -1$ in $\mathbb{F}_2$.
- We may assume $p \geq 3$ is an odd prime number. By the corollary above the group of units $\mathbb{F}_p^\times$ is cyclic, of order $p - 1$, and since $p \geq 3$ the element $-1 \in \mathbb{F}_p$ is of order 2 – it is the only element of order 2. An element x with $x^2 = -1$ is thus, any element of order 4. Such an element exists if and only if 4 divides $\left|\mathbb{F}_p^\times\right|$ which is the cases if and only if $p \equiv 1 \pmod 4$.

□

Example 1.130

The ring $\mathbb{Z}[i]$ is a Euclidean ring with respect to the norm map

$$\begin{aligned} N &: \mathbb{Z}[i] \to \mathbb{Z} \\ (a + ib) &\mapsto |a + ib|^2 = (a + ib)(a - ib) = a^2 + b^2, \end{aligned}$$

and it has the property $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[i]$. Furthermore, an element of $\mathbb{Z}[i]$ is a unit if and only if its norm is 1 hence, $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Proposition 1.131

Let p be a prime number.

1. If $p = 2$, then $p = (1 + i)(1 - i)$ and the elements $1 \pm i$ are prime in $\mathbb{Z}[i]$.
2. If $p \equiv 3 \pmod 4$, then $p = p + 0i$ is prime $\mathbb{Z}[i]$.
3. If $p \equiv 1 \pmod 4$, then there exists integers $0 \leq a \leq b$ with $p = a^2 + b^2 = (a + ib)(a - ib)$. The elements $a \pm ib$ are prime in $\mathbb{Z}[i]$.

Proof. First we note that any factorisation of an element $x \in \mathbb{Z}[i]$ yields a factorisation of $N(x)$ in $\mathbb{Z}$, so an element of $\mathbb{Z}[i]$ whose norm is a prime number is itself a prime in $\mathbb{Z}[i]$. We prove each statement in turn.

1. In particular $1 \pm i$ are prime since these elements have norm $N(1 \pm i) = 2$.
2. Let $p \geq 3$ be an odd prime. Routine checking shows that there is a well-defined map
$$\begin{gathered} \mathbb{Z}[i]/p\mathbb{Z}[i] \to \mathbb{F}_p[X]/(X^2 + 1) \\ [a + ib] \mapsto [a + bX] \end{gathered}$$
and that this map is an isomorphism of rings. It follows that the element $p \in \mathbb{Z}[i]$ is prime if and only if the element $X^2 + 1 \in \mathbb{F}_p[X]$ is prime, which by the corollary above is the case if and only if $p \equiv 3 \pmod 4$.
3. If $p \equiv 1 \pmod 4$, then p is not irreducible, hence p admits a factorisation $p = xy$ where neither x nor y is a unit. Since $p^2 = N(p) = N(x)N(y)$ and elements of norm 1 are units, we find $N(x) = N(y) = p$, hence x and y are irreducible. Setting $x = a + ib$ we find $p = N(x) = a^2 + b^2 = (a + ib)(a - ib)$ hence, $y = a - ib$.

□

Definition 1.132. Let R be a UFD. The **content** of a non-zero polynomial $f \in R[X]$ is the gcd of its coefficients. We denote the content of f by $\mathrm{c}(f)$, and say that f is primitive if $\mathrm{c}(f) = 1$.

Lemma 1.133. Let R be a UFD. We have

$$\mathrm{c}(fg) = \mathrm{c}(f)\mathrm{c}(g)$$

for all $f, g \in R[X]$.

Proof. Let $f, g \in R[X]$ be non-zero polynomials. We may write $f = c(f)f_0$ and $g = c(g)g_0$ for primitive polynomials f_0 and g_0. The content of fg is then given by

$$c(fg) = c(f)c(g)c(f_0g_0)$$

and hence it is enough to show that $c(f_0g_0) = 1$. In other words, it suffices to show that the product of primitive polynomials is primitive, or else, that if an irreducible element of R divides $c(fg)$, then it divides $c(f)$ or $c(g)$, which is what we will do.

Let $a \in R$ be an irreducible element dividing $c(fg)$. The ideal $I = aR$ of R is prime, hence R/I is an integral domain. The canonical quotient map $R \to R/I$ extends to a surjective ring homomorphism

$$\pi : R[X] \to R/I[X]$$

defined by applying the quotient map to the coefficients of polynomials. The kernel of π is the set of those polynomials whose coefficients all belong to I. Since $R/I[X]$ is an integral domain, the ideal $\ker(\pi)$ in $R[X]$ is prime. To say that a divides $c(fg)$ is to say that $fg \in \ker(\pi)$, hence $f \in \ker(\pi)$ or $g \in \ker(\pi)$. It follows that the irreducible element a divides $c(f)$ or $c(g)$. □

Proposition 1.134 (Gauss' lemma)

Let R be UFD. Let $f \in R[X]$ be a non-constant polynomial, and denote by K the fraction field of R. If f is irreducible in $R[X]$, then f is irreducible in $K[X]$.

Note 1.135. f irreducible implies f is primitive.

Proof. Let $f \in R[X]$ be irreducible of degree ≥ 1. Viewed as a polynomial of degree 0, the content of f divides f. But f is irreducible and nonconstant, so $c(f) = 1$ and hence f must be primitive.

Let $g, h \in K[X]$ be polynomials with $f = gh$. We must show that g or h is constant, hence a unit in $K[X]$. We may write g and h as $g = \frac{1}{a}g_0$ and $h = \frac{1}{b}h_0$ for non-zero elements $a, b \in R$ and primitive polynomials $g_0, h_0 \in R[X]$. The equality $abf = g_0h_0$ in $R[X]$ shows

$$ab = c(abf) = c(g_0h_0) = c(g_0)c(h_0) = 1$$

hence a and b are units in R, and g, h belong to $R[X]$. But f was supposed to be irreducible in $R[X]$, hence either g or h is constant, equal to a unit in R. □

Theorem 1.136

Let R be a Noetherian integral domain. The ring R is a UFD if and only if $R[X]$ is a UFD.

Note 1.137. Peter states: let R be a Noetherian UFD, then $R[X]$ is a UFD.

Proof. We prove each direction in turn.

- Proof of ($\Rightarrow$).

  Suppose that R is a unique factorisation domain, and let us show that $R[X]$ is a unique factorisation domain. As R is Noetherian, so is the ring $R[X]$ by Hilbert's basis theorem. Using Proposition 1.109, it suffices to show that every irreducible element of $R[X]$ is prime. Let $f \in R[X]$ be irreducible.

  If f is constant, then f is prime in R and R/fR is an integral domain. But then also $(R/fR)[X] \cong R[X]/fR[X]$ is an integral domain, hence $fR[X] \subseteq R[X]$ is a prime ideal and f is prime in $R[X]$.

  Suppose now that f is irreducible and not constant, so in particular $c(f) = 1$. Let K denote the fraction field of R. By Gauss' Lemma, the polynomial f is irreducible in $K[X]$, hence $K[X]/fK[X]$ is an integral domain. Let us show that, as subsets of $K[X]$, the inclusion

  $$fR[X] \subseteq R[X] \cap fK[X] \qquad (\star)$$

  is an equality. An element of the right hand side set is a polynomial $g \in R[X]$ which can be written as a product of polynomials fh with $h \in K[X]$. Write $h = \frac{1}{b}h_0$ for some primitive polynomial $h_0 \in R[X]$. We find $bg = fh_0$, hence

  $$bc(g) = c(bg) = c(fh_0) = c(f)c(h_0) = 1$$

  hence b is a unit of R, and thus h belongs to $R[X]$ and $g = fh \in fR[X]$ belongs to the left-hand side of $(\star)$. This shows that $(\star)$ is an equality as claimed. The kernel of the canonical ring homomorphism

  $$R[X] \to K[X]/fK[X]$$

  is $R[X] \cap fK[X]$, hence equal to $fR[X]$. This ring homomorphism induces therefore an injective ring homomorphism from $R[X]/fR[X]$ into the integral domain $K[X]/fK[X]$, so $R[X]/fR[X]$ itself is an integral domain. This shows that $fR[X]$ is a prime ideal of $R[X]$, hence $f \in R[X]$ is prime.

- Proof of ($\Leftarrow$).

  If $R[X]$ is a unique factorisation domain, then every non-zero element of R, when viewed as a constant polynomial, admits an essentially unique factorisation in $R[X]$. All factors in such a factorisation must be constant irreducible polynomials, thus irreducible elements of R. This shows that R is a unique factorisation domain.

□

Theorem 1.138 (Eiseinstein's criterion)
Let $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 1$. Suppose there exists a prime number p such that

- $p \nmid a_n$,
- $p \mid a_0, a_1, \ldots, a_{n-1}$, and
- $p^2 \nmid a_0$.

Then f is irreducible in $\mathbb{Q}[X]$.

Proof. Without loss of generality assume f is primitive. It is then enough, by Gauss' lemma, to show that f is irreducible in $\mathbb{Z}[X]$. Let $g, h \in \mathbb{Z}[X]$ be polynomials with $f = gh$. Denote by $\bar{f}, \bar{g}$ and $\bar{h}$ the reductions of f, g and h modulo p respectively, and note that

$$a_nX^n = \bar{f}(X) = \bar{g}(X)\bar{h}(X)$$

holds. This implies that $\bar{g}(X) = b_rX^r$ and $\bar{h}(X) = c_sX^s$ for some integers $r, s \geq 0$ with $r + s = n$, where b_r and c_s denote the leading coefficients of g and h. Since $b_rc_s = a_n$, these leading coefficients are prime to p. Now examine the constant coefficients a_0, b_0 and c_0 of f, g and h. If $r > 0$ and $s > 0$, then b_0 and c_0 are both divisible by p, hence $a_0 = b_0c_0$ is divisible by p^2 contrary to our hypotheses, so in fact either $r = 0$ or $s = 0$ must hold. But that means that either g or h is constant equal to some non-zero integer, and since f was primitive, this further implies that g or h is a unit 1 or -1, hence f is indeed irreducible in $\mathbb{Z}[X]$. □

Example 1.139
Let

$$f(x) = 2x^7 - 15x^6 + 60x^5 - 18x^4 - 9x^3 + 45x^2 - 3x + 6.$$

Then $f(x)$ is irreducible over $\mathbb{Q}$. We apply Eisenstein with $p = 3$. Then the top coefficient is not divisible by 3, the others are, and the smallest coefficient is not divisible by $9 = 3^2$.

Definition 1.140. Cyclotomic polynomials are polynomials $\Phi_n(X) \in \mathbb{Z}[X]$ defined by $\Phi_1(X) = X - 1$ and inductively by

$$X^n - 1 = \prod_{m|n} \Phi_m(X)$$

where the product runs all over the divisors of n.

Corollary 1.141. Let $p > 0$ be a prime number. The cyclotomic polynomial $\Phi_p(X)$ is irreducible in $\mathbb{Q}[X]$.

Proof. By Gauss' Lemma, it is enough to show that $\Phi_p(X)$ is irreducible in $\mathbb{Z}[X]$. We may as well show that $\Phi_p(X + 1)$ is irreducible, which is what we will do. By definition of the cyclotomic polynomial the equality $(X+1)^p - 1 = X\Phi_p(X+1)$ holds, hence

$$\Phi_p(X+1) = X^{-1}\left(-1 + \sum_{j=0}^{p} \binom{p}{j} X^j\right) = X^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} X^{j-1}$$

by Newton's formula. Eisenstein's Criterion applies to this polynomial, which is therefore irreducible as claimed. □

1.4.8 Local rings

Definition 1.142. A **local ring** is a commutative ring R which is not a field, and which has exactly one maximal ideal.

Definition 1.143. The quotient of R by its unique maximal ideal is then called the **residue field** of R.

Example 1.144

Let k be a field, and denote by $k[[x]]$ the ring of formal power series with coefficient in k in the variable X is a local ring. The maximal ideal is the set of all power series that have a constant term equal to zero, i.e.

$$\langle x \rangle = \{a_1 x + a_2 x^2 + \cdots : a_i \in k\}.$$

2 Modules

2.1 Modules over a ring

Note 2.1. We can think of modules as "vector spaces over a ring". Unfortunately, the theory developed over linear algebra for modules over a field does not work for a general ring.

2.1.1 Definitions

In this section we assume the rings to not be commutative. As such, for each definition there is a "left" and corresponding "right" definition.

Definition 2.2. Let R be a ring. A **left R-module** is a set M with binary operation $+ : M \times M \to M$ and $\cdot : R \times M \to M$, and a given element $0_M \in M$ such that the following holds:

1. $(M, +)$ is an abelian group with identity 0_M;
2. the operation $\cdot : R \times M \to M$ (an action of R on M) denoted by $(x, m) \mapsto xm$ satisfies
   - $(r+s)(m+n) = rm + rn + sm + sn$
   - $r(sm) = (rs)m$

for all $r, s \in R$ and $m, n \in M$, and

3. $1_R \cdot m = m$ for all $m \in M$;
4. $0_R \cdot m = 0_M$ for all $m \in M$.

The map $R \times M \to M$ is called the **module structure** on M (or **left action** of R on M). We can also call it **scalar multiplication**, where we call the elements of R "scalars".

Remark 2.3. The first condition of the module structure is equivalent to the conditions:

- $(r+s)m = rm + sm$ and
- $r(m+n) = rm + sn$

for all $r, s \in R$ and $m \in M$.

Remark 2.4. Recall, for an abelian group A, the set

$$\mathrm{End}(A) = \{f : A \to A : f \text{ is a group homomorphism}\}$$

is the endomorphism ring of A with operations $(f+g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(g(x))$. An equivalent definition of an R-module is an abelian group M equipped with a ring homomorphism $\phi : R \to \mathrm{End}(M)$. Given $r \in R$ and $m \in M$, we write $r \cdot m$ to denote $\phi(r)(m)$.

Remark 2.5. The symbol $+$ is just that, a symbol. It does not mean addition!

Proposition 2.6

Let M be an R-module then, we have that

$$(-1)_R \cdot m = -m$$

for all $m \in M$.

Example 2.7

When R is a field then an R-module is precisely a vector space over R.

Definition 2.8. Let R be a ring and let M and N be left R-modules.

1. A map $f : M \to N$ is a **module homomorphism** (or **R-linear map**) if
   - $f(m_1 + m_2) = f(m_1) + f(m_2)$ for all $m_1, m_2 \in M$, and
   - $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$.
2. A module homomorphism, f, is an **isomorphism** (of modules) if f^{-1} is also a module homomorphism.

3. A module homomorphism $f : M \to M$ is a **module endomorphism**.
4. An **automorphism** is an isomorphic module endomorphism.

Note 2.9. We can combine the two conditions of a module homomorphism into

$$f(rm_1 + sm_2) = rf(m_1) + sf(m_2)$$

for all $r, s \in R$ and $m_1, m_2 \in M$.

Remark 2.10. We use this characterisation of the definition of a module isomorphism because (pedantically) if f is a bijective module homomorphism then, its inverse is not necessarily a module homomorphism.

Definition 2.11. Let $\alpha : R \to S$ be a ring homomorphism, and let M be an S-module. We can regard M as an R-module using the left action of R on M defined by

$$(r, m) \mapsto \alpha(r)m$$

for all $r \in R$ and $m \in M$. We refer to this R-module as the R-module obtained from the S-module M, or also to by **restriction of scalars**.

Definition 2.12. Let R be a ring, and let $f : M \to N$ and $g : M \to N$ be a homomorphism of R-modules. Define the **sum homomorphism** by

$$\begin{aligned} f + g : M &\to N \\ m &\mapsto f(m) + g(m) \end{aligned}$$

Definition 2.13. We denote by $\mathrm{Hom}_R(M, N)$ the set of all homomorphisms of R-modules from M to N.

Theorem 2.14. The set $\mathrm{Hom}_R(M, N)$ is a commutative group with respect to addition of homomorphisms, the identity element being the **zero homomorphism** $0 : M \to N$ with $0_M \mapsto 0_N$.

Definition 2.15. Let R be a commutative ring. For every $x \in R$ and every R-module homomorphism $f : M \to N$, define the **scalar multiplication** map

$$\begin{aligned} xf : M &\to N \\ m &\mapsto xf(m). \end{aligned}$$

Theorem 2.16. The scalar multiplication defined above gives $\mathrm{Hom}_R(M, N)$ the structure of an R-module.

Theorem 2.17

Let R be a commutative ring, and let M be an R-module. The map

$$\begin{aligned} \varepsilon_M : M &\to \mathrm{Hom}_R(\mathrm{Hom}_R(M, R), R) \\ \varepsilon_M(m)(f) &\mapsto f(m) \end{aligned}$$

for $m \in M$ and $f \in \mathrm{Hom}_R(M, R)$ is a module homomorphism.

> **Remark 2.18.** This map is an isomorphism when R is a field and when M is a finite dimensional vector space.

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

- An element $m \in M$ is called a **torsion element** if there exists a non-zero element $x \in R$ such that $xm = 0$.
- We say that M is a **torsion module** if ALL of its elements are torsion elements.
- We say that M is **torsion free** if it contains NO torsion elements except 0.

Definition 2.20. Let R be a ring, let M be an R-module and let S be a subset of M. The **annihilator** of S is the ideal of R:

$$\mathrm{Ann}_R(S) = \{r \in R : rm = 0 \;\; \forall m \in S\}.$$

Theorem 2.21. A commutative ring R is an integral domain if and only if R (viewed as an R-module) is torsion free.

Theorem 2.22

An element $m \in M$ of an R-module M is torsion if and only if the annihilator ideal $\mathrm{Ann}_R(\{m\})$ is non-trivial.

2.1.2 Examples

Example 2.23 ($\mathbb{Z}$-modules)

Let $R = \mathbb{Z}$ and let M be *any* abelian group (finite or infinite) and write the operation of M as $+$. We make M as a $\mathbb{Z}$-module as follows: for any $x \in \mathbb{Z}$ and $m \in M$ define

$$xm = \begin{cases} m + \cdots + m \text{ } (x \text{ times}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -m - \cdots - m \text{ } (-x \text{ times}) & \text{if } n < 0 \end{cases}$$

(where 0 is the identity of group M). Therefore, we can conclude

$\mathbb{Z}$-modules are the same as abelian groups.

2.1.3 Sums and products of modules

Definition 2.24. Let R be a ring, let M and N be R-modules. The **direct sum**, is the R-module

$$M \oplus N = \{(m, n) : m \in M, n \in N\}$$

where the addition and scalar multiplication is done component wise. That is,

$$\begin{aligned} \text{Addition:} \quad & (m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2) \quad \text{and} \\ \text{Scalar multiplication:} \quad & r(m, n) = (rm, rn) \end{aligned}$$

for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r \in R$ If the direct sum is finite this is the same as the **product**, $M \times N$.

Remark 2.25. The definition above is a for a finite amount of modules.

Example 2.26

The ring $R^N = \underbrace{R \oplus R \oplus \cdots \oplus R}_{N \text{ times}}$.

Proposition 2.27. The sum of modules is a torsion module if and only if the modules are individually torsion modules.

Definition 2.28. Let R be a ring and let $(M_i)_{i \in I}$ be a family of R-modules. The **product** of this family is the R-module

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i \ \ \forall i \in I\}$$

whose elements are tuples $(m_i)_{i \in I}$ with $m_i \in M_i$. Addition and scalar multiplication is defined component wise.

Note 2.29. By tuple we mean $(m_1, m_2, \cdots)$.

Remark 2.30. If the family of R-modules I is finite the product is equal to the (finite) direct sum.

Definition 2.31. Let R be a ring and let $(M_i)_{i \in I}$ be a family of R-modules. The **direct sum** of this family is the R-module

$$\bigoplus_{i \in I} M_i = \left\{ (m_i)_{i \in I} \in \prod_{i \in I} M_i : m_i = 0 \text{ for all but finitely many } i \in I \right\} \subseteq \prod_{i \in I} M_i$$

whose elements are tuples $(m_i)_{i \in I}$ with $m_i \in M_i$. Addition and scalar multiplication is defined component wise.

Note 2.32. By the phrase "$m_i = 0$ for all but finitely many $i \in I$" we mean that each element of the direct sum is a tuple where almost all the components are zero – only a finite number of them can be non-zero.

Example 2.33. Let $R = \mathbb{Z}, I = \mathbb{N}$ and $M_i = \mathbb{Z}/6\mathbb{Z}$. The direct sum and product are

$$\bigoplus_{i=1}^{\infty} M_i = \{\text{sequences which eventually go to zero where the elements are from } \mathbb{Z}/6\mathbb{Z}\} \subseteq$$

$$\prod_{i=1}^{\infty} M_i = \{(m_i)_{i=1}^{\infty} : m_i \in \mathbb{Z}/6\mathbb{Z}\}.$$

2.1.4 Free modules

Definition 2.34. Let R be a ring, and let S be a set. The **free module** generated by S is the set of all formal sums

$$\sum_{s\in S} x_s s$$

where only finitely many of the coefficients $x_s \in R$ are non-zero. We denote this module by $R^{\oplus S}$.

> **Note 2.35.** By formal sum we mean a symbolic expression representing the addition of objects, like variables or vectors, focusing on their abstract properties rather than their numerical values.

Definition 2.36. Let R be a ring, and M be an R-module. We say M is **free** if it admits a basis.

Definition 2.37. We say that an R-module is free if it is isomorphic to the free module generated by some set.

Definition 2.38. Let R be a ring, and M be an R-module. To say that M is free is to say that there exists a set S and an isomorphism of R-modules $f : R^{\oplus S} \to M$. For every $s \in S$, let us denote by $e_s \in M$ the element $f(s)$, where s is the formal sum $1_R s$ with just one term. Since f is an isomorphism, every element $m \in M$ can be written as an R-linear combination

$$m = \sum_{s\in S} x_s e_s$$

with uniquely determined scalars $x_s \in R$, all but finitely many zero. We say that the set $\{e_s : s \in S\}$ is a **basis** of the free R-module M.

> **Note 2.39.** We can think of M being isomorphic to a finite amount of copies of R i.e. $M \cong R^{\oplus S} \cong R \oplus \cdots \oplus R$.

2.1.5 Submodules

> **Remark 2.40.** In this section, we assume all modules are left modules. However, the following definitions can be tweaked to use right modules.

Definition 2.41. Let M be an R-module. A **submodule** of M is a subset $N \subseteq M$ such that the element $r_1n_1 + r_2n_2 \in M$ also belongs to N for all $n_1, n_2 \in N$ and all $r_1, r_2 \in R$.

> **Remark 2.42.** An equivalent definition of an R-submodule.
> Let M be an R-module. A subset $N \subseteq M$ is an R-submodule
>
> - if it is a subgroup of $(M, +, 0_M)$,
> - if $n \in N$ and $r \in R$ then, $rn \in N$.

Example 2.43

Some examples of submodules.

- A subset of a ring R is a submodule if and only if it is an ideal.
- Let $f : M \to N$ be a homomorphism of R-moduels. The image of f is a submodule of N.
- A subset of a K-module V, where K is a field, is a K-submodule if and only if it is a vector subspace of V.

Definition 2.44. Let M be an R-module, and let $S \subseteq M$ be a subset. The **submodule** of M **generated** by S is the set of all sums

$$r_1 s_1 + \cdots + r_k s_k$$

with $r_1, \ldots, r_k \in R$ and $s_1, \ldots, s_k \in S$. We denote it by $\langle S \rangle \subseteq M$.

Definition 2.45. If $\langle S \rangle = M$ then we say that S generated M. We say that M is a **finitely generated module** if there exists a finite subset $S \subseteq R$ which generates M.

Proposition 2.46. If R is a field, then $\langle S \rangle$ is called the linear span of S, and M is finitely generated if and only if M is a finite dimensional vector space.

2.1.6 Quotient modules

> **Remark 2.47.** In this section, we assume all modules are left modules. However, the following definitions can be tweaked to use right modules.

Definition 2.48. Let $N \subseteq M$ be an R-submodule. The **quotient module** M/N is the set of N-cosets in the group $(M, +, 0_M)$ with the R-module structure defined by

$$(r, [m]) \mapsto [rm]$$

for all $r \in R$ and $m \in M$, where $[m]$ denotes the equivalence class of m in M/N.

> **Remark 2.49.** Note that modules are different from rings and groups. In groups, we had subgroups, and we have some really nice ones called normal subgroups. We are only allowed to quotient by normal subgroups. In rings, we have subrings and ideals, which are unrelated objects, and we only quotient by ideals. In modules, we only have submodules, and we can quotient by arbitrary submodules.

Proposition 2.50

Let R be a commutative ring, let $I \subseteq R$ be an ideal and let M be a free R-module. We have that M/IM is a free R/I-module.

2.1.7 Basic theory of modules

Definition 2.51. Let $f : M \to N$ be an R-module homomorphism. Then

$$\ker(f) = \{m \in M : f(m) = 0\} \subseteq M$$

is an R-submodule of M. Similarly,

$$\operatorname{Im}(f) = \{f(m) : m \in M\} \subseteq N$$

is an R-submodule of N.

Theorem 2.52 (Isomorphism theorem)
Let $f : M \to N$ be an R-module homomorphism. Then

$$\frac{M}{\ker(f)} \cong \operatorname{Im}(f).$$

Note that, unlike the situation for rings, the fact that $\operatorname{im} f \subseteq N$ is a submodule means that one further module $N/\operatorname{Im} f$ arises for an R-module homomorphism $f : M \to N$. This leads to a new concept:

Definition 2.53. Let R be a ring and let M_1 and M_2 be submodules of an R-module M. The **sum** $M_1 + M_2$ is the submodule of M whose elements are all sums $m_1 + m_2$ with $m_1 \in M_1$ and $m_2 \in M_2$.

Theorem 2.54
Let M be an R-module. We have that M is finitely generated if and only if M is a quotient of R^n for some integer $n \geq 0$.

Note 2.55. The language "X is a quotient of Y" means there is a canonical (obvious) surjective homomorphism $\alpha : X \to Y$.

Proof. We prove each direction in turn.

- Proof of ($\Rightarrow$).
  Suppose M is finitely generated by the set $\{m_1, \dots, m_n\}$ then the homomorphism

  $$\begin{aligned} R^n &\to M \\ e_i &\mapsto m_i \end{aligned}$$

  is a surjective map. Here the e_i are a canonical basis of R^n.

- Proof of ($\Leftarrow$).
  Given a surjective module homomorphism $f : R^n \to M$ we have that $f(e_1), \dots, f(e_n)$ generate M where $e_1, \dots, e_n$ are the canonical basis of R^n.

□

Example 2.56

The sum $M_1 + M_2$ is the submodule of M generated by $M_1 \cup M_2$. In the case where M_1 and M_2 are ideals of R, we recover the sum of ideals as defined in the "Ideal arithmetic" section.

There is a close relation between the direct sum of two R-modules and the sum of two submodules of a given R-module. Let M_1 and M_2 be submodules of an R-module M. There is a canonical R-linear map

$$\alpha : M_1 \oplus M_2 \to M$$

sending (m_1, m_2) to $m_1 + m_2$. This is map neither surjective nor injective in general. Its image is M_1+M_2, and its kernel is the submodule of all pairs $(m, -m)$ with $m \in M_1 \cap M_2$. If α is an isomorphism, that is to say if $M_1 + M_2 = M$ and $M_1 \cap M_2 = \{0\}$, then we may with a slight abuse of notation write $M = M_1 \oplus M_2$ and say that M is the direct sum of M_1 and M_2. We also say in that situation that M_2 is a **complement** of M_1 in M.

2.1.8 Exact sequences

Definition 2.57. Let $n \geq 2$ be an integer and let

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \cdots \xrightarrow{f_n} M_{n+1}$$

be morphism of R-modules. We say that the sequence above is **exact** if

$$\operatorname{Im}(f_i) = \ker(f_{i+1})$$

holds for all $1 \leq i \leq n$.

> **Remark 2.58.** In an exact sequence the composition of two successive maps is the zero morpshim.

Definition 2.59. An exact sequence of the form

$$0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$$

is called a **short exact sequence**. To say that the sequence above is short exact amounts to saying that

- $\operatorname{Im}(f_1) = \ker(f_2)$ (because $\ker(f_1) = \{0\}$);
- f_2 is surjective (because $\operatorname{Im}(f_1) = \ker f_2$).

Corollary 2.60

In a short exact sequence we have the following isomorphisms

- $M_1 \cong \operatorname{Im}(f_1) = \ker(f_2)$ and,
- $M_3 \cong M_2/\operatorname{Im}(f_1) \cong M_2/\ker(f_2)$.

Example 2.61

Some examples of short exact sequences.

- $0 \to 3\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \to 0$.
- $0 \to M \to M \oplus N \to N \to 0$ with
$$\begin{aligned} M &\to M \oplus N \\ m &\mapsto (m, 0) \end{aligned}$$
and
$$\begin{aligned} M \oplus N &\to N \\ (m, n) &\mapsto n. \end{aligned}$$
- Let M be an R-module and let N_1, N_2 be submodules Set
$$\begin{aligned} N_1 + N_2 &= \{n_1 + n_2 \in N \mid n_1 \in N_1, n_2 \in N_2\} \\ N_1 \oplus N_2 &= \{(n_1, n_2) \in N \times N \mid n_1 \in N_1, n_2 \in N_2\} \end{aligned}$$
The map
$$\begin{aligned} N_1 \oplus N_2 &\to N_1 + N_2 \\ (n_1, n_2) &\mapsto n_1 + n_2 \end{aligned}$$
is a surjective module homomorphism. We have the following short exact sequence
$$0 \to N_1 \cap N_2 \to N_1 \oplus N_2 \to N_1 + N_2 \to 0$$
where
$$\begin{aligned} N_1 \cap N_2 &\to N_1 \oplus N_2 \\ n &\mapsto (n, -n). \end{aligned}$$
If $s(n_1, n_2) = 0$ then $n_1 = -n_2 \in N_1 \cap N_2$

Proposition 2.62

Let R be a commutative ring and let
$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$
be a short exact sequence of modules. We have that if L and N are

1. torsion then M is torsion;
2. finitely generated then M is finitely generated;
3. free then M is free;
4. torsion free then M is torsion free.

Proof. We prove each statement in turn.

1. Let $m \in M$. We have to find $r \in R$ such that $rm = 0$ for $r \neq 0$. Since N is torsion there exists $s \in R$ such that $sg(m) = g(sm) = 0$. Therefore, there exists $\ell \in L$

such that $f(\ell) = sm$ and, since L is torsion there exist $t \in R$ such that $tl = 0$. We have $0 = f(0) = f(tl) = tf(\ell) = tsm$ hence, $r = ts$.

2. Let $\{\ell_1, \dots, \ell_i\}$ be a generating set for L and let $\{n_1, \dots, n_j\}$ be a generating set for N. Let $m_1, \dots, m_j \in M$ be elements such that

$$g(m_k) = n_k \quad \text{for } k = 1, \dots, j.$$

We claim $\{f(\ell_1), \dots, f(\ell_i), m_1, \dots, m_j\}$ generates M.
Let $m \in M$ then we have

$$g(m) = a_1 n_1 + \cdots a_j n_j$$

and so,

$$f(\ell) = m - (a_1 n_1 + \cdots a_j n_j) \in \ker(g) = \operatorname{Im}(f).$$

We can write

$$\ell = b_1 \ell_1 + \cdots b_i \ell_i$$

hence,

$$b_1 f(\ell_1) + \cdots + b_i f(\ell_i) = m - (a_1 n_1 + \cdots a_j n_j).$$

3. Idem of (2) but instead of using a generating set use a basis.

4. We want to show that for a given $m \neq 0$ and $rm = 0$ implies $r = 0$ for $r \in R$.
Let non-zero $m \in M_1$ and let $r \in R$ such that $rm = 0$. We have $rg(m) = g(rm) = g(0) = 0$ thus,

- if $g(m) \neq 0$ then $r = 0$.
- On the other hand, if $g(m) = 0$ then $m = f(\ell)$ for some $\ell \in L$. We have $0 = rm = rf(\ell) = f(r\ell)$ hence, $rl = 0$. Since $\ell \neq 0$ we find $r = 0$.

□

Proposition 2.63. Let R be a commutative ring, and let $m, n \geq 0$ be integers. If there exists an isomorphism of R-modules $R^m \to R^n$, then $m = n$.

Proof. The statement is well known in the case where R is a field. To deduce the general case from this, choose a maximal ideal $I \subseteq R$, and set $K = R/I$. Any R-linear map $\varphi : M \to N$ between R-modules induces a K-linear map $\widetilde{\varphi} : M/IM \to N/IN$ between vector spaces over K, and if φ is an isomorphism, then so is $\widetilde{\varphi}$. In particular, since $R^n/IR^n \cong (R/I)^n = K^n$, any isomorphism $R^n \to R^n$ induces an isomorphism $K^m \to K^n$, from which $m = n$ follows. □

2.2 Structure of modules

2.2.1 Vector spaces

Theorem 2.64

A commutative ring R is a field if and only if every R-module is free.

Proof. We prove each direction in turn.

- Proof of ($\Rightarrow$).
  Assume every R-module is free and let a non-zero $x \in R$. Set $I = \langle x \rangle = xR$. The quotient R/I is not the trivial module, and it is free by assumption thus, R/I admits a non-empty basis. Let $[y] \in R/I$ be an element of a basis of R/I then, $x[y] = [xy] = 0$ which contradict the assumption that $[y]$ belongs to a basis. Therefore, $\varnothing$ is the basis for R/I which implies $R/I = \{0\}$ hence, $I = R$ and x is a unit.

- Proof of ($\Leftarrow$).
  First, we recall some terminology linear algebra. Let K be a field, and let V be a vector space over K. The subset $E \subseteq V$ is *linearly independent* if the relation

  $$\sum_{i=1}^{n} x_i e_i \Rightarrow x_1 = \cdots = x_n = 0 \quad \text{for } x_i \in K \text{ and } e_i \in S.$$

  In particular the empty set is linearly independent.
  Suppose $R = K$ is field and let V be a K-vector space. To show that V admits a basis we consider the family of all linearly independent subsets of V ordered by inclusion, denote this family by $\mathcal{F}$. We have $\varnothing \in \mathcal{F}$ and so, it is non-empty. If $F_1 \subseteq F_2 \subseteq \cdots$ is a chain in $\mathcal{F}$ then $\bigcup_{i=1}^{\infty} F_i$ is an upper bound. By Zorn's lemma, $\mathcal{F}$ contains a maximal element, say B. We claim that B is a basis of V. By assumption B is linearly independent so, we need to show that B generates V. For the sake of contradiction, suppose it does not. Then there exists an element $v \in V$ which is not contained in $\langle B \rangle$. But, the set $B \cup \{v\}$ is also linearly independent hence, B is not the maximal element.

□

2.2.2 Modules over a Noetherian ring

Theorem 2.65

A commutative ring R is Noetherian if and only if all submodules of finitely generated R-modules are finitely generated.

Proof. First, we prove this statement in the case where the R-module $M = R^n$ for some $n \geq 0$ by induction on n. For $n = 0$ there is nothing to prove, so we assume that $n \geq 1$ and that every submodule of R^k for $k = 1, 2, \ldots, n-1$ is finitely generated. Let $N \subseteq R^n$ be a submodule and let

$$\pi : R^n \to R$$
$$\pi \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto x_n$$

denote the projection onto the last coordinate. We have

$$\ker(\pi) = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{n_1} \\ 0 \end{pmatrix} : x_1, \ldots, x_{n-1} \in R \right\} = R^{n-1}.$$

Consider the short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & N \cap R^{n-1} \arrow[r, "\subseteq"] \arrow[d, "\subseteq"'] & N \arrow[r, "\pi"] \arrow[d, "\subseteq"] & \pi(N) \arrow[r] \arrow[d, "\subseteq"'] & 0 \\
0 \arrow[r] & R^{n-1} \arrow[r, "\subseteq"] & R^n \arrow[r, "\pi"] & R \arrow[r] & 0
\end{tikzcd}$$

By induction $N \cap R^{n-1}$ and $\pi(R)$ are finitely generated hence, N is finitely generated by Proposition 2.62.

For the general case, P be any finitely generated R-module, and let $Q \subseteq P$ be a submodule. Let $p_1, \ldots, p_n$ be generators of P. The module homomorphism

$$p : R^n \to P$$
$$p(x_1, \ldots, x_n) = x_1p_1 + \cdots x_np_n$$

is surjective. By the previous case we considered we know $p^{-1}(Q) \subseteq R^n$ is finitely generated, say by $q_1, \ldots, q_k \in p^{-1}(Q)$. Hence, $Q = p\left(p^{-1}(Q)\right)$ is generated by $p(q_1), \ldots, p(q_n)$. □

Definition 2.66. Let $f : M \to N$ be an R-module homomorphism. The **cokernel** of f, is

$$\operatorname{coker}(f) = N/\operatorname{Im}(f).$$

Corollary 2.67

Let M be a finitely generated module over a commutative Noetherian ring R. There exists integers $r, s \geq 0$ and a morphims of R-modules $f : R^r \to R^s$ such that

$$M \cong R^s/\operatorname{Im}(f) \cong \operatorname{coker}(f).$$

Proof. The module M being finitely generated, there exist generators $m_1, \ldots, m_s$ of M. These generators allow us to define the surjective morphism

$$g : R^s \to M$$
$$e_i \mapsto m_i$$

where $e_1, \ldots, e_s$ is the canonical basis of R^s. By the theorem above the kernel of g is a finitely generated submodule of R^s, so it admits a finite set of generators, say $n_1, \ldots, n_r$, for this we define a morphism $f : R^r \to R^s$ whose image is $\ker(g)$. In summary, the sequence of R-modules

$$0 \to R^r \xrightarrow{f} R^s \xrightarrow{g} M \to 0$$

is exact, which means that the map g induces an isomorphism $\operatorname{coker}(f) \cong M$. □

Note 2.68. The corollary above provides us a way to concretely present every finitely generated module over a Noetherian ring. Homomorphisms $f : R^m \to R^n$ are in bijection with $n \times m$-matrices with coefficients in R, say A. The coefficients a_{ij} of the matrix A corresponding to f are characterised by

$$f(e_i) = \sum_{j=1}^{n} a_{ij}e_j \quad \text{for } 1 \leq i \leq m,$$

where e_i stand for the canonical basis vectors in either of the free modules R^m or R^n. We write $\operatorname{coker}(A)$ instead of $\operatorname{coker}(f) = \operatorname{coker}(A)$.

Proposition 2.69

If $f : R^m \to R^n$ is given by the matrix $A \in M_{n\times m}(R)$ i.e. $f(x) = Ax$ for all $x \in R^m$ then we write, $\operatorname{coker}(f) = \operatorname{coker}(A)$. Furthermore, we have

$$\operatorname{Im}(f) = \langle \text{columns of } A \rangle$$

i.e. the image of f is equal to the submodule generated by the columns of A.

Proposition 2.70

Some properties of the cokernel.

1. If $f : R^m \to R^n$ is surjective then $\operatorname{coker}(f) = 0$ so, whenever the columns of a matrix A of size $n \times m$ generate R^n then $\operatorname{coker}(A) = 0$.

2. $\operatorname{coker}(A) = 0$ when A is an invertible matrix.

3. Let
$$\begin{tikzcd} R^n \arrow[r, "g"] \arrow[d, "u"'] & R^s \arrow[r] \arrow[d, "v"] & \operatorname{coker}(g) \arrow[r] \arrow[d, dashed] & 0 \\ R^n \arrow[r, "f"] & R^s \arrow[r] & \operatorname{coker}(f) \arrow[r] & 0 \end{tikzcd}$$
be a commutative diagram of R-modules. If u and v are isomorphism then v induces and isomorphism
$$\operatorname{coker}(f) = \operatorname{coker}(vgu^{-1}) = \operatorname{coker}(g).$$
In terms of matrices: for any matrix A of size $n \times m$ and, invertible matrices U and V of size $m \times m$ and $n \times n$ respectively there exsist an isomorphism
$$\operatorname{coker}(UAV^{-1}) = \operatorname{coker}(A)$$
of R-modules.

4. For any morpshims $f : R^{m_1} \to R^{n_1}$ and $g : R^{m_2} \to R^{n_2}$ there is a canonical isomorphism
$$\operatorname{coker}(f \oplus g) \cong \operatorname{coker}(f) \oplus \operatorname{coker}(g)$$
where
$$\begin{aligned} f \oplus g : R^{m_1} \oplus R^{m_2} &\to R^{n_1} \oplus R^{n_2} \\ (x, y) &\mapsto (f(x), g(y)). \end{aligned}$$
In terms of matrices,
$$\operatorname{coker}\begin{pmatrix} F & 0 \\ 0 & G \end{pmatrix} \cong \operatorname{coker}(F) \oplus \operatorname{coker}(G)$$
for any two matrices F and G. The block matrix on the left is often written as $F \oplus G$ and called the **direct sum** of F and G.

5. In the above, if $F \oplus G$ is in block shape such that G is an invertible matrix then A and F represent isomorphic modules.

Remark 2.71. By $\operatorname{coker}(A) = 0$ we mean that it is equal to the trivial module.

Note 2.72. The third property implies that elementary row and column operation do not affect the cokernel.

Example 2.73

Some examples to illustrate the above.

- Let $R = \mathbb{Z}$ and define the module homomorphism
$$\begin{aligned} \mathbb{Z}^2 &\to \mathbb{Z}^2 \\ x &\mapsto Ax \end{aligned}$$
where $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore, $\operatorname{coker}(A) = 0$ since the matrix is invertible.

- Let $R = \mathbb{Z}$ and define the module homomorphism
$$\begin{aligned} \mathbb{Z}^2 &\to \mathbb{Z}^2 \\ x &\mapsto Ax \end{aligned}$$
where $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Therefore, $\operatorname{coker}(A) = \mathbb{Z}^2 / \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle = \mathbb{Z}^2/\mathbb{Z} = \mathbb{Z}$.

- Let $R = \mathbb{Z}$ and define the module homomorphism
$$\begin{aligned} \mathbb{Z}^2 &\to \mathbb{Z}^2 \\ x &\mapsto Ax \end{aligned}$$
with $A = \begin{pmatrix} -1 & 2 \\ 0 & -3 \end{pmatrix}$. Notice that $A \sim \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} = A'$. Therefore,
$$\begin{aligned} \operatorname{coker}(A) \cong \operatorname{coker}(A') &\cong \operatorname{coker} \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \\ &\cong \operatorname{coker}(1) \oplus \operatorname{coker}(3) \\ &\cong 0 \oplus \mathbb{Z}/3\mathbb{Z} \\ &\cong \mathbb{Z}/3\mathbb{Z} \end{aligned}$$

- Using the previous scenario but with $A = \begin{pmatrix} 2 & 12 \\ 0 & -24 \end{pmatrix}$. First, we notice that $A \sim \begin{pmatrix} 2 & 0 \\ 0 & -24 \end{pmatrix}$. Therefore,
$$\begin{aligned} \operatorname{coker}(A) &\cong \operatorname{coker}(2) \oplus \operatorname{coker}(-24) \\ &\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}. \end{aligned}$$

Example 2.74

Let $R = \mathbb{R}[X]$, let the R-module $M = R^2$. Do

$$\begin{pmatrix} X^2+1 \\ X^3 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} X^2+X \\ X \end{pmatrix}$$

generate the module M?

Solution. Let $A = \begin{pmatrix} X^2+1 & X^2+X \\ X^3 & X \end{pmatrix}$. This amounts to asking if $\operatorname{coker}(A) = 0$. We notice that

$$A \sim \begin{pmatrix} -X^4 - X^3 + X^2 + 1 & 0 \\ 0 & X \end{pmatrix}.$$

Therefore,

$$\operatorname{coker}(A) \cong \mathbb{R}[X]/\langle X^4 + X^3 - X^2 - 1\rangle \oplus \mathbb{R}[X]/\langle X\rangle$$

which is not zero.

Corollary 2.75

Let R be a Noetherian ring, let M be a finitely generated R-module such that and, let A be an $n \times m$ matrix. Then we have

$$R^n/AR^m \cong M.$$

Proof. Suppose M is generated by $m_1, \dots, m_n$ and define the map

$$\begin{aligned} \pi : R^n &\to M \\ e_i &\mapsto m_i. \end{aligned}$$

This map is surjective. Suppose $\ker(\pi)$ is generated by $\ell_1, \dots, \ell_m$ and define the short exact sequence

$$\begin{aligned} 0 \to R_m &\to R_n \to M \to 0 \\ e_i &\mapsto \ell_i. \end{aligned}$$

□

2.2.3 Modules over a PID

Definition 2.76. Let A and B be two matrices with coefficients in R. We say A and B are equivalent and, denote this by $A \sim B$,

- if they are of the same size and,
- if there exists invertible matrices U and V of the appropriate size such that

$$B = UAV^{-1}.$$

> **Remark 2.77.** This is an equivalence relation.

Definition 2.78. We define **elementary row (column)** operations on a matrix.

1. add a multiple of one row (column) to a different row (column).
2. Multiply a row (column) by a unit of R.
3. Rearranging the order of the rows (columns.)

> **Remark 2.79.** Each elementary operation row (column) corresponds to:
>
> 1. multiplying the matrix on the left (right) with a matrix which looks like the identity matrix except for one entry outside the diagonal which may be any element of R;
> 2. multiplying the matrix on the left (right) with a matrix which looks like the identity matrix except for one diagonal entry which may be any unit of R;
> 3. multiplying the matrix on the left (right) with a permutation matrix;

Definition 2.80. A matrix B with coefficients in a PID R is in **Smith normal form**

- if it is diagonal i.e. the entries b_{ij} satisfy $b_{ij} = 0$ for $i \neq j$ and,
- such that the divisibility relations $b_{11} \mid b_{22} \mid b_{33} \mid \cdots$ hold for those diagonal entries.

Theorem 2.81

Every matrix with coefficients in a PID, R, is equivalent to a matrix in Smith normal form.

Proof. Let A be a matrix with coefficients in R of size $m \times n$ with $m \geq 1$ and $n \geq 1$. If A has only one row i.e. $A = \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}$ define

$$\gcd(a_1, \dots, a_n) = b = x_1 a_1 + \cdots + x_n a_n.$$

Then $A \sim \begin{pmatrix} b & 0 & \cdots & 0 \end{pmatrix}$ (since all the other entries are multiples of b we can use elementary operation to reduce the entries to 0).
Suppose the statements holds for matrices of size $(m-1) \times (n-1)$. Let S be the set of ideals $S = \{\langle b_{11} \rangle : B \sim A\}$ and, let $\langle b_{11} \rangle$ be maximal in S where b_{11} is the top left coefficient of the matrix B. We claim that b_{11} divides every coefficient of in the leftmost column and in the top row of B i.e. $b \mid b_{1j}$ and $b \mid b_{i1}$. To show this in the leftmost column, suffices to show that $b_{11} \mid b_{21}$. Set $c = \gcd(b_{11}, b_{21}) = x_1 b_{11} + x_2 b_{21}$ where x_1 and x_2 are coprime. We can write

$$1 = x_1 y_2 - x_2 y_1 = \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}.$$

The matrix B is equivalent to

$$\begin{pmatrix} x_1 & x_2 & 0 & \cdots & 0 \\ y_1 & y_2 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} = \begin{pmatrix} c & * & \cdots & * \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix} \sim A,$$

and it follows from our assumption on the maximality of $b_{11}R$ that b_{11} divides c, hence b_{21}. A similar argument, now performing column operations, shows that b_{11} divides all coefficients of the top row, and our claim is proven. We conclude that A is equivalent to a matrix of the form

$$A \sim B' = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & b'_{22} & \cdots & b'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b'_{m2} & \cdots & b'_{mn} \end{pmatrix}$$

This shows in particular that the statement of the theorem holds when A has only one row or only one column. Arguing by induction, let us from now on assume $n \geq 2$ and $m \geq 2$, and that the statement of the theorem holds for matrices of size $(n-1)\times(m-1)$. We now claim that b_{11} divides all remaining coefficients of B'. Indeed, any of the coefficients b'_{ij} can be moved to the leftmost column of the matrix by an elementary column operation, and we already have shown that b_{11} divides all coefficients in the leftmost column. This shows that A is equivalent to a matrix

$$A \sim \begin{pmatrix} b_{11} & 0 \\ 0 & b_{11}A' \end{pmatrix}$$

where A' is a matrix of size $(m-1)\times(n-1)$. By induction hypothesis, the matrix A' is equivalent to a diagonal matrix in Smith normal form, which implies the same for A. □

Example 2.82 (Algorithm to reduce to SNF)

Case of Euclidean rings: R.
Given A a matrix A with coefficients in R, we have the following algorithm.

1. Is A zero?
   Yes: output A
   No: Go to 2

2. Permute rows and columns so that a_{11} is non-zero and smallest possible.

3. Perform column operations so that row coefficients $a_{12}, a_{13}, \ldots$ is zero or smaller than a_{11}.

   If any of the $a_{12}, a_{13}, \cdots$ is non-zero then go back to 2. If not go to 3.

3' Do (3) with rows

4. Does a_{11} divide all coefficients of A?
   No: say a_{11} fails; add the i-th row to the first row and then go back to 2.

   Yes: set

$$A = \left(\begin{array}{c|c} a_{11} & 0 \\ \hline 0 & a_{11}\cdot A' \end{array}\right)$$

   Then go back to 1 and use A' on A.

Theorem 2.83 (Chinese Remainder Theorem)

Let R be a PID, let $x \in R$ be a non-zero element and, let $x = x_1 x_2 \cdots x_n$ be a factorisation of x into pairwise coprime factors $x_1, x_2, \ldots, x_n$. The map of R-modules

$$\begin{aligned} R/xR &\to \bigoplus_{i=1}^{n} R/x_iR \\ [z] &\mapsto ([z], [z], \ldots, [z]) \end{aligned}$$

is an isomorphism.

Proof. Arguing by induction on n, it is enough to prove the case $n = 2$. Thus, changing notations, we must show that for any two non-zero, coprime elements $x, y \in R$ the map

$$R/xyR \longrightarrow R/xR \oplus R/yR$$

sending the class $[z]$ to the pair of classes $([z], [z])$ is an isomorphism. This amounts to prove that the map $\varphi\colon R \to R/xR \oplus R/yR$ defined by $\varphi(z) = ([z], [z])$ is surjective, and that its kernel is the ideal xyR. Let us choose $a, b \in R$ with $ax + by = 1$. Such elements exist since x and y are coprime.

We start by showing that φ is surjective. Let u and v be any elements of R. We need to find an element $z \in R$ such that $u \equiv z \pmod{x}$ holds and $v \equiv z \pmod{y}$ holds. To this end, define

$$s = a(u - v), \quad t = -b(u - v), \quad z = u - sx.$$

Then $u = z + sx$ or in other words $u \equiv z \pmod{x}$ holds by definition of z. We also have

$$v = u - (u - v)(ax + by) = u - (u - v)ax - (u - v)by = u - sx + ty = z + ty$$

so $v \equiv z \pmod{y}$ as required.

It remains to identify the kernel of φ. Since $\varphi(xy) = ([xy], [xy]) = ([0], [0])$, the ideal xyR is contained in $\ker\varphi$. Reciprocally, let $z \in R$ be any element with $\varphi(z) = ([0], [0])$, so $z \in xR \cap yR$. Since x and y are coprime, the ideals xR and yR are coprime, hence their intersection is equal to their product by a proposition from "Ideal arithmetic", which shows $z \in xyR$ as required. □

Theorem 2.84

Let M be a finitely generated module over a PID R. Then we have

$$M \cong R^n \oplus \bigoplus_{i=1}^{m} R/x_iR$$

for

- some integer $n \geq 0$ and,
- non-zero, non-unit elements $x_1, \ldots, x_m \in R$ such that $x_i \mid x_{i+1}$ for $1 \leq i < m$.

The integer n is unique, and the elements $x_1, \ldots, x_m \in R$ are unique up to multiplication with a unit.

Note 2.85. R^n is known as free part and the the rest is known as the torsion part.

Remark 2.86. We cannot distinguish between x_i and $-x_i$.

Remark 2.87. We can also write for $x_j = p_1^{e_{1j}} \cdots p_k^{e_{kj}}$

$$M \cong R^n \oplus \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m} R/p_i^{e_{ij}} R$$

where p_i are primes and $e_{ij} \geq 0$ are integers.

Theorem 2.88 (Elementary divisors theorem)
Let M be a finitely generated free module over a PID R and, let $N \subseteq M$ be a submodule. Then

1. N is free and,
2. there exists a basis $e_1, \dots, e_r$ of M and elements $x_1, \dots, x_s$ of R with $s \leq r$ such that $x_1 e_1, \dots, x_s e_s$ is a basis of N.

Corollary 2.89
Let A be a finitely generated module over the PID $\mathbb{Z}$ (i.e. A is a commutative group) Then,

$$A \cong \mathbb{Z}^n \oplus F$$

where F is finite group. The integer n is unique and, called the **rank** of A, the finite group F is called the **torsion subgroup** of A. Furthermore,

$$F \cong \bigoplus_{i=1}^{m} \mathbb{Z}/d_i\mathbb{Z}$$

where $d_1, \dots, d_m$ are positive unique integers satisfying $d_1 \mid d_2 \mid \cdots \mid d_m$

Remark 2.90. We can represent the torsion group as

$$F \cong \bigoplus_{i=1}^{m} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

where p_i are prime numbers, not necessarily distinct and e_i are positive integers.

2.3 The tensor product

Definition 2.91. Let M, N and P be R-modules. A map $\beta : M \times N \to P$ is said to be R-**bilinear** if

$$\beta(x_1 m_1 + x_2 m_2, n) = x_1 \beta(m_1, n) + x_2 \beta(m_2, n)$$
$$\beta(m, x_1 n_1 + x_2 n_2) = x_1 \beta(m, n_1) + x_2 \beta(m, n_2)$$

holds for all $x_1, x_2 \in R$, $m, m_1, m_2 \in M$ and, $n, n_1, n_2 \in N$.

Note 2.92. This mean the map is linear in each entry. The map is a linear for one entry given the other remains fixed.

Definition 2.93. Let R be a commutative ring and, let M and N be R-module. The **tensor product** $M \otimes_R N$ is the R-module F/G, where F is the free R-module generated by the set of symbols

$$\{s(m,n) : m \in M, n \in N\}$$

and $G \subseteq F$ is the submodule generated by all elements of the form

- $s(x_1m_1 + x_2m_2, n) - x_1s(m_1, n) - x_2s(m_2, n)$ and,
- $s(m, x_1n_1 + x_2n_2) - x_1s(m, n_1) - x_2s(m, n_2)$

where $x_1, x_2 \in R, m, m_1, m_2 \in M$ and $n, n_1, n_2 \in N$. We denote the class of $s(m, n)$ of $F/G = M \otimes_R N$ by $m \otimes n$.

Definition 2.94. Elements of $M \otimes_R N$ of the form $m \otimes n$ are called **elementary tensors**.

Remark 2.95. In general, not every element of the tensor product $M \otimes_R N$ is an elementary tensor but, rather a finite sum of elementary tensors. Furthemore, it is not true in general that $m_1 \otimes n = m_2 \otimes n \Rightarrow m_1 = m_2$.

Note 2.96. Elements of $M \otimes_R N$ are formal sums of symbols

$$\sum_{i=1}^{k} m_i \otimes n_i$$

with $m_i \in M$ and $n_i \in N$. We impose the following two computation rules

$$(x_1m_1 + x_2m_2) \otimes n = x_1(m_1 \otimes n) + x_2(m_2 \otimes n)$$

$$m \otimes (x_1n_1 + x_2n_2) = x_1(m \otimes n_1) + x_2(m \otimes n_2)$$

for all $x_1, x_2 \in R$ and $m, m_1, m_2 \in M$ and $n, n_1, n_2 \in N$. These rules explain the external multiplication of elements of R with elements of $M \otimes_R N$. The two rules can be summarised by saying that the canonical map $\gamma : M \times N \to M \otimes_R N$ sending (m, n) to the symbol $m \otimes n$ is R-bilinear.

Example 2.97

Let $R = \mathbb{Z}$. We have that
$$\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$$
as an element of this R-module is of the form $a \otimes b$ where $a \in \mathbb{Z}/2\mathbb{Z}$ and $b \in \mathbb{Z}/3\mathbb{Z}$. Therefore, $3 \equiv 1 \pmod 2$ so,
$$\begin{aligned} a \otimes b &= (3a) \otimes b \\ &= 3(a \otimes b) \\ &= a \otimes (3b) \\ &= a \otimes 0 \\ &= 0 \otimes 0 = 0. \end{aligned}$$

Theorem 2.98 (Universal property)

Let M, N and P be R-modules, and let $\beta : M \times N \to P$ be a bilinear map. Define the map
$$\begin{aligned} b : M \otimes_R N &\to P \\ b(m \otimes n) &= \beta(m, n) \end{aligned}$$
Suppose T is an R-module and $\tau : M \times N \to T$ is a bilinear map, such that for every bilinear map $\beta : M \times N \to P$ there exists a unique linear map $b : T \to P$ such that $b \circ \tau = \beta$. Then, there exists a unique isomorphism of R-modules $\alpha : M \otimes_R N \to T$ such that $c = \alpha \circ \gamma$.

Note 2.99. Let M, N and P be R-modules, and let $\beta : M \times N \to P$ be a bilinear map. Out of β we construct a linear map $b : M \otimes_R N \to P$ defined by $b(m \otimes n) = \beta(m, n)$ and R-linearity. The linear map b is the only linear map $b : M \otimes_R N \to P$ for which the diagram
$$\begin{tikzcd} M \times N \arrow[r, "\beta"] \arrow[d, "\gamma"'] & P \\ M \otimes_R N \arrow[ur, dashed, "\exists! b \text{ bilinear}"'] & \end{tikzcd}$$
commutes. We find this way a natural bijection
$$\{R\text{-linear maps } M \otimes_R N \to P\} \simeq \{R\text{-bilinear maps } M \times N \to P\}$$
sending b to $\beta = \gamma \circ b$.

2.3.1 Functoriality of the tensor product

Definition 2.100. Let $f : M_1 \to M_2$ and $g : N_1 \to N_2$ be homomorphism of R-modules. The homomorphism
$$\begin{aligned} f \otimes g : M_1 \otimes_R N_1 &\to M_2 \otimes_R N_2 \\ (f \otimes g)(m \otimes n) &= f(m) \otimes g(n) \end{aligned}$$
on elementary tensors is called the **homomorphism induced** by f and g.

Theorem 2.101. The map defined above corresponds to the bilinear map

$$\begin{aligned} M_1 \times N_1 &\to M_2 \otimes N_2 \\ (m, n) &\mapsto f(m) \otimes g(n). \end{aligned}$$

Proposition 2.102 (Additivity of the tensor product)
Let R be a commututative ring and, let M_1, M_2 and N be R-modules. The map

$$\begin{aligned} (M_1 \oplus M_2) \otimes N &\to (M_1 \otimes N) \oplus (M_2 \otimes N) \\ (m_1, m_2) \otimes n &\mapsto (m_1 \otimes n, m_2 \otimes n). \end{aligned}$$

is an isomorphism.

Proof. The inverse map is given by

$$(m_1 \otimes n_1, m_2 \otimes n_2) \mapsto (m_1, 0) \otimes n + (0, m_2) \otimes n_2.$$

□

Proposition 2.103
In general,

$$\left(\bigoplus_{i=1}^{k} M_i\right) \otimes \left(\bigoplus_{j=1}^{\ell} N_j\right) \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\ell} M_i \otimes N_j.$$

Example 2.104. We have $\mathbb{R}^n \otimes \mathbb{R}^m \cong \underbrace{\mathbb{R} \oplus \cdots \oplus \mathbb{R}}_{\text{n times}} \otimes \underbrace{\mathbb{R} \oplus \cdots \oplus \mathbb{R}}_{m \text{ times}}$.

Example 2.105
How many elements are there in the $\mathbb{Z}$-module

$$\mathbb{Z}/68\mathbb{Z} \otimes \mathbb{Z}[i]?$$

Solution. We have that

$$\begin{aligned} \mathbb{Z}/68\mathbb{Z} \otimes (\mathbb{Z} \oplus \mathbb{Z}) &= (\mathbb{Z}/68\mathbb{Z} \otimes \mathbb{Z}) \oplus (\mathbb{Z}/68\mathbb{Z} \otimes \mathbb{Z}) \\ &= \mathbb{Z}/68\mathbb{Z} \oplus \mathbb{Z}/68\mathbb{Z}. \end{aligned}$$

Therefore, there are 68^2 elements.

Proposition 2.106

Let k be a field, and let V and W be finite dimensional vector spaces over k, and denote by $V^* = \mathrm{Hom}(V, k)$ the dual of V. The natural linear map

$$\Phi : V \otimes_k W \to \mathrm{Hom}(V^*, W)$$

defined by $\Phi(v \otimes w)(\varphi) = \varphi(v)w$ for all $v \in V$, $w \in W$ and $\varphi \in V^*$ is an isomorphism.

Proof. The vector spaces $V \otimes_k W$ and $\mathrm{Hom}(V^*, W)$ have the same dimension, so it suffices to show that Φ is injective. Let

$$x = \sum_{i=1}^{n} v_i \otimes w_i$$

be an element of the kernel of Φ, and assume without loss of generality that the elements $w_1, \ldots, w_n$ of W are linearly independent. That x belongs to the kernel of Φ means that

$$\Phi(x)(\varphi) = \sum_{i=1}^{n} \varphi(v_i)w_i = 0$$

holds for all linear forms $\varphi : V \to k$. By assumption on the linear independence of $w_1, \ldots, w_n$, this implies that for all $1 \leq i \leq n$ the equality $\varphi(v_i) = 0$ holds for every linear form φ. We deduce that $v_i = 0$ for all i, hence that $x = 0$ and that Φ is indeed injective. □

Proposition 2.107. Let R be a commutative ring and, let M, N and P be are R-modules. The map

$$\begin{aligned} \alpha : \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) &\to \mathrm{Hom}_R(M \otimes_R N, P) \\ \phi &\mapsto [m \otimes n \mapsto \phi(m)(n)] \end{aligned}$$

is an isomorphism.

Proof. It is enough to write the inverse map:

$$\begin{aligned} \beta : \mathrm{Hom}_R(M \otimes_R N, P) &\to \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \\ \psi &\mapsto [m \mapsto [n \mapsto \psi(m, n)]]. \end{aligned}$$

□

Proposition 2.108. Let R be a commutative ring, let S be a commutative R-algebra, let M be an R-module and let N be an S-module. The map

$$\begin{aligned} \mathrm{Hom}_R(M, N) &\to \mathrm{Hom}_S(S \otimes M, N) \\ f &\mapsto [s \otimes m \mapsto sf(m)] \end{aligned}$$

is an isomorphism of S-modules.

2.3.2 The adjuction formulas

Proposition 2.109 (L'isomorphisme cher à Cartan)
Let R be a commutative ring, and let M, N, and P be R-modules. The **adjuction map**

$$\alpha : \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \to \mathrm{Hom}_R(M \otimes_M N, P)$$
$$\alpha(f)(m \otimes n) = f(m)(n)$$

is an isomorphism of R-modules.

Proof. To prove the bijectivity it is enough to find the inverse module homomorphism of α which is given by

$$\beta : \mathrm{Hom}_R(M \otimes_M N, P) \to \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$$
$$\beta(g)(m)(n) = g(m \otimes n).$$

□

Proposition 2.110. Let R be a commutative ring and let S be an R-algebra. Let M be an R-module and let N be an S-module. The **adjuction map**

$$\alpha : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes M, N)$$
$$\alpha(f)(s \otimes m) = sf(m)$$

is an isomorphism of R-modules.

Proof. To prove the bijectivity it is enough to find the inverse module homomorphism of α which is given by

$$\beta : \mathrm{Hom}_S(S \otimes M, N) \to \mathrm{Hom}_R(M, N)$$
$$\beta(g)(m) = g(1 \otimes m).$$

□

3 Rings and Modules

3.1 Endomorphisms of modules

3.1.1 The Cayley-Hamilton theorem

Theorem 3.1

Let R be a commutative ring and let M be a finitely generated R-module. Let $m_1, \dots, m_n$ be generators of M and, let $\phi : M \to M$ be an endomorphism of M. Let A be a matrix of size $n \times n$ with coefficients in R such that

$$\phi(m_i) = \sum_{j=1}^{n} a_{ij} m_j \quad \forall i \in \{1, \dots, n\}.$$

Define the **characteristic polynomial** of A as

$$\chi_A(X) = \det(X \operatorname{id}_n - A) \in R[X].$$

Then,

$$\chi_A(\phi) = 0$$

in $\operatorname{End}(M)$.

Proof. The module M is naturally a module over the ring $R[\phi]$. The equation (3.1) can be rewritten as

$$0 = \sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij}) m_j \quad \text{for all } 1 \le i \le n$$

where δ_{ij} is Kronecker's delta. We can compactify this relation further by introducing the $n \times n$ matrix P with coefficients $p_{ij} = (\delta_{ij}\phi - a_{ij}) \in R[\phi]$. This matrix describes a homomorphism

$$P \colon M^n \to M^n, \quad y \mapsto Py$$

and the above relation reads $Pm = 0$, where m is the column vector with coefficients $m_1, \dots, m_n$. Let Q be the adjugate matrix of P, that is, the transpose of the matrix of cofactors of P. The matrix Q has the property $PQ = QP = \det(P)\mathrm{Id}_n$. We find in particular the equality

$$\det(P)m = QPm = 0$$

in M^n, or alternatively, the equalities $\det(P)m_i = 0$ for $1 \le i \le n$. But $\det(P) = \chi_A(\phi)$, so we have indeed shown that $\chi_A(\phi)$ is the zero endomorphism of M, which is what the proposition claims. □

3.1.2 Nakayama's lemma

Theorem 3.2 (Nakayama's lemma)

Let M be a finitely generated R-module and, let $I \subseteq R$ be an ideal. If $IM = M$ then, there exists $x \in R$ such that

$$x \equiv 1 \pmod{I} \quad \text{and} \quad xM = 0.$$

Proof. Let $m_1, \dots, m_n$ be generators of M, write $\operatorname{id} : M \to M$ for the identity map. Notice that $IM \subseteq M$ consists of those elements of M which can be written as R-linear combinations of $m_1, \dots, m_n$ with coefficients in I. Since $M = IM$, each m_i can be written as

$$\mathrm{id}(m_i) = m_i = \sum_{j-1}^{n} a_{ij} m_j$$

for some elements $a_{ij} \in I$. Let A denote the $n \times n$ matrix with coefficients a_{ij} and write

$$\chi_A(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

and notice that the coefficients $a_0, \ldots, a_{n-1} \in I$. The endomorphism

$$\chi_A(\mathrm{id}) = (1 + a_{n-1} + \cdots + a_1 + a_0)\,\mathrm{id} = 0.$$

Setting $x = 1 + a_{n-1} + \cdots + a_1 + a_0$ we find $xM = 0$ and $x \equiv 1 \pmod{I}$. □

Corollary 3.3 (Nakayama's lemma — version 2)

Let R be a commutative ring, let M be a finitely generated R-module and, denote by $J \subseteq R$ the Jacobson radical of R.

1. If $JM = M$ then $M = 0$.
2. Let $N \subseteq M$ be a submodule, if $M = N + JM$, then $N = M$.
3. The elements $x_1, \ldots, x_m \in M$ generate M if and only if their classes $[x_1], \ldots, [x_n] \in M/JM$ generate M/JM.

Proof. An element $x \in R$ which satisfies $x \equiv 1 \mod J$ is a unit by Proposition 1.84. Therefore, $JM = M$ implies that there exists a unit $x \in R^\times$ such that $xM = 0$, which implies $M = 0$. This shows statement (1). To show statement (2), set $Q = M/N$, and notice that the relation $M = N + JM$ is equivalent to $JQ = Q$, which by (1) implies $Q = 0$ or equivalently $N = M$. Statement (3) follows by applying (2) to the submodule N of M generated by $x_1, \ldots, x_n$. □

3.1.3 The Jordan normal form

Note 3.4. In linear algebra a common problem is to find a basis of V with respect to which the matrix of the given endomorphism ϕ is simple as possible. In this section we apply classification theorem for finitely generated modules over a PID to this problem.

Note 3.5 (SETUP)**.** In this section, k is a field, V is a finite dimension vector space over k and, $\phi : V \to V$ is a k-linear endomorphism of V. We set $R = k[X]$ and regard V as an R-module by means of the scalar multiplication defined by

$$(f, v) \mapsto f(\phi)(v)$$

for every $f \in R$ and $v \in V$.

Lemma 3.6

As an $R = k[X]$-module, we have that

$$V \cong R/f_1R \oplus \cdots \oplus R/f_nR$$

for some non-constant polynomials $f_1, \ldots, f_n$. These polynomials satisfy

$$\dim(V) = \sum_{i=1}^{n} \deg(f_i).$$

Moreover, the polynomials $f_1, \ldots, f_n$ can be chosen to be monic and, in such a way that either one of the following tow properties are satisfied

1. The polynomial $f_i \mid f_{i+1}$ for all $1 \leq i < n$.
2. Each polynomial f_i is a power of an irreducible polynomial.

Definition 3.7. Let $f \in R$ be a monic polynomial of degree $d > 0$, say

$$f(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0$$

with coefficients $a_0, \ldots, a_{d-1} \in k$. The R-module R/fR is finitely dimensional of dimension d as a k-vector space, indeed, the classes $[1], [X], \ldots, [X^{d-1}]$ form a k-basis of R/fR. As a vector space, R/fR comes with a distinguished endomorphism which is multiplication by X, that is, $[g(X)] \mapsto [Xg(X)]$. With respect to the basis $[1], [X], \ldots, [X^{d-1}]$, this endomorphism is given by the **companion matrix** of f, which is the matrix

$$C(f) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{d-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}$$

of size $d \times d$ and coefficients in k.

Corollary 3.8. We deduce that if $f_1, \ldots, f_n$ are polynomials such as in the lemma above, then ϕ (from Note 3.5) is represented by the block-diagonal matrix

$$\begin{pmatrix} C(f_1) & 0 & \cdots & 0 \\ 0 & C(f_2) & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & C(f_n) \end{pmatrix}$$

with respect to an appropriate basis of V.

Definition 3.9. A polynomial $f \in R = k[X]$ of degree $d > 0$ is said to be **separable** if f is coprime to its derivative f'.

Definition 3.10. The field k is said to be a **perfect field** if every irreducible polynomial with coefficient in k is separable.

Definition 3.11. A field F is called **algebraically closed** if every non-constant polynomial $p(x) \in F[x]$, where $F[x]$ denotes the ring of polynomials with coefficients in F, has at least one root in F. In other words, there are no non-constant polynomials over F that are irreducible, meaning every polynomial can be factored into linear factors in $F[x]$.

Theorem 3.12

The following are all perfect fields:

- all finite fields,
- all fields of characteristic zero and,
- all algebraically closed fields.

Theorem 3.13. Let $g \in R = k[X]$ be an irreducible, separable polynomial of degree $d > 0$, let $s > 0$ be an integer and set $f = g^s$. The k-vector space R/fR has a basis with respect to which the matrix of the endomorphism given by multiplication with X is

$$\begin{pmatrix} C(g) & I_d & 0 & \cdots & 0 & 0 \\ 0 & C(g) & I_d & 0 & \cdots & 0 \\ 0 & 0 & C(g) & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & I_d & 0 \\ 0 & 0 & \cdots & 0 & C(g) & I_d \\ 0 & 0 & \cdots & 0 & 0 & C(g) \end{pmatrix}$$

which is a matrix of size $ds \times ds$ divided in $s \times s$ blocks each of size $d \times d$. In particular, I_d denotes the identity matrix of size $d \times d$.

Corollary 3.14. Let k be an algebraically closed field, and let $\varphi : V \to V$ be an endomorphism of a finite dimensional k-vector space V. There exists a basis of V with respect to which the matrix associated with φ has block diagonal form,

$$\begin{pmatrix} J(\lambda_1) & 0 & \cdots & 0 \\ 0 & J(\lambda_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J(\lambda_n) \end{pmatrix}$$

and each block on the diagonal is of the form

$$J(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$$

for some eigenvalue λ of φ.

3.2 Finite algebras

Remark 3.15. In this context, the adjective *finite* means that algebras are finitely generated as modules and, it does NOT refer to any ring or algebra having finitely many elements.

Note 3.16. Recall, a R-algebra is a R-module with a ring structure.

3.2.1 Generalities on finite algebras

Definition 3.17. Let A be a commutative ring and let B be a commutative A-algebra.

- We say that B is a **finite A-algebra** if B is finitely generated as an A-module.
- If the structural map $A \to B$ is injective, we say that B is a **finite ring extension** of A.
- If A and B are both fields, we talk about **finite field extensions**.

Example 3.18

Let k be a field. A k-algebra B is finite if and only if B is finite dimensional as a vector space over k. Thus, for example, C is a finite $\mathbb{R}$-algebra, and the ring of polynomials $\mathbb{R}[X]$ is not a finite $\mathbb{R}$-algebra, although it is finitely generated $\mathbb{R}$-algebra.

Theorem 3.19. Let k be a field, and let B be a finite k-algebra. If B is an integral domain, then B is a field.

Proposition 3.20. Let A be a commutative ring, let B be a finite A-algebra and let C be a finite B-algebra. Then C is a finite A-algebra.

Proof. Let $b_1, \ldots, b_n$ be generators of B as an A-module, and let $c_1, \ldots, c_m$ be generators of C as a B-module. Then the elements $\{b_i c_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ of C generate C as an A-module. □

Definition 3.21. Let A be a commutative ring and let B be a commutative A-algebra. An element $b \in B$

- is **algebraic over** A if there exists a non-zero polynomial $f \in A[X]$ such that $f(b) = 0$,
- is **transcendental** if not algebraic;
- is **integral over** A if there exists a monic polynomial $f \in A[X]$ such that $f(b) = 0$.

Example 3.22. Integral elements are algebraic elements, and if A is a field, then all algebraic elements are integral. In the case $A = \mathbb{Z}$ and $B = \mathbb{C}$ one speaks of algebraic and transcendental numbers, and of algebraic integers.

Example 3.23

π is a transcendental number: There is no non-zero polynomial f with integer or rational coefficients with $f(\pi) = 0$. On the other hand, the complex number $\sqrt{2}$ is an algebraic integer. The number $\frac{1}{2}(\sqrt{3}+1)$ is algebraic, since it is a root of the polynomial $2X^2 - 2X - 1$, but it is not an algebraic integer. Indeed, the polynomial $2X^2 - 2X - 1$ is irreducible, hence divides any polynomial $f \in \mathbb{Z}[X]$ satisfying $f\left(\frac{1}{2}(\sqrt{3}+1)\right) = 0$. Any such polynomial must therefore have an even leading coefficient. The number $\frac{1}{2}(\sqrt{5}+1)$ on the other hand is an algebraic integer, as it is a root of the monic polynomial $X^2 - X - 1$.

Lemma 3.24. Let A be a commutative Noetherian ring and let B be elements of a commutative A-algebra B. The elements $b_1, \ldots, b_n \in B$ are integral over A if and only if the A-subalgebra of B generated by $b_1, \ldots, b_n$ is a finite A-algebra.

Proof. We may suppose without loss of generality that B is generated, as an A-algebra, by the elements $b_1, \ldots, b_n$.

- Proof of ($\Rightarrow$).
  Suppose that $b_1, \ldots, b_n$ are integral over A, and let us show that B is finite. By induction and the proposition above, it suffices to show that if b is integral, then the A-algebra $A[b] \subseteq B$ generated by b is finite. By hypothesis, there exists a monic polynomial $f(X) \in A[X]$, say of degree $n \geq 1$, such that $f(b) = 0$. We claim that $1, b, \ldots, b^{n-1}$ generate B as an A-module. Indeed, every element $c \in B$ can be written as $c = g(b)$ for some polynomial $g \in A[X]$. Since f is monic, we can use polynomial division to write $g = fh + r$ where $r \in A[X]$ is of degree $< n$. We find

  $$c = g(b) = f(b)h(b) + r(b) = r(b)$$

  and $r(b)$ is an A-linear combination of $1, b, b^2, \ldots, b^{n-1}$, hence the claim.

- Proof of ($\Leftarrow$).
  Suppose B is finite, pick any $b \in B$ and let us show that b is integral over A. For every integer $i \geq 0$, let $B_i \subseteq B$ be the A-submodule generated by $1, b, b^2, \ldots, b^i$. Since B is finitely generated as an A-module and A is Noetherian, the chain of submodules $B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots$ eventually stabilises, so there exists an integer $n \geq 1$ such that $B_n = B_{n-1}$ holds. This means that $b^n \in B_{n-1}$, hence b^n can be written as

  $$b^n = a_0 + a_1 b + a_2 b^2 + \ldots + a_{n-1} b^{n-1}$$

  for some $a_0, \ldots, a_{n-1} \in A$. This shows that b is integral over A.

□

Theorem 3.25. Let A be a commutative Noetherian ring and let B be an A-algebra. Let $b_1, b_2 \in B$ be integral over A. Then $b_1 + b_2$ and $b_1 b_2$ are integral over A.

Proof. The sum $b_1 + b_2$ and the product $b_1 b_2$ are both elements of the A-subalgebra of B generated by b_1 and b_2. By the lemma above, this A-algebra is finite, hence all of its elements are integral over A. □

3.2.2 Rings of algebraic integers

Definition 3.26. A **number field** k is a finite field extension of $\mathbb{Q}$ i.e. a field containing $\mathbb{Q}$ which is finitely dimensional as a $\mathbb{Q}$-linear vector space. The dimension of k as a $\mathbb{Q}$-linear vector space is denoted by $[k : \mathbb{Q}]$ and called the **degree** of k.

Example 3.27

Some examples of number fields.

- $\mathbb{Q}$,
- $\mathbb{Q}[\sqrt{2}]$,
- any adjoint of $\mathbb{Q}$,
- $\mathbb{Q}\left[e^{\frac{2\pi i}{n}}\right]$ has degree equal to the Euler totient function $\phi(n)$.

Definition 3.28. We call the non-zero ring homomorphism $\sigma : k \to \mathbb{C}$ a **complex embedding** of k.

> **Remark 3.29.** This map is injective because the ideals of k are k and 0, since the kernel is an ideal $\ker(\sigma)$ is also trivial.

Theorem 3.30. The set of ring homomorphism $\mathrm{Hom}_{\mathbb{Q}}(k, \mathbb{C})$ is finite and has exactly $[k : \mathbb{Q}]$ elements.

Lemma 3.31. Let K be a field of characteristic zero and let $f, g \in K[X]$ be non-zero separable polynomials and let $a, b \in K$ with $f(a) = 0$ and $g(b) = 0$. For all but finitely many $\lambda \in K$ the greatest common divisor of the polynomials $g(X)$ and $f(a + \lambda b - \lambda X)$ is $X - b$.

Proof. We may without loss of generality suppose that f and g are monic, and that K is algebraically closed, so f and g split into products of linear factors, say

$$f(X) = (X - a_1) \cdots (X - a_m) \quad \text{and} \quad g(X) = (X - b_1) \cdots (X - b_n)$$

with $a = a_1$ and $b = b_1$. Since g is separable, the roots $b_1, \ldots, b_n$ are distinct. Since $g(b) = 0$ and $f(a+\lambda b-\lambda X) = f(a) = 0$ the linear factor $X - b$ divides $g(X)$ and $f(a+\lambda b-\lambda X)$. Now suppose that $X - c$ is another common factor of $g(X)$ and $f(a + \lambda b - \lambda X)$. Then $c = b_j$ for some $j \neq 1$ and $a+\lambda b-\lambda b_j$ is a root of f, hence $a+\lambda b-\lambda b_j = a_i$ or equivalently

$$\lambda = \frac{a_i - a}{b - b_j}$$

for some $i \neq 1$. This leaves finitely many choices for λ. □

Theorem 3.32 (Primitive element theorem)

Let k be a number field. There exists an element $\alpha \in k$ such that $k = \mathbb{Q}[\alpha]$. We call this element **primitive**.

Proof. We will show more generally that if $k_0 \subseteq k$ are fields of characteristic zero such that k is finite dimensional as a vector space over k_0, then there exists an element in k which generates k as a k_0-algebra. Since k is finite dimensional as a vector space over k_0, the field k is finitely generated as a k_0-algebra, that means there exist finitely many elements $a_1, \dots, a_n \in k$ such that $k = k_0[a_1, \dots, a_n]$. Arguing by induction on n we may suppose for our purposes that $n = 2$, so $k = k_0[a, b]$ for some $a, b \in k$. Let $f, g \in k_0[X]$ be the minimal polynomials of a and b respectively. The polynomials f and g are separable since they are irreducible and k_0 is of characteristic zero, hence perfect.
We claim that for all but finitely many choices of $\lambda \in k_0$, the element $c = a + \lambda b$ in k generates k as a k_0-algebra, that is to say $k = k_0[c]$. Set $k_1 = k_0[c]$ and let $h \in k_1[X]$ be the minimal polynomial of b. The polynomial $h(X)$ is irreducible, hence divides $g(X)$ and $f(a + \lambda b - \lambda X)$ in the ring $k_1[X]$. Let us now choose $\lambda \in k_0$ such that the greatest common divisor of $g(X)$ and $f(a + \lambda b - \lambda X)$ is $X - b$. Such an element λ exists by Lemma 3.28 and the fact that k_0 has infinitely many elements. With this choice of λ, the minimal polynomial h divides $X - b$, hence $h(X) = X - b$, and thus $b \in k[c]$. But then also $a = c - \lambda b$ belongs to $k[c]$, hence $k = k[a, b] \subseteq k[c]$. □

Corollary 3.33

Let k be a number field of degree n. There exists exactly n complex embeddings $\sigma : k \to \mathbb{C}$.

Proof. By the primitive element theorem there exists $\alpha \in k$ with $k = \mathbb{Q}[\alpha]$ (i.e. α is the primitive element). Let $f \in \mathbb{Q}[X]$ be the minimal polynomial of α. The ring homomorphism

$$\begin{aligned}\mathbb{Q}[X]/\langle f\rangle &\to k\\ [p] &\mapsto p(\alpha)\end{aligned}$$

is an isomorphism. Comparing dimension, we see that the degree of f is equal to the degree of the number field k. Let $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ denote the complex roots of f. These roots are distinct since f is irreducible hence, separable. Every ring homomorphism

$$\begin{aligned}\mathbb{Q}[X]/\langle f\rangle &\to \mathbb{C}\\ [p] &\mapsto p(\lambda)\end{aligned}$$

for $\lambda \in \{\lambda_1, \dots, \lambda_n\}$. In other words, a ring homomorphism $\phi : k \to C$ is uniquely determined by $\phi(\alpha)$, and the possible choices for $\phi(\alpha)$ are $\lambda_1, \dots, \lambda_n$. □

Lemma 3.34 (Dedekind)

Let k be a number field of degree n. The complex embeddings $\sigma_1, \dots, \sigma_n : k \to \mathbb{C}$ of k are $\mathbb{C}$-linearly independent in the complex vector space $\operatorname{Hom}(k, \mathbb{C})$ of group homomorphism from k to $\mathbb{C}$.

Proof. Let $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ such that $\alpha_1\sigma_1(x) + \dots + \alpha_n\sigma_n(x) = 0$ for all $x \in k$. We must show that $\alpha_1 = \dots = \alpha_n = 0$ holds. If this is false, then we may choose, reindexing the σ_i if necessary, the shortest linear combination

$$\alpha_1\sigma_1 + \ldots + \alpha_q\sigma_q = 0$$

in the sense that $\alpha_1, \dots, \alpha_q$ are all non-zero and $1 \leq q \leq n$ is minimal. Clearly $q \geq 2$, and

$$0 = \sum_{i=1}^{q} \alpha_i \sigma_i(yx) = \sum_{i=1}^{q} \alpha_i \sigma_i(y)\sigma_i(x)$$

$$0 = \sigma_q(y) \sum_{i=1}^{q} \alpha_i \sigma_i(x) = \sum_{i=1}^{q} \alpha_i \sigma_q(y)\sigma_i(x)$$

holds for all $x, y \in k$. Taking the difference shows that

$$0 = \sum_{i=1}^{q-1} \alpha_i(\sigma_i(y) - \sigma_q(y))\sigma_i(x)$$

holds for all $x, y \in k$. By minimality of q, and since we assumed $\alpha_i \neq 0$ we deduce that $\sigma_i = \sigma_q$ holds for all $y \in k$ and $i < q$. But this contradicts the assumption that $\sigma_1, \dots, \sigma_n$ are distinct complex embeddings of k.

□

Proposition 3.35

Let k be a number field of degree n, and let $a \in k$. Let $\chi_a(X) \in \mathbb{Q}[X]$ denote the characteristic polynomial of the $\mathbb{Q}$-linear map $a : k \to k$ sending x to ax. It is a monic polynomial of degree n, say

$$\chi_a(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$$

with $a_{n-1} = -\mathrm{tr}(a)$ and $\det(a) = (-1)^n a_0$. We have the relations

- $\mathrm{tr}(a + b) = \mathrm{tr}(a) + \mathrm{tr}(b)$;
- $\det(ab) = \det(a)\det(b)$;
- if $a \in \mathbb{Q}$, then $\mathrm{tr}(a) = na$ and $\det(a) = a^n$.

hold for all $a, b \in k$.

Definition 3.36. Let k be a number field of degree n. The **discriminant** of a vector $(x_1, \dots, x_n) \in k^n$ is the determinant

$$D(x_1, \dots, x_n) = \det((\mathrm{tr}(x_i x_j))_{ij})$$

of the symmetric $n \times n$ matrix with coefficients $\mathrm{tr}(x_i x_j) \in \mathbb{Q}$.

> **Remark 3.37.** If $x_1, \dots, x_n$ are all algebraic integers, then $\mathrm{tr}(x_i x_j)$ is an integer for all i, j, and hence $D(x_1, \dots, x_n)$ is an integer as well.

Proposition 3.38

Let A be a matrix of size $n \times n$ with coefficients $a_{ij} \in \mathbb{Q}$, and define

$$y_i = \sum_{j=1}^{n} a_{ij} x_j$$

for $i = 1, 2, \ldots, n$. Then we have

$$D(y_1, \ldots, y_n) = \det(A)^2 \cdot D(x_1, \ldots, x_n).$$

Definition 3.39. Let k be a number field of degree n, and let $B \subseteq k$ be a subgroup which is free of rank n. The discriminant of B is the rational number

$$D_B := D(x_1, \ldots, x_n)$$

where $x_1, \ldots, x_n$ is any basis of B.

Proposition 3.40. Let k be a number field of degree n and let $B_0 \subseteq B_1$ be finitely generated subgroups of rank n. Then B_0 has finite index in B_1 and $D_{B_1} = [B_1 : B_0]^2 D_{B_0}$.

Proof. By the Elementary Divisors Theorem there exists a basis $x_1, \ldots, x_n$ of B_1 and integers $e_1, \ldots, e_n$ such that $e_1 x_1, \ldots, e_n x_n$ is a basis of B_0. The integers e_i are non-zero, and the index of B_0 in B_1 is $[B_1 : B_0] = e_1 e_2 \cdots e_n$. The statement follows from the observations that $D(x_1, \ldots, x_n) = \det(\operatorname{tr}(x_i x_j)_{ij})$, taking for A the diagonal matrix with diagonal entries $e_1, \ldots, e_n$. □

Proposition 3.41

Let k be a number field of degree n, let $\sigma_1, \ldots, \sigma_n$ denote the n homomorphisms $k \to \mathbb{C}$ and let $x_1, \ldots, x_n$ be elements of k. Then $D(x_1, \ldots, x_n) = [\det(\sigma_i(x_j))]^2$.

Proof. Denote by T the matrix with coefficients $t_{ij} = \operatorname{tr}(x_i x_j)$ and denote by S the matrix with coefficients $s_{ij} = \sigma_j(x_i)$. From

$$t_{ij} = \operatorname{tr}(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j) = \sum_{k=1}^{n} s_{ik} s_{jk}$$

we deduce the equality $T = S \cdot S^\top$. Hence, $D(x_1, \ldots, x_n) = \det(T) = \det(S \cdot S^\top) = \det(S)^2$. □

Corollary 3.42. Let k be a number field of degree n, let $\sigma_1, \ldots, \sigma_n$ denote the n homomorphisms $k \to \mathbb{C}$ and let $x_1, \ldots, x_n$ be a $\mathbb{Q}$-basis of k. Then $D(x_1, \ldots, x_n) \neq 0$.

Proof. If the determinant of the matrix with coefficients $(\sigma_i(x_j))$ was zero, then the rows of this matrix would be $\mathbb{C}$-linearly dependent. Since $x_1, \ldots, x_n$ is a $\mathbb{Q}$-basis of k, this would result in a $\mathbb{C}$-linear dependence relation between the complex embeddings $\sigma_1, \ldots, \sigma_n$ of k, contradicting Dedekind's lemma. □

Definition 3.43. Let k be a number field and let $a \in k$ be said to be **integral** or an **algebraic integer** if there exists a monic polynomial $f \in \mathbb{Z}[X]$ with $f(a) = 0$. The set of algebraic integers in k is denoted by $\mathcal{O}_k$.

Remark 3.44. The algebraic integers $\mathcal{O}_k$ form indeed a subring of k. As a $\mathbb{Z}$-module, $\mathcal{O}_k$ is torsion free because k is so.

Theorem 3.45

Let k be a number field of degree n. The ring of integers $\mathcal{O}_k$ is finitely generated and free of rank n as a $\mathbb{Z}$-module.

Proof. A free subgroup $B \subseteq \mathcal{O}_k$ is of rank at most n, and there exist free subgroups $B \subseteq \mathcal{O}_k$ of rank exactly n, since indeed for any $a \in k$ some integer multiple na with $n \geq 0$ belongs to $\mathcal{O}_k$, hence $\mathcal{O}_k$ contains a $\mathbb{Q}$-basis of k. The discriminant D_B of any free subgroup $B \subseteq \mathcal{O}_k$ of rank n is an integer. Let us choose a subgroup $B \subseteq \mathcal{O}_k$ of rank n with whose discriminant D_B is minimal in absolute value. We claim that $B = \mathcal{O}_k$. Indeed, pick any $b \in \mathcal{O}_k$, and denote by $B' \subseteq k$ the subgroup generated by B and b. The group B' is free of rank n, and contains B with finite index. By Proposition 3.39, the relation

$$D_{B'} = [B' : B]^{-1} D_B$$

holds. Since $D_B \leq D_{B'}$ and $[B' : B] \geq 1$, the only possibility is $[B' : B] = 1$, and hence $B = B'$ and $b \in B$. □

Definition 3.46. Let k be a number field. The discriminant D_k of k is the discriminant of the ring of integers $\mathcal{O}_k \subseteq k$.

Appendix

A Zorn's lemma

Definition A.1. We say the set X is a **partially ordered set** if there is a given relation $\leq$ on X which is

- reflexive: $x \leq x$;
- transitive: $x \leq y$ and $y \leq z$ implies $x \leq z$;
- antisymmetric: $x \leq y$ and $y \leq x$ implies $x = y$;

these hold for all $x, y, z \in X$.

Note A.2. The symbol $\leq$ is just a symbol used to denote this relation, we could have easily used any arbitrary symbol such as $\sim$.

Definition A.3. An **upper bound** of a subset $\mathcal{C} \subseteq X$ is an element $x_0 \in X$ such that $x \leq x_0$ holds for all $x \in \mathcal{C}$.

Definition A.4. A **maximal element** in X is any element $x_0 \in X$ such that $x_0 \leq x$ implies $x_0 = x$ for all $x \in X$.

Theorem A.5 (Zorn's lemma)
Let X be a non-empty partially ordered set. If every chain $\mathcal{C} \subseteq X$ admits an upper bound in X then, X contains a maximal element.