Contents

1 Rings

1.1 Definitions and basic properties

Definition 1.1.1 (Ring)**.** A *ring* (with identity) R is a set together with two binary operations $+$ and $\cdot$ such that

(i) $(R, +)$ is an abelian group with identity $0 \in R$;

(ii) $(xy)z = x(yz)$ for all $x, y, z \in R$;

(iii) there exists $1 \in R$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$;

(iv) $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all $x, y, z \in R$.

A ring R is *commutative* if $xy = yx$ for all $x, y \in R$.

Proposition 1.1.2. *1. The identities 0 and 1 are unique.*

2. $0 \cdot x = x \cdot 0 = 0$ *for all* $x \in R$.

3. $(-x)y = x(-y) = -(xy)$ *for all* $x, y \in R$.

Definition 1.1.3 (Unit / inverse)**.** An element $x \in R$ is a *unit* (is *invertible*) if there exists $y \in R$ such that $xy = yx = 1$. Such a y is an *inverse* of x.

Proposition 1.1.4. *1. If* $x \in R$ *is invertible, then its inverse is unique.*

2. If $x, y \in R$ *are invertible, then* xy *is invertible with* $(xy)^{-1} = y^{-1}x^{-1}$.

3. The set $R^\times = \{x \in R \mid x \text{ is a unit}\}$ *forms a group under multiplication.*

Definition 1.1.5 (Unit group)**.** $R^\times$ is the *unit group* of R.

Definition 1.1.6 (Domain)**.** Let $x \in R$ be non-zero. We say that x is a *(left) zero divisor* if there exists a non-zero $y \in R$ such that $xy = 0$.

A commutative ring R is a *domain* (or *integral domain*) if $R \neq 0$ and R has no zero divisors.

Proposition 1.1.7. *If* R *is a domain and* $xy = xz$ *with* $x \neq 0$*, then* $y = z$.

Example 1.1.8. 1. The *zero ring* is $0 = \{0\}$ with $0 = 1$. Conversely, if $0 = 1$ in R, then $R = 0$.

2. A *field* is a commutative ring $F \neq 0$ for which $F^\times = F \backslash \{0\}$. Examples include $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

3. $\mathbb{Z}$ is a domain, but not a field. Its unit group is $\mathbb{Z}^\times = \{\pm 1\}$.

4. If R is a ring, then $\mathrm{Mat}_n(R) = \{n \times n \text{ matrices over } R\}$ is a non-commutative ring for $n \geq 2$. Its unit group is $(\mathrm{Mat}_n(R))^\times = GL_n(R)$, the general linear group of degree n over R. If R is commutative, then $A \in GL_n(R)$ if and only if $\det A \neq 0$.

5. $\mathbb{Z}/n\mathbb{Z}$, $n > 0$, is a commutative ring. Its unit group is $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \mid \gcd(a, n) = 1\}$, which has order $\varphi(n)$. $\mathbb{Z}/n\mathbb{Z}$ is a domain if and only if n is prime, in which case $\mathbb{Z}/n\mathbb{Z}$ is a field.

6. An *endomorphism* of a group A is a homomorphism $A \to A$. If A is an abelian group, then the set of endomorphisms of A, denoted $\operatorname{End} A$, is a ring with pointwise addition and composition. It is generally not commutative. Its unit group is $(\operatorname{End} A)^\times = \operatorname{Aut} A$.

7. If R is a ring, then
$$R[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R\}$$
is the *polynomial ring over* R. By induction, we define polynomial rings in several variables by $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$. More generally, we may construct polynomial rings $R[X]$ in an arbitrary set X of commuting variables as sums of (finite) monomials.

   If R is commutative, then $R[x]$ is commutative.

8. Taking variables in a set X to be non-commuting, we obtain non-commutative polynomial rings, which are denoted $R\langle X\rangle$.

9. If R is a ring and G a group (written multiplicatively), we write $R[G]$ for the *group ring* of all formal finite linear combinations $\sum_{g\in G} r_g g$ with $r_g \in R$. The product in $R[G]$ is induced by the one in G.

Definition 1.1.9 (Ring homomorphism)**.** Let R and S be rings. A map $f : R \to S$ is a *(ring) homomorphism* if

(i) $f(1) = 1$;

(ii) $f(x + y) = f(x) + f(y)$;

(iii) $f(xy) = f(x)f(y)$.

Notation. Write $f^\times$ for the group homomorphism $R^\times \to S^\times$ induced by f.

Example 1.1.10. There is no ring homomorphism $\mathbb{Q} \to \mathbb{Z}$.

Notation. The category of rings is denoted **Ring**, while the category of commutative rings is denoted **CRing**.

Proposition 1.1.11. *1. In* **Ring***, $\mathbb{Z}$ is an initial object.*

2. **CRing** *is a full subcategory of* **Ring***.*

3. Forget : **CRing** $\to$ **Set** *has left adjoint $X \mapsto \mathbb{Z}[X]$.*

4. Forget : **Ring** $\to$ **Set** *has left adjoint $X \mapsto \mathbb{Z}\langle X\rangle$.*

5. Forget : **Ring** $\to$ **Groups** *taking R to $R^\times$ has left adjoint $G \mapsto \mathbb{Z}[G]$.*

Definition 1.1.12 (Subring)**.** A *subring* of R is a subset $S \subset R$ such that $0, 1 \in S$ and S forms a ring with the inherited operations from R.

Proposition 1.1.13. *If $S \subset R$ is a subring, then the inclusion $i : S \hookrightarrow R$ is a ring homomorphism.*

Example 1.1.14. 1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ as subrings.

2. The set $S = \left\{\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}\right\} \subset \operatorname{Mat}_2(R)$ is not a subring of $\operatorname{Mat}_2(R)$, even though it forms a ring with the inherited operation, since $I \notin S$.

1.2 Ideals

Definition 1.2.1 (Ideal)**.** Let R be a ring. A subset $I \subset R$ is a *left ideal* of R if

(i) $(I, +)$ is a subgroup of $(R, +)$;

(ii) if $x \in R$, then $xI \subset I$.

A *right ideal* is defined analogously.

We say that I is an *ideal* (or *two-sided ideal*) if I is a left ideal and a right ideal. We write I is a (left) ideal if I is a left or right ideal.

Example 1.2.2. 1. Every ring R has the *zero ideal* $0 = \{0\}$ and the *unit ideal* R.

2. In $\mathrm{Mat}_n(R)$, the set of matrices for which all columns but the first are zero is a left ideal.

3. The intersection of any family of (left) ideals is a (left) ideal.

4. If I and J are (two-sided) ideals in R, then the group IJ generated by all products xy, where $x \in I$ and $y \in J$ is a (two-sided) ideal in R.

5. For any $x \in R$, $Rx = \{ax \mid a \in R\}$ is a left ideal, the *principal left ideal generated by* x. In particular, $0 = R \cdot 0$ and $R = R \cdot 1$. We write similarly xR for the right ideal generated by x.

6. If $X \subset R$ is a subset, we write $\langle X \rangle$ for the intersection of all (left) ideals containing X and call it *the (left) ideal generated by* X. Clearly, $\langle X \rangle$ is the smallest (left) ideal containing X. The left ideal $\langle X \rangle$ consists of all finite sums $\sum_{x \in X} r_x x$, where $r_x \in R$. We have $\langle \{x\} \rangle = Rx$ for every $x \in X$.

7. If $(I_k)_{k \in K}$ is a family of (left) ideals, then the abelian group $\sum_{k \in K} I_k$ is a (left) ideal. It is the smallest (left) ideal containing all I_k. Equivalently, it is the (left) ideal generated by $\cup_{k \in K} I_k$.

8. If I is a (left) ideal and $I \cap R^\times$ is non-empty, then $I = R$.

9. Given two ideals $I, J \subset R$, the *product ideal* IJ is the smallest ideal containing all products ab with $a \in I$ and $b \in J$.

Proposition 1.2.3. *1. $u \in R^\times$ if and only if $Ru = uR = R$.*

2. $a \in R$ is non-zero if and only if $Ra \neq 0$.

Definition 1.2.4 (Quotient ring)**.** Let R be a ring and $I \subset R$ be an ideal. The *quotient ring* R/I is the quotient group R/I together with the multiplication $(x + I)(y + I) = xy + I$.

Proposition 1.2.5. *1. The multiplication is well-defined and makes R/I a ring.*

2. The canonical map $\pi : R \to R/I$ is a ring homomorphism.

Definition 1.2.6 (Kernel / image)**.** Let $f : R \to S$ be a homomorphism.

1. The *kernel* of f is $\mathrm{Ker}(f) := f^{-1}(0) \subset R$.

2. The *image* of f is $\operatorname{Im}(f) := f(R) \subset S$.

Proposition 1.2.7. $\operatorname{Ker} f \subset R$ *is an ideal and* $\operatorname{Im} f \subset S$ *is a subring.*

Theorem 1.2.8 (First isomorphism theorem)**.** *Let $f : R \to S$ be a ring homomorphism. Then the map $\overline{f} : R/\operatorname{Ker} f \to \operatorname{Im} f$ given by $\overline{f}(x + \operatorname{Ker} f)) = f(x)$ is an isomorphism.*

Proof. By the first isomorphism theorem for groups, $\overline{f}$ is a group isomorphism of $(R/\operatorname{Ker} f, +)$ and $(\operatorname{Im} f, +)$. For products, $\overline{f}((x+I)(y+I)) = \overline{f}(xy+I) = f(xy) = f(x)f(y) = \overline{f}(x+I)\overline{f}(y+I)$. □

Theorem 1.2.9 (Correspondence theorem)**.** *Let $I \subset R$ be an ideal. Then there is a bijection between ideals of R/I and ideals of R containing I given by $J \mapsto \overline{J} = J/I$ and $\overline{J} \mapsto J = \pi^{-1}(\overline{J})$.*

Example 1.2.10.

1. $\mathbb{Z}/n\mathbb{Z}$ is the quotient of $\mathbb{Z}$ by the ideal $n\mathbb{Z}$.
2. Let $f : \mathbb{R}[x] \twoheadrightarrow \mathbb{C}$ be given by $f(g) = g(i)$. Then $\operatorname{Ker} f = (x^2+1)\mathbb{R}[x]$, so $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$.

Notation. Let $I \subset R$ be an ideal and $x, y \in R$. We write $x \equiv y \pmod I$ if $x - y \in I$.

1.3 Product of rings

Definition 1.3.1. Let $R_1, R_2 \ldots, R_n$ be rings. The *product ring* $R = R_1 \times R_2 \times \cdots \times R_n$ (in the category **Ring**) is the Cartesian product of the R_i with component-wise operations. This extends to arbitrary products.

For any $i = 1, 2, \ldots, n$ write e_i for the element in R with all but i-th components zero and the i-th component equal to 1. Clearly the elements $e_1, e_2, \ldots, e_n$ satisfy the following conditions:

(i) $e_i^2 = e_1$ (idempotents);

(ii) $e_ie_j = 0$ if $i \neq j$ (orthogonality);

(iii) $e_1 + e_2 + \cdots + e_n = 1$ (partition of 1);

(iv) $e_ir = re_i$ for all $r \in R$ (centrality).

We reverse this construction as follows. Let R be a ring and let $e_1, e_2, \ldots, e_n \in R$ be the elements satisfying the 4 conditions above. For any i the set $R_i := Re_i \subset R$ is closed under addition and multiplication. Moreover, R_i is a ring with the identity e_i. (Note that R_i is NOT a subring of R since $e_i \neq 1$ in general!)

Proposition 1.3.2. *The map $f : R_1 \times R_2 \times \cdots \times R_n \to R$ defined by $f(r_1, r_2, \ldots, r_n) = r_1 + r_2 + \cdots + r_n$ is a ring isomorphism.*

Proof. Clearly, f is additive. Let $r_i, r_i' \in R_i$ for all i. Then

$$f(r_1, r_2, \ldots, r_n)f(r_1', r_2', \ldots, r_n') = (\sum r_i)(\sum r_j') = \sum r_ir_j' = \sum r_ir_i' =$$

$$f(r_1r_1', r_2r_2', \ldots, r_nr_n') = f((r_1, r_2, \ldots, r_n)(r_1', r_2', \ldots, r_n'))$$

since $r_i r_j' = r_i e_i r_j' e_j = r_i e_i e_j r_j' = 0$ if $i \neq j$ and $f(e_1, e_2, \ldots, e_n) = \sum e_i = 1$, hence f is a ring homomorphism.

If $r \in R$, then $re_i \in R_i$ and $f(re_1, re_2, \ldots, re_n) = r$, i.e., f is surjective. We show that $\operatorname{Ker}(f) = 0$. Let $f(r_1, r_2, \ldots, r_n) = \sum r_i = 0$. For any j,

$$0 = (\sum r_i)e_j = r_j e_j = r_j$$

since $r_i e_j = r_i e_i e_j = 0$ if $i \neq j$. Thus, f is a ring isomorphism. □

Definition 1.3.3 (Relatively prime ideals)**.** Two ideals $I_1, I_2 \subset R$ are *relative prime* (or *coprime*) if $I_1 + I_2 = R$.

Theorem 1.3.4 (Chinese remainder theorem)**.** *Let R be a ring, $I_1, \ldots, I_n$ be pairwise relatively prime ideals of R, and $a_1, \ldots, a_n \in R$. Then there exists x such that $x \equiv a_i \pmod{I_i}$ for all i.*

Proof. We induct on n. The case $n = 1$ is trivial. When $n = 2$, we have $I_1 + I_2 = R$, so in particular $a_1 - a_2 = b_1 + b_2$ for some $b_1 \in I_1$ and $b_2 \in I_2$. Take $x = a_1 - b_1$.

Now consider $n \geq 3$. We claim that $(I_1 \cap \cdots \cap I_{n-1}) + I_n = R$. For each $i < n$, we have $I_i + I_n = R$, so we can pick $y_i \in I_i$ and $z_i \in I_n$ such that $y_i + z_i = 1$ for each i. Then

$$1 = (y_1 + z_1) \cdots (y_{n-1} + z_{n-1}) = y_1 \cdots y_{n-1} + (\text{monomials including } z_i\text{'s}) \in I_1 \cap \cdots \cap I_{n-1} + I_n,$$

as required. By induction, there exists $x' \in R$ such that $x' \equiv a_i \pmod{I_i}$ for $i < n$. By the claim and the case $n = 2$, there exists $x \in R$ with $x \equiv x' \pmod{I_1 \cap \cdots \cap I_{n-1}}$ and $x \equiv a_n \pmod{I_n}$. For $i < n$, we have $x \equiv x' \pmod{I_1 \cap \cdots \cap I_{n-1}}$ and $I_1 \cap \cdots \cap I_{n-1} \subset I_i$, so $x \equiv x' \equiv a_i \pmod{I_i}$. □

Corollary 1.3.5. *Let $I_1, \ldots, I_n$ be pairwise relatively prime ideals of R. Then*

$$R/(I_1 \cap \cdots \cap I_n) \cong (R/I_1) \times \cdots \times (R/I_n).$$

Proof. Define the ring homomorphism $f : R \to (R/I_1) \times \cdots \times (R/I_n)$ by

$$f(x) = (x + I_1, x + I_2, \ldots, x + I_n).$$

Then $\operatorname{Ker} f = I_1 \cap \cdots \cap I_n$, and by the Chinese remainder theorem, f is surjective, so

$$\overline{f} : R/(I_1 \cap \cdots \cap I_n) \to (R/I_1) \times \cdots \times (R/I_n)$$

is an isomorphism by the first isomorphism theorem. □

Example 1.3.6. Let $m_1, \ldots, m_n \in \mathbb{Z}$ with $\gcd(m_i, m_j) = 1$ for $i \neq j$. Let $I_i = m_i\mathbb{Z}$, so then $I_1 \cap \cdots \cap I_n = m_1 \cdots m_n\mathbb{Z}$. We have

$$\mathbb{Z}/(m_1 \cdots m_n\mathbb{Z}) \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}.$$

If we consider the sizes of the multiplicative groups and note that $(R \times S)^\times = R^\times \times S^\times$, we get

$$\varphi(m_1 \cdots m_n) = \varphi(m_1) \cdots \varphi(m_n)$$

whenever $m_1, \ldots, m_n$ are pairwise relatively prime.

1.4 Prime and maximal ideals

Definition 1.4.1 (Prime ideal)**.** Let R be a commutative ring. An ideal $P \subset R$ is *prime* if $P \neq R$ and whenever $xy \in P$, we have $x \in P$ or $y \in P$.

Theorem 1.4.2. *An ideal $P \subset R$ is prime if and only if R/P is a domain.*

Proof. ($\Longrightarrow$) Since $P \neq R$, $R/P \neq 0$. Suppose $(x+P)(y+P) = P$. Then $xy \in P$, so $x \in P$ or $y \in P$, i.e. $x + P = P$ or $y + P = P$. Hence there are no zero divisors in R/P, so R/P is a domain.

($\Longleftarrow$) If $R/P \neq 0$, then $P \neq R$. If $xy \in P$, then $P = xy + P = (x+P)(y+P)$. Since R/P is a domain, $x + P = P$, in which case $x \in P$, or $y + P = P$, in which case $y \in P$. □

Definition 1.4.3 (Maximal ideal)**.** Let R be a commutative ring. An ideal $M \subset R$ is *maximal* if $M \neq R$ and if $M \subset I$ for an ideal I, then $I = M$ or $I = R$.

Lemma 1.4.4. *A commutative ring R has exactly two ideals if and only if R is a field.*

Theorem 1.4.5. *An ideal $M \subset R$ is maximal if and only if R/M is a field.*

Proof. Ideals of R/M correspond bijectively to ideals of R containing M. Thus M is maximal if and only if R/M has exactly two ideals, which happens if and only if R/M is a field. □

Example 1.4.6.

1. The zero ring has no prime or maximal ideals.
2. Let $R = \mathbb{Z}$ and $n \geq 0$. Then $n\mathbb{Z}$ is prime if and only if $n = 0$ or $n = p$ is prime. It is maximal if and only if $n = p$ is prime.

Theorem 1.4.7. *Every non-zero commutative ring has a maximal ideal.*

Proof. Let $\mathcal{I}$ be the set of all proper ideals of a non-zero commutative ring R. Then $0 \in \mathcal{I}$, so $\mathcal{I}$ is non-empty. Order $\mathcal{I}$ by inclusion and let $\mathcal{T}$ be a chain in $\mathcal{I}$. We claim that $I = \bigcup_{J \in \mathcal{T}} J$ is a proper ideal of R, so $I \in \mathcal{I}$ is an upper bound for $\mathcal{T}$. Let $x, y \in I$. Then $x \in J$ and $y \in J'$ for some $J, J' \in \mathcal{T}$. Since $\mathcal{T}$ is totally ordered, either $J \subset J'$ or $J' \subset J$, say $J \subset J'$ without loss of generality. Then $x, y \in J'$, so $x + y \in J' \subset I$, and for any $r \in R$, we have $rx \in J \subset I$. This shows that I is an ideal, and to see that it is proper, note that $1 \notin J$ for any $J \in \mathcal{T}$, so $1 \notin I$. Thus Zorn's lemma applies, so $\mathcal{I}$ has a maximal element M, which is a maximal ideal. □

Corollary 1.4.8. *Every non-zero commutative ring has a prime ideal.*

1.5 Euclidean rings

Definition 1.5.1 (Euclidean ring)**.** A *Euclidean ring* is a commutative ring R for which there is a function $\varphi : R\backslash\{0\} \to \mathbb{Z}^{\geq 0}$ such that for every $a \in R$ and $0 \neq b \in R$, there exist $q, r \in R$ with $a = bq + r$, where either $r = 0$ or $\varphi(r) < \varphi(b)$. Such a function is a *Euclidean function* for R.

Example 1.5.2.

1. For $\mathbb{Z}$, we may take $\varphi(x) = |x|$.
2. For F a field and $R = F[x]$, we may take $\varphi(f) = \deg f$.

3. Consider the ring of *Gaussian integers* $\mathbb{Z}[i]$. Letting $\varphi(a+bi) = a^2+b^2 = |a+bi|^2$ makes $\mathbb{Z}[i]$ a Euclidean ring.

Remark 1.5.3. Euclidean rings do not come with a specification of Euclidean function. It is only necessary that some Euclidean function exists.

Definition 1.5.4 (Principal ideal ring)**.** A *principal ideal ring* is a commutative ring R for which every ideal of R is principal.

Theorem 1.5.5. *Every Euclidean ring is a principal ideal ring.*

Proof. Let $I \subset R$ be an ideal. If $I = 0$, then we are done. Otherwise, choose $b \in I$ non-zero to have minimal $\varphi(b)$. We claim that $I = bR$. It is clear that $bR \subset I$, and conversely, let $a \in I$. Since R is Euclidean, we can write $a = bq + r$. If $r = 0$, then $a = bq \in bR$. Otherwise, $\varphi(r) < \varphi(b)$, contradicting the choice of b. Thus $a \in bR$, so $I \subset bR$. □

Remark 1.5.6. The converse does not hold. For example, $\mathbb{Z}[(1+\sqrt{-19})/2]$ is a principle ideal ring which is not a Euclidean ring.

1.6 Factorization in domains

Throughout, let R be a domain unless otherwise specified.

Definition 1.6.1 (Divisibility)**.** Let $a, b \in R$ with $b \neq 0$. We say that b *divides* a (a *is divisible by* b), written $b \mid a$, if there exists $q \in R$ with $a = bq$.

Proposition 1.6.2. *1. $b \mid a$ if and only if $(b) \supset (a)$.*

2. If $a \mid b$, then $a \mid bc$ for all $c \in R$.

3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

4. $(a) = (b)$ if and only if $b = au$ for some $u \in R^\times$.

Definition 1.6.3 (Associates)**.** Two elements a, b in R are *associates* if $(a) = (b)$. We write $a \sim b$.

Definition 1.6.4 (Irreducible element)**.** Let $c \in R$ be a non-zero non-unit element of R. Then c is *irreducible* if whenever $c = xy$ for $x, y \in R$, either $x \in R^\times$ or $y \in R^\times$.

Remark 1.6.5. Fields have no irreducible elements. There are domains that are not fields but have no irreducible elements (for example, the ring of all algebraic integers).

Proposition 1.6.6. *An element $c \in R$ is irreducible if and only if $c \neq 0$, $c \notin R^\times$ and the ideal (c) is maximal in the set of principal ideals different from R.*

Proof. $\Rightarrow$: If $c \in R$ is irreducible and $(c) \subset (a) \neq R$, then $c = ab$ and a is not invertible. Since c is irreducible we must have $b \in R^\times$ and therefore $(c) = (a)$, i.e., (c) is maximal in the set of principal ideals different from R.

$\Leftarrow$: Let $c \neq 0$, $c \notin R^\times$ and the ideal (c) be maximal in the set of principal ideals different from R. Suppose $c = ab$. Then $(c) \subset (a)$ and therefore, either $(a) = R$ or $(c) = (a)$. In the first case $a \in R^\times$ and in the other case $(a) = (c) = (ab)$, hence $R = (b)$ and $b \in R^\times$. Thus, c is irreducible. □

Definition 1.6.7 (Prime element)**.** A non-zero non-unit element $p \in R$ is *prime* if whenever $p \mid xy$, either $p \mid x$ or $p \mid y$.

Proposition 1.6.8. *An element $p \in R$ is prime if and only if (p) is a nonzero prime ideal.*

Proof. A non-zero non-unit element $p \in R$ is *prime* iff $p \mid xy$ implies either $p \mid x$ or $p \mid y$ iff $xy \in (p)$ implies either $x \in (p)$ or $x \in (p)$ iff the ideal (p) is prime. □

Proposition 1.6.9. *Every prime element is irreducible.*

Proof. Suppose $p \in R$ is prime and $p = ab$. Then $p \mid a$ or $p \mid b$, so wlog suppose $p \mid a$ with $a = pc$. We have $p = ab = pbc$, so $bc = 1$. Hence b is a unit, so p is irreducible. □

Example 1.6.10. In $\mathbb{Z}[\sqrt{-5}]$, 2 divides $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ but 2 does not divide either factor, hence 2 is not prime. But 2 is irreducible. Indeed, if $2 = xy$, then $4 = |2|^2 = |x|^2|y|^2$. Note that if $x = a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$, then $|x|^2 = a^2 + 5b^2$ is a positive integer. Also $|x|^2$ is never equal to 2. It follow that either $|x|^2 = 1$ or $|y|^2 = 1$, i.e., either $x = \pm 1$ or $y = \pm 1$ is invertible.

Proposition 1.6.11. *In a PID, every irreducible element is prime.*

Proof. Let $c \in R$ be an irreducible element. Since every ideal in a PID is principal, according to Proposition 1.6.6, the ideal (c) is maximal and hence (c) is a nonzero prime ideal. We conclude that c is prime. □

Example 1.6.12. It follows from Example 1.6.10 that the ring $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

Definition 1.6.13 (Existence of factorization)**.** We say that R *admits factorization* if for any nonzero non-unit $a \in R$, there exist irreducibles $b_1, \ldots, b_n$ such that $a = b_1 \cdots b_n$. In terms of ideals, R admits factorization when we can write $(a) = (b_1)\cdots(b_n)$ as ideals with $b_1, \ldots, b_n$ irreducible.

Definition 1.6.14 (Uniqueness of factorization)**.** We say that R *has unique factorization* if whenever $b_1 \cdots b_n = c_1 \cdots c_m$, where the b_i's and c_j's are irreducible, then $n = m$ and, after suitable rearrangement, b_i and c_i are associates for each i. In terms of ideals, the factorization is unique if whenever $(b_1)\cdots(b_n) = (c_1)\cdots(c_m)$, we have $n = m$ and, after suitable rearrangement, $(b_i) = (c_i)$ for each i.

Proposition 1.6.15. *Let R be a domain. Then*

1. Suppose R admits factorization. If factorization in R is unique, then every irreducible element in R is prime.

2. If every irreducible element in R is prime, then factorization in R is unique.

Proof. 1. Let c be irreducible and suppose $c \mid xy$, so $xy = cd$ for some d. Since R admits factorization, we can write x, y, d as products of irreducibles

$$x = q_1 \cdots q_l, \qquad y = r_1 \cdots r_m, \qquad d = s_1 \cdots s_n,$$

so we have

$$(q_1)\cdots(q_l)(r_1)\cdots(r_m) = (c)(s_1)\cdots(s_n).$$

By uniqueness of factorization, either $(c) = (q_i)$ for some i or $(c) = (r_j)$ for some j. In the first case c divides x, in the second case c divides y, i.e., c is prime.

2. Suppose that

$$(b_1) \cdots (b_n) = (c_1) \cdots (c_m),$$

where b_i and c_j are irreducible. By induction on m we show that $n = m$ and after suitable rearrangement, $(b_i) = (c_i)$ for each $i = 1, \ldots, n$. By assumption, b_n is prime. Since b_n divides the product $c_1 c_2 \cdots c_m$, then b_n divides c_j for some j. We may assume that $j = m$: $c_m = b_n d$ for some d. As c_m and b_n are irreducible we have $d \in R^\times$ and hence $(c_m) = (b_n)$. By cancellation,

$$(b_1) \cdots (b_{n-1}) = (c_1) \cdots (c_{m-1}).$$

By the induction hypothesis, $n - 1 = m - 1$ and after suitable rearrangement, $(b_i) = (c_i)$ for each $i = 1, \ldots, n - 1$. □

Definition 1.6.16 (Unique factorization domain)**.** We say that R is a *unique factorization domain* (UFD) if it admits factorization which is unique.

Corollary 1.6.17. *A domain R is a UFD if and only if R admits factorization and every irreducible element is prime.*

Proposition 1.6.18. *Let R be a commutative ring. The following are equivalent:*

(1) every ideal in R is finitely generated;

(2) every ascending chain of ideals $I_1 \subset I_2 \subset \cdots$ eventually terminates, in the sense that there exists N for which $I_n = I_{n+1}$ for all $n \geq N$.;

(3) every non-empty set of ideals in R has a maximal element by inclusion.

Proof. (1) $\implies$ (2) Let $I_1 \subset I_2 \subset \cdots$ be an ascending chain of ideals and let $I = \bigcup_n I_n$. Since every ideal is finitely generated, we can write $I = (a_1, \ldots, a_m)$ for some $a_1, \ldots, a_m \in R$. For each i, since $a_i \in I$, we have $a_i \in I_{n_i}$ for some n_i. Setting $N = \max(n_1, \ldots, n_m)$, we have $a_i \in I_N$ for all i, so $I = (a_1, \ldots, a_m) \subset I_N \subset I$. Thus $I = I_N = I_{N+1} = \cdots$.

(2) $\implies$ (3) Let S be a non-empty set of ideals and pick $I_1 \in S$. If I_1 is maximal in S, we are done. Otherwise, we can find $I_2 \in S$ with $I_1 \subsetneq I_2$. This process must stop at some maximal I_n, as otherwise, we obtain a strictly ascending chain $I_1 \subsetneq I_2 \subsetneq \cdots$, a contradiction.

(3) $\implies$ (1) Let I be an ideal of R and let $S = \{J \subset R \mid J \subset I \text{ is a finitely generated ideal}\}$. This is non-empty, since it includes 0, so it has a maximal element I'. If $I \neq I'$, then there exists $x \in I \backslash I'$, but then the ideal (I', x) is finitely generated, contained in I, and contains I', contradicting maximality. Hence $I = I' \in S$ is finitely generated. □

Definition 1.6.19 (Noetherian ring)**.** Let R be a commutative ring. We say that R is *noetherian* if all the conditions (1), (2) and (3) of the proposition hold.

Example 1.6.20. Every PID is noetherian.

Proposition 1.6.21. *Noetherian rings admit factorization.*

Proof (noetherian induction). We must show that every principal ideal factors into principal ideals generated by irreducible elements. Let S be the set of all principal ideals, other than 0 and R, which do not have such a factorization. Suppose S is non-empty. Then S has a maximal element (a). If a is irreducible, then it factors as itself, so a is not irreducible. Then we can factor $a = bc$ with b, c not units, so $(a) \subsetneq (b)$ and $(a) \subsetneq (c)$. By maximality of (a) in S, it must be that (b) and (c) are not in S, so b and c admit factorizations into irreducibles, hence so does a, contradiction. □

Corollary 1.6.22. *If R is noetherian domain, then R is a UFD if and only if every irreducible element is prime.*

Corollary 1.6.23. *Every PID is a UFD.*

Definition 1.6.24 (Greatest common divisor)**.** Let $\{a_i\}$ be nonzero elements of R. A *greatest common divisor* (GCD) for $\{a_i\}$ is a principal ideal $(d) \subset R$ such that $(d) \mid (a_i)$ for all i and, if $(c) \mid (a_i)$ for all i, then $(c) \mid (d)$.

Proposition 1.6.25. *The GCD is unique.*

Proof. If (d) and (d') are greatest common divisors of elements $\{a_i\}$, then $(d) \mid (d')$ and $(d') \mid (d)$, hence $(d) = (d')$. □

Proposition 1.6.26. *In a UFD, the GCD of a finite set of elements exists.*

Proof. Let $a_1, \dots, a_n$ be elements of a UFD R, and let $(p_1), \dots, (p_r)$ be all of the primes ideals appearing in the factorizations of $(a_1), \dots, (a_n)$, so that for each i,

$$(a_i) = (p_1)^{e_{i,1}} \cdots (p_r)^{e_{i,r}}, \qquad e_{ij} \geq 0.$$

The GCD is then

$$\gcd(a_1, \dots, a_n) = (p_1)^{\min(e_{1,1}, \dots, e_{n,1})} \cdots (p_r)^{\min(e_{1,r}, \dots, e_{n,r})}.$$

□

1.7 Factorization in polynomial rings

Throughout, let R be a UFD unless stated otherwise.

Definition 1.7.1 (Content)**.** Let $f = a_0 + \cdots + a_n x^n \in R[x]$ be a nonzero polynomial. The *content* of f, denoted $\operatorname{cont} f$, is the GCD of all nonzero coefficients $a_0, \dots, a_n$.

Definition 1.7.2 (Primitive polynomial)**.** A polynomial $f \in R[x]$ is *primitive* if $\operatorname{cont} f = R$.

Proposition 1.7.3. *If $a \in R$ and $f \in R[x]$, then* $\operatorname{cont}(af) = a \operatorname{cont} f$.

Lemma 1.7.4 (Gauss)**.** *If $f, g \in R[x]$ are primitive, then fg is primitive.*

Proof. Let $p \in R$ be prime. Reducing coefficients modulo p, and noting that $(R/pR)[x]$ is a domain since p is prime, if f and g are primitive, then $\overline{f} \neq 0$ and $\overline{g} \neq 0$, so $\overline{f}\overline{g} \neq 0$, showing that p does not divide every coefficient of fg. Hence fg is primitive. □

Corollary 1.7.5. *If $f, g \in R[x]$, then* $\operatorname{cont}(fg) = (\operatorname{cont} f)(\operatorname{cont} g)$.

Definition 1.7.6 (Quotient field)**.** Let R be an integral domain. The *quotient field* (or *field of fractions*) F of R is the set

$$\{(a,b) \in R^2 \mid b \neq 0\}/\sim, \qquad (a,b) \sim (c,d) \iff ad - bc = 0,$$

together with operations

$$(a,b) + (c,d) = (ad + bc, bd), \qquad (a,b) \cdot (c,d) = (ac, bd).$$

The class of (a,b) is written a/b.

Proposition 1.7.7. *1. Addition and multiplication are well-defined, and F is a field with identities $0/1$ and $1/1$.*

2. The map $i : a \mapsto a/1$ is the ring homomorphism $R \to F$.

3. If $f : R \to S$ is a homomorphism such that $f(r) \in S^\times$ for all $r \neq 0$, then there is a unique homomorphism $g : F \to S$ such that $g \circ i = f$.

Lemma 1.7.8. *Let R be a UFD and F be its quotient field and $f, g \in R[x]$. If f is primitive and f divides g in $F[x]$, then f divides g in $R[x]$.*

Proof. Write $g = fh$ for some $h \in F[x]$. Choose a nonzero $a \in R$ such that $ah \in R[x]$. Then by Corollary 1.7.5, $a \operatorname{cont}(g) = \operatorname{cont}(ag) = \operatorname{cont}(f) \operatorname{cont}(ah) = \operatorname{cont}(ah)$ since f is primitive. It follows that all coefficients of ah are divisible by a, hence $h \in R[x]$. □

Lemma 1.7.9. *Let R be a UFD and F be its quotient field. Then a nonconstant polynomial $f \in R[x]$ is irreducible if and only if f is primitive and f is irreducible in $F[x]$.*

Proof. $\Rightarrow$: Clearly, f is primitive. Write $f = gh$ in $F[x]$ for some nonconstant $g, h \in F[x]$. Scaling, we may assume that $g \in R[x]$ is primitive. By Lemma 1.7.8, $h \in R[x]$, i.e., f is not irreducible in $R[x]$.

$\Leftarrow$: Let $f = gh$ in $R[x]$. As f is irreducible in $F[x]$, one of g and h, say g, is constant. We have $R = \operatorname{cont}(f) = g \operatorname{cont}(h)$, hence g is invertible in R and therefore, f irreducible in $R[x]$. □

Theorem 1.7.10. *If R is a UFD, then $R[x]$ is a UFD.*

Proof. We first show that $R[x]$ admits factorization. We show that a nonzero polynomial $f \in R[x]$ is a product of irreducibles by induction on $n = \deg(f)$. If $n = 0$, then $f \in R$ and we are done since R is a UFD. In general, we may assume that f is primitive. If f is not irreducible in $R[x]$, it is the product of two polynomials g and h in $R[x]$ of degree less than n. By induction, g and h and hence f are products of irreducibles.

By Corollary 1.6.17 it suffices to show that every irreducible polynomial $f \in R[x]$ is prime. Clearly, f is primitive. Let f divide gh for some $g, h \in R[x]$. Then f divides gh in $F[x]$. Since $F[x]$ is a UFD (even PID), and by Lemma 1.7.9, f is irreducible over F, the polynomial f divides one of g and h in $F[x]$, say $f|g$. By Lemma 1.7.8, f divides g in $R[x]$, hence f is prime. □

To factor $f \in R[x]$, let F be the quotient field of R and factor $f = p_1 \cdots p_m$ in $F[x]$ with $p_i \in F[x]$ irreducible. For each i, find $\alpha_i \in F^\times$ such that $q_i = \alpha_i f_i \in R[x]$ is primitive. Then $f = \beta q_1 \cdots q_m$ with the $q_i \in R[x]$ primitive, hence irreducible over R. The product $q_1 \cdots q_m$ is primitive by Gauss Lemma. Since $q_1 \cdots q_m \mid f$ in $F[x]$, it follows from Lemma 1.7.8 that $\beta \in R$. Finally, factor β in R. Thus the irreducibles in $R[x]$ are the irreducible constants and primitive polynomials in $R[x]$ that are irreducible in $F[x]$.

Theorem 1.7.11 (Eisenstein criterion)**.** *Let R be a UFD and F be its quotient field. Let $f = a_0 + \cdots + a_n x^n \in R[x]$. Let $p \in R$ be a prime element such that*

1. *$p \nmid a_n$;*
2. *$p \mid a_i$ for all $i < n$;*
3. *$p^2 \nmid a_0$.*

Then f is irreducible in $F[x]$.

Proof. Let c be the content of f and write $f = cf'$ with $f' \in R[x]$ primitive. Since $c \mid a_n$, which is not divisible by p, we also have that $p \nmid c$. Thus the conditions hold for f', so we can assume that f is primitive. By Gauss's lemma, it is enough to show that f is irreducible in $R[x]$. Let $f = gh$ be a non-trivial factorization with $g, h \in R[x]$. Consider the map $R[x] \to (R/pR)[x] \subset K[x]$ given by reduction of coefficients modulo p, where K is the quotient field of R/pR. Then $\overline{f} = \overline{a_n} x^n = \overline{g}\overline{h}$, so the constant terms of g and h are both divisible by p (factorization over $K[x]$ is unique). Then $p^2 \mid a_0$, a contradiction. □

Example 1.7.12.

1. $x^5 - 12 \in \mathbb{Q}[x]$ is irreducible by taking $p = 3$.
2. For p a prime integer, $x^{p-1} + \cdots + 1 \in \mathbb{Q}[x]$ is irreducible by letting $x = y + 1$ and taking the prime to be p in Eisenstein.

1.8 Factorization in quadratic fields

Definition 1.8.1 (Quadratic field)**.** Let $1 \neq d \in \mathbb{Z}$ be square-free. Then

$$K = \mathbb{Q}(\sqrt{d}) = \left\{ x + y\sqrt{d} \mid x, y \in \mathbb{Q} \right\}$$

is a *quadratic field.*

For the rest of this section, we will assume that $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field. It contains $\mathbb{Z}[\sqrt{d}]$ as a subring.

Definition 1.8.2 (Conjugate)**.** The *conjugate* of $x + y\sqrt{d} \in K$ is $x - y\sqrt{d}$.

Proposition 1.8.3. *Let $\alpha, \beta \in K$. Then*

1. *$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$;*
2. *$\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$;*

3. *$\overline{\overline{\alpha}} = \alpha$;*

4. *$\overline{\alpha} = \alpha$ if and only if $\alpha \in \mathbb{Q}$.*

Definition 1.8.4 (Trace / norm)**.** Let $\alpha = x + y\sqrt{d} \in K$.

1. The *trace* of α is $\operatorname{tr}(\alpha) = \alpha + \overline{\alpha} = 2x$.
2. The *norm* of α is $N(\alpha) = \alpha\overline{\alpha} = x^2 - dy^2$.

Theorem 1.8.5. *Let $\alpha, \beta \in K$. Then*

$$\operatorname{tr}(\alpha + \beta) = \operatorname{tr}(\alpha) + \operatorname{tr}(\beta), \qquad N(\alpha\beta) = N(\alpha)N(\beta).$$

For any $\alpha \in K$, we have

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - \operatorname{tr}(\alpha)x + N(\alpha) \in \mathbb{Q}[x].$$

However, the coefficients may not be in $\mathbb{Z}$.

Definition 1.8.6 (Algebraic integer)**.** We say that $\alpha \in K$ is an *(algebraic) integer* if $\operatorname{tr}(\alpha), N(\alpha) \in \mathbb{Z}$.

Example 1.8.7. 1. If $\alpha \in \mathbb{Z}[\sqrt{d}]$, then $\operatorname{tr}(\alpha)$ and $N(\alpha)$ are in $\mathbb{Z}$, so α is an integer.

2. If $d \equiv 1 \pmod 4$, then $\alpha = (1 + \sqrt{d})/2$ is an integer.

Notation. The set of integers in K is denoted $\mathcal{O}_K$.

Theorem 1.8.8. *If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field, then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[(1 + \sqrt{d})/2] & d \equiv 1 \pmod 4. \end{cases}$$

In particular, $\mathcal{O}_K$ is a subring of K.

Proof. Suppose $\alpha = x + y\sqrt{d} \in K$ is an integer. Then $\operatorname{tr}(\alpha) = 2x$ and $N(\alpha) = x^2 - dy^2$ are ordinary integers, so $x \in \mathbb{Z}$ or $x = c/2$ for $c \in \mathbb{Z}$ odd. Since d is square-free, if $dy^2 \in \mathbb{Z}$ and $y \in \mathbb{Q}$, then $y \in \mathbb{Z}$. Hence if $x \in \mathbb{Z}$, we have $y \in \mathbb{Z}$.

Suppose $x = c/2$ for c odd. Since $x^2 - dy^2 \in \mathbb{Z}$, we have $c^2 - d(2y)^2 \in 4\mathbb{Z}$, so $d(2y)^2 \in \mathbb{Z}$, hence $2y \in \mathbb{Z}$. If $y \in \mathbb{Z}$, then $c^2 - d(2y)^2 \equiv c^2 \not\equiv 0 \pmod 4$, a contradiction. If y is half an odd integer, then we must have $d \equiv 1 \pmod 4$. □

Notation. Let

$$\omega = \begin{cases} \sqrt{d} & d \equiv 2, 3 \pmod 4, \\ (1 + \sqrt{d})/2 & d \equiv 1 \pmod 4, \end{cases}$$

so that $\mathcal{O}_K = \mathbb{Z}[\omega]$.

Theorem 1.8.9. *Let $\alpha \in K$. Then $\alpha \in \mathcal{O}_K$ if and only if it is a root of a monic polynomial $x^2 + mx + n \in \mathbb{Z}[x]$.*

Proof. ($\Longrightarrow$) If $\alpha \in \mathcal{O}_K$, then $(x-\alpha)(x-\overline{\alpha})$ will do.

($\Longleftarrow$) If $\alpha \in \mathbb{Q}$, then write $\alpha = a/b$ with $\gcd(a,b)=1$. Then

$$\left(\frac{a}{b}\right)^2 + m\left(\frac{a}{b}\right) + n = 0 \implies a^2 = -mab - nb^2,$$

so any prime divisor of b must also divide a, hence $b = \pm 1$ and $\alpha = a/b \in \mathbb{Z}$.

If $\alpha \notin \mathbb{Q}$ and $\alpha^2 + m\alpha + n = 0$, then since we also have $\alpha^2 - \operatorname{tr}(\alpha)\alpha + N(\alpha) = 0$, we get

$$(m + \operatorname{tr}(\alpha))\alpha + (n - N(\alpha)) = 0.$$

Since $\alpha \notin \mathbb{Q}$, this means $m + \operatorname{tr}(\alpha) = 0$ and $n - N(\alpha) = 0$, from which it follows that $\operatorname{tr}(\alpha)$ and $N(\alpha)$ are ordinary integers.

□

Theorem 1.8.10. *For $m \in \mathbb{Z}$ and $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, then $m \mid \alpha$ in $\mathbb{Z}[\omega]$ if and only if $m \mid a$ and $m \mid b$ in $\mathbb{Z}$.*

Theorem 1.8.11. *$\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ and $K = \{\alpha/\beta \mid \alpha, \beta \in \mathcal{O}_K\}$.*

Theorem 1.8.12. *If $\alpha \in \mathcal{O}_K$, then $\overline{\alpha} \in \mathcal{O}_K$.*

Theorem 1.8.13. *Let K be a quadratic field. Then*

$$\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid N(\alpha) = \pm 1\}$$

and $\mathcal{O}_K^\times \cap \mathbb{Q} = \{\pm 1\}$.

Proof. Suppose $\alpha \in \mathcal{O}_K^\times$, so there exists $\beta \in \mathcal{O}_K^\times$ such that $\alpha\beta = 1$. Then $N(\alpha\beta) = N(\alpha)N(\beta) = 1$ and $N(\alpha), N(\beta) \in \mathbb{Z}$, so $N(\alpha) \in \mathbb{Z}^\times = \{\pm 1\}$. Conversely, if $N(\alpha) = \alpha\overline{\alpha} = 1$, then α is a unit with inverse $\overline{\alpha}$.

If $\alpha \in \mathcal{O}_K^\times \cap \mathbb{Q}$, then $N(\alpha) = \alpha^2 = \pm 1$, so $\alpha = \pm 1$. □

1.9 The spectrum of a commutative ring

Let R be a commutative ring.

Definition 1.9.1 (Spectrum)**.** The *spectrum* of R, denoted $\operatorname{Spec} R$, is the set of prime ideals of R.

Notation. For any subset $S \subset R$, let

$$V(S) = \{P \in \operatorname{Spec} R \mid S \subset P\}.$$

Definition 1.9.2 (Radical of an ideal)**.** Let I be an ideal of R. The *radical* of I is

$$\sqrt{I} = \{x \in R \mid x^n \in I \text{ for some } n\}.$$

Lemma 1.9.3. *1. If I is the ideal generated by S, then $V(S) = V(I) = V(\sqrt{I})$.*

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

3. *If $\{I_j\}_{j\in J}$ is a family of ideals in R, then $\cap_j V(I_j) = V(\sum_j I_j)$.*

4. *$V(I_1) \cup V(I_2) = V(I_1 \cap I_2) = V(I_1 I_2)$.*

Proof. 1. Since $S \subset I$, we have $V(I) \subset V(S)$. Any ideal containing S contains the ideal I generated by S, so $V(S) \subset V(I)$.

Since $I \subset \sqrt{I}$, we have $V(\sqrt{I}) \subset V(I)$. Suppose $P \in \operatorname{Spec} R$ contains I. If $x \in \sqrt{I}$, then there exists n for each $x^n \in I \subset P$, so $x \in P$. Hence $\sqrt{I} \subset P$, so we get $V(I) \subset V(\sqrt{I})$.

2. Trivial.

3. Let $P \in \operatorname{Spec} R$ and suppose first that $P \in \bigcap_j V(I_j)$. Then $I_j \subset P$ for each $j \in J$, so $\sum_j I_j \subset P$, hence $P \in V(\sum_j I_j)$. Conversely, if $P \in V(\sum_j I_j)$, then $P \supset \sum_j I_j \supset I_j$ for each j, so $P \in \bigcap_j V(I_j)$.

4. Suppose $P \in V(I_1) \cup V(I_2)$. Then either $I_1 \subset P$ or $I_2 \subset P$, so in either case, P contains $I_1 \cap I_2$, i.e. $P \in V(I_1 \cap I_2)$. Conversely, if $P \in V(I_1 \cap I_2)$ and $I_1 \not\subset P$, then let $x \in I_1 \backslash P$. For any $y \in I_2$, we have $xy \in I_1 I_2 \subset I_1 \cap I_2 \subset P$, so $y \in P_2$. Hence $I_2 \subset P$, so $P \in V(I_1) \cup V(I_2)$.

To see that these sets are both equal to $V(I_1 I_2)$, run the same proof.

□

Definition 1.9.4 (Zariski topology)**.** The *Zariski topology* is the topology on $\operatorname{Spec} R$ defined by taking the closed sets to be the sets $V(I)$ for ideals $I \subset R$.

Example 1.9.5. 1. If F is a field, then $\operatorname{Spec} F = \{0\}$ has one point.

2. $\operatorname{Spec} \mathbb{Z} = \{p\mathbb{Z} \mid p \in \mathbb{Z} \text{ a prime number or } 0\}$.

3. If R is a commutative ring and $I \subset R$ is an ideal, then there is a bijection $V(I) \to \operatorname{Spec}(R/I)$ given by $P \mapsto P/I$.

4. Since $\mathbb{C}[x]$ is a PID, prime ideals are in bijection with monic irreducible polynomials in $\mathbb{C}[x]$. Since $\mathbb{C}$ is algebraically closed, the monic irreducible polynomials are precisely in monic irreducibles $x - \alpha$ for $\alpha \in \mathbb{C}$. Thus $\operatorname{Spec} \mathbb{C}[x] = \{x - \alpha \mid \alpha \in \mathbb{C}\} \cup \{0\}$. As in $\operatorname{Spec} \mathbb{Z}$, every point except for 0 is closed, and 0 is generic in the sense that its closure is $\operatorname{Spec} \mathbb{C}[x]$. There is a bijection $\operatorname{Spec} \mathbb{C}[x] \to \mathbb{C} \cup \{*\}$ where $x - \alpha \mapsto \alpha$ and $0 \mapsto *$.

If R is a commutative ring and $P \in \operatorname{Spec} R$, there is a canonical map $\pi_P : R \to R/P$. In this example, if $P = (x - \alpha) \in \operatorname{Spec} \mathbb{C}[x]$, denote π_P by π_α. There is a map $\mathbb{C}[x] \to \mathbb{C}$ given by $f \mapsto f(\alpha)$, which has kernel precisely $(x - \alpha) = P$, so this map descends to an isomorphism $\mathbb{C}[x]/(x - \alpha) \to \mathbb{C}$ via π_α.

Proposition 1.9.6. *If R is a commutative ring, then* $\operatorname{Nil} R$ *is the intersection of all prime ideals.*

Notation. Given $f \in R$, let $D(f) = \operatorname{Spec} R \backslash V((f))$ be the largest open set not containing f.

Lemma 1.9.7. *$\{D(f)\}_{f\in R}$ is a basis for the Zariski topology.*

Proof. Let U be an open subset of $\operatorname{Spec} R$, i.e. $U = \operatorname{Spec} R \backslash V(I)$ for some ideal $I \subset R$. We claim that $U = \bigcup_{f\in I} D(f)$. Since $(f) \subset I$ for all $f \in I$, we have $V((f)) \supset V(I)$, so $U \supset D(f)$ for all $f \in I$, i.e. $U \supset \bigcup_{f\in I} D(f)$. Conversely, if $P \in U$, so that $I \not\subset P$, then there exists $f \in I \backslash P$, so $P \in D(f)$, and hence $U \subset \bigcup_{f\in I} D(f)$. □

Lemma 1.9.8. *$\sqrt{I}$ is the intersection of all prime ideals containing I.*

Proof. Let $\pi : R \to R/I$ be the canonical map. Then

$$\sqrt{I} = \pi^{-1}(\mathrm{Nil}(R/I)) = \pi^{-1}\left(\bigcap_{\overline{P}\in\mathrm{Spec}(R/I)} \overline{P}\right) = \bigcap_{P\supset I} P$$

by the earlier bijection. □

Proposition 1.9.9. 1. *$D(f) \cap D(g) = D(fg)$;*

2. *$D(f) = \emptyset$ if and only if $f \in \mathrm{Nil}\, R$;*

3. *$D(f) = \mathrm{Spec}\, R$ if and only if $f \in R^\times$;*

4. *$D(f) = D(g))$ if and only if $\sqrt{(f)} = \sqrt{(g)}$.*

Proof. 1. Immediate from $V((f)) \cup V((g)) = v((f)(g)) = V((fg))$.

2. $f \in \mathrm{Nil}\, R$ if and only if $f \in P$ for all prime P if and only if $D(f) = \emptyset$.

3. $f \in R^\times$ if and only if $(f) = R$ if and only if $f \notin P$ for all $P \in \mathrm{Spec}\, R$ if and only if $D(f) = \mathrm{Spec}\, R$.

4. Equivalent to showing that $V((f)) = V((g))$ if and only if $\sqrt{(f)} = \sqrt{(g)}$. If $\sqrt{(f)} = \sqrt{(g)}$, then $V((f)) = V(\sqrt{(f)}) = V(\sqrt{(g)} = V((g))$. Conversely, suppose $V((f)) = V((g))$. Then the intersections of the prime ideals containing (f) and (g) are equal, and these are precisely the radicals of (f) and (g).

□

Proposition 1.9.10. $\mathrm{Spec}\, R$ *is compact.*

Proof. Let $\{U_i\}_{i\in I}$ be an open cover of $\mathrm{Spec}\, R$. Since the sets $\{D(f)\}$ form a basis for $\mathrm{Spec}\, R$, it suffices to suppose $U_i = D(f_i)$ for each i. Then

$$\mathrm{Spec}\, R = \bigcup_{i\in I} D(f_i) = \bigcup_{i\in I} \mathrm{Spec}\, R \backslash V(f_iR) = \mathrm{Spec}\, R \backslash \bigcap_{i\in I} V(f_iR) = \mathrm{Spec}\, R \backslash V\left(\sum_{i\in I} f_iR\right),$$

so $V(\sum_i f_iR) = \emptyset$, meaning that $\sum_i f_iR = R$. Hence $1 = f_1g_1 + \cdots + f_ng_n$ for some $f_1, \ldots, f_n, g_1, \ldots, g_n \in R$ with $f_1, \ldots, f_n \in \{f_i\}$, so $D(f_1), \ldots, D(f_n)$ cover $\mathrm{Spec}\, R$. □

Definition 1.9.11 (Irreducibility of topological spaces)**.** A topological space X is *irreducible* if every pair of non-empty open sets has non-empty intersection, or equivalently, every non-empty open subset is dense.

Proposition 1.9.12. $\mathrm{Spec}\, R$ *is irreducible if and only if* $\mathrm{Nil}\, R \in \mathrm{Spec}\, R$*.*

Proof. ($\implies$) Suppose $f, g \notin \mathrm{Nil}\, R$. There exist prime ideals P, Q such that $P \in D(f)$ and $Q \in D(g)$, so $D(f)$ and $D(g)$ are non-empty. Therefore, $D(f) \cap D(g) = D(fg) \neq \emptyset$, so $fg \notin \mathrm{Nil}\, R$.

($\Longleftarrow$) Reverse the logic.

□

Corollary 1.9.13. *If R is a domain, then* $\operatorname{Spec} R$ *is irreducible.*

1.10 Spec as a functor

Proposition 1.10.1. *Let R, S be commutative rings and $\varphi : R \to S$ be a homomorphism. Then φ induces a set function* $\operatorname{Spec}\varphi : \operatorname{Spec} S \to \operatorname{Spec} R$*.*

Proof. If $P \in \operatorname{Spec} S$, then $\varphi^{-1}(P) \in \operatorname{Spec} R$, so we take $\operatorname{Spec}\varphi(P) = \varphi^{-1}(P)$. □

Theorem 1.10.2. $\operatorname{Spec}\varphi : \operatorname{Spec} S \to \operatorname{Spec} R$ *is continuous.*

Proof.

$$\operatorname{Spec}(\varphi)^{-1}(D(f)) = \{Q \in \operatorname{Spec} S \mid f \in \varphi^{-1}(Q)\} = \{Q \in \operatorname{Spec} S \mid \varphi(f) \notin Q\} = D(\varphi(f)).$$

□

Corollary 1.10.3. Spec *defines a contravariant functor* ***CRing*** $\to$ ***Top****.*

Example 1.10.4.

1. Let F be a field with non-trivial automorphisms. Then distinct automorphisms of F induce the same map on $\operatorname{Spec} F$, so Spec is not faithful.

2. Let $\varphi : \operatorname{Spec}(\mathbb{C}[x]) \to \operatorname{Spec}(\mathbb{C}[x])$ be the identity map, except for swapping (x) and $(x-1)$. Then φ is continuous, but is not induced by a ring homomorphism as described, so Spec is not full.

Lemma 1.10.5. *Let R be a commutative ring and $I, J \subset R$ be ideals. Then $V(I) \subset V(J)$ if and only if $\sqrt{I} \supset \sqrt{J}$.*

Proof. ($\Longrightarrow$) If $V(I) \subset V(J)$, then

$$\sqrt{I} = \bigcap_{P \in V(I)} P \supset \bigcap_{P \in V(J)} P = \sqrt{J}.$$

($\Longrightarrow$) If $\sqrt{I} \supset \sqrt{J}$ and $P \in V(I)$, then

$$P \supset \sqrt{I} \supset \sqrt{J} \supset J,$$

so $P \in V(J)$.

□

Proposition 1.10.6. *Let $\varphi : A \to B$ be a ring homomorphism and let $\varphi^* = \operatorname{Spec}(\varphi) : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$.*

1. *If $I \subset A$ is an ideal, then $(\varphi^*)^{-1}(V(I)) = V(\varphi(I)B)$.*

2. *If $J \subset B$ is an ideal, then* $\overline{\varphi^*(V(B))} = V(\varphi^{-1}(J))$.

3. *If φ is surjective, then φ^* is a homeomorphism onto the closed subset* $V(\operatorname{Ker}\varphi)$ *of* $\operatorname{Spec}(A)$.

4. *If φ is injective, then* $\varphi^*(\operatorname{Spec}(B))$ *is a dense subset of* $\operatorname{Spec}(A)$. *More generally,* $\varphi^*(\operatorname{Spec}(B))$ *is dense in* $\operatorname{Spec}(A)$ *if and only if* $\operatorname{Ker}\varphi \subset \operatorname{Nil}(A)$.

Corollary 1.10.7. $\operatorname{Spec}(A)$ *and* $\operatorname{Spec}(A/\operatorname{Nil}(A))$ *are naturally homeomorphic.*

Proposition 1.10.8. *Let* $A = \prod_i A_i$ *for commutative rings* $A_1, \ldots, A_n$. *Then there is a homeomorphism* $\coprod_i \operatorname{Spec}(A_i) \to \operatorname{Spec}(A)$ *such that each* $\operatorname{Spec}(A_i)$ *is mapped onto an open subset* $D(f_i)$ *of* $\operatorname{Spec}(A)$. *Moreover,* $\operatorname{Spec}(A_i)$ *is mapped onto a closed subset* $V(J_i)$, *so* $\operatorname{Spec}(A)$ *is disconnected.*

Proposition 1.10.9. *Let A be a commutative ring. The following are equivalent:*

(1) $\operatorname{Spec}(A)$ *is disconnected;*

(2) $A \cong A_1 \times A_2$ *for some non-zero* A_1, A_2;

(3) A contains an idempotent other than 0 or 1.

Let X be a compact Hausdorff space and $C(X)$ be the ring of real-valued continuous functions on X. Then $M_x = \{f \in C(X) \mid f(x) = 0\}$ is a maximal ideal of X, and if $\tilde{X} = m - \operatorname{Spec}(C(X))$, then $\mu : X \to \tilde{X}$ given by $x \mapsto M_x$ is a homeomorphism.

2 Modules

2.1 Definitions and basic properties

Definition 2.1.1 (Module)**.** Let R be a ring. A *left R-module* is an (additive) abelian group M together with a left scalar multiplication $R \times M \to M$ such that

(i) $r(m+n) = rm + rn$ for all $r \in R$ and $m, n \in M$;

(ii) $(r+s)m = rm + sm$ for all $r, s \in R$ and $m \in M$;

(iii) $1 \cdot m = m$ for all $m \in M$;

(iv) $r(sm) = (rs)m$ for all $r, s \in R$ and $m \in M$.

Right R-modules are defined analogously.

Remark 2.1.2. Let M be a left R-module, and attempt to define a right scalar multiplication $M \times R \to M$ by $mr := rm$. This does not generally define a right R-module. However, if R is a commutative ring, then this does become a valid right scalar multiplication, and we have an equivalence of left and right R-modules. In other words, modules over commutative rings can be regarded as "two-sided modules."

Proposition 2.1.3. *1. $0 \cdot m = 0$ for all $m \in M$ and $r \cdot 0 = 0$ for all $r \in R$.*

2. $(-r)m = -(rm) = r(-m)$ for all $m \in M$ and $r \in R$.

Example 2.1.4. 1. If F is a field, then F-modules are vector spaces over F.

2. $\mathbb{Z}$-modules are abelian groups.

3. Let R° be the opposite ring of R. Then (left) R-modules are (right) R°-modules.

4. (Left) ideals are also (left) R-modules. In particular, R itself is a left R-module and a right R-module. Conversely, if $S \subset R$ is a left R-module, then S is a left ideal of R.

5. If M is a (left) R-module and $I \subset R$ is an ideal such that $IM = 0$, then M has the structure of an R/I-module via $(r+I)m = rm$.

6. Let $f : R \to S$ be a ring homomorphism and let M be a left S-module. Then we can make M a left R-module by defining $rm = f(r)m$.

7. Let M be an abelian group. Then M is a left $(\operatorname{End} M)$-module by $f \cdot m = f(m)$.

8. Let M be a left R-module. There is a ring homomorphism $R \to \operatorname{End} M$ which is given by $r \mapsto (m \mapsto rm)$, i.e. r is sent to its corresponding left multiplication map. Conversely, if M is an abelian group and $f : R \to \operatorname{End} M$ is a ring homomorphism, then we can pull back the left $(\operatorname{End} M)$-module structure on M to make M a left R-module.

From the last three examples, we obtain the following result.

Proposition 2.1.5 (Universal property of the endomorphism ring)**.** *Let M be an abelian group. There is a functor $\textbf{\textit{Ring}}^{\mathrm{op}} \to \textbf{\textit{Set}}$ sending R to the set of all left R-module structures on M, and this functor is corepresented by* $\operatorname{End} M$.

Definition 2.1.6 (Module homomorphism)**.** Let R be a ring and let M, N be (left) R-modules. An *R-module homomorphism* $M \to N$ is a homomorphism of abelian groups $f : M \to N$ such that $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$.

Notation. The category of left R-modules is denoted R**-Mod** and the category of right R-modules is denoted **Mod-**R.

Definition 2.1.7 (Submodule)**.** A subgroup $N \subset M$ is an *R-submodule* of M if $RN \subset N$.

Definition 2.1.8 (Kernel / image)**.** Let M, N be (left) R-modules and $f : M \to N$ be an R-module homomorphism. The *kernel* of f is $\operatorname{Ker} f = f^{-1}(0)$ and the *image* of f is $\operatorname{Im} f = f(M)$.

Proposition 2.1.9. $\operatorname{Ker} f \subset M$ *and* $\operatorname{Im} f \subset N$ *are R-submodules.*

Definition 2.1.10 (Quotient module)**.** Let $N \subset M$ be a submodule. The *quotient module* (or *factor module*) is the quotient group M/N with scalar multiplication $r(m + N) = rm + N$.

Theorem 2.1.11 (Isomorphism theorems)**.**

1. *If $f : M \to N$ is an R-module homomorphism, then $\overline{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$ is an isomorphism.*
2. *If $N, P \subset M$ are R-submodules, then $(N + P)/P \cong N/(N \cap P)$.*
3. *If $N \subset P \subset M$ are R-submodules, then $(M/N)/(P/N) \cong M/P$.*

Theorem 2.1.12 (Correspondence theorem)**.** *If $N \subset M$ is an R-submodule and $q : M \to M/N$ is the quotient map, then there is a bijection*

$$\begin{aligned} \{R\text{-submodules of } M/N\} &\longleftrightarrow \{R\text{-submodules of } M \text{ containing } N\}, \\ \overline{P} &\longmapsto q^{-1}(\overline{P}), \\ P/N &\to P. \end{aligned}$$

2.2 Exact sequences of modules

Let $\{M_i \mid i \in I\}$ be a family of (left) R-modules. The product module $\prod_i M_i$ is the Cartesian product with componentwise operations, and this agrees with the categorical definition of the product.

Definition 2.2.1 (Direct sum)**.** Let $\{M_i \mid i \in I\}$ be a family of (left) R-modules. Their *direct sum* is

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

This is a submodule of $\prod_i M_i$.

Proposition 2.2.2. *The direct sum of modules is the categorical coproduct of R-modules, i.e.*

$$\bigoplus_{i \in I} M_i = \coprod_{i \in I} M_i.$$

Proof. Let $M = \bigoplus_i M_i$ and for $i \in I$, define $f_i : M_i \to M$ by $f_i(m) = (m_j)$ with $m_j = m$ if $j = i$ and $m_j = 0$ otherwise. Let $g_i : M_i \to N$ be homomorphisms for some R-module N. We must show that there is a unique $h : M \to N$ for which $h \circ f_i = g_i$ for each i. Let $(m_i) \in M$. Then we have $(m_i) = \sum_i f_i(m_i)$. (This is a valid equality since $m_i = 0$ for all but finitely many i, so the sum is finite.) Hence any $h : M \to N$ with $h \circ f_i = g_i$ for each i must satisfy

$$h((m_i)) = \sum_{i\in I}(h \circ f_i)(m_i) = \sum_{i\in I} g_i(m_i), \tag{†}$$

so if h exists, it is unique. For existence, we define h by (†). □

For given (left) R-modules M, N, the hom-set $\operatorname{Hom}_R(M, N)$ forms an abelian group, so together with the existence of products and coproducts, kernels and cokernels and the First Isomorphism Theorem, R-**Mod** and **Mod**-R are abelian categories.

As in any abelian category, there is the concept of an exact sequence. In particular, a short exact sequence is an exact sequence

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0,$$

so f is injective, g is surjective, and $\operatorname{Ker} g = \operatorname{Im} f$. Then we can identify N with $\operatorname{Im} f$, which gives

$$M/N = M/\operatorname{Im} f = M/\operatorname{Ker} g \cong \operatorname{Im} g = P.$$

If $N \subset M$ is a submodule, then

$$0 \longrightarrow N \hookrightarrow M \xrightarrow{\pi} M/N \longrightarrow 0$$

is a *standard* short exact sequence.

Given a ring R, there is a category $\mathcal{C}(R)$ of short exact sequences whose objects are short exact sequences and whose morphisms are triples of R-module homomorphisms for which the diagram commutes.

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, "u"] & M \arrow[r] \arrow[d, "v"] & P \arrow[r] \arrow[d, "w"] & 0 \\
0 \arrow[r] & N' \arrow[r] & M' \arrow[r] & P' \arrow[r] & 0
\end{tikzcd}$$

The morphism (u, v, w) is an isomorphism in $\mathcal{C}(R)$ if and only if u, v, w are isomorphisms in R-**Mod**. For example, every short exact sequence is isomorphic to a standard short exact sequence.

Theorem 2.2.3. *Let $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ be a short exact sequence of (left) R-modules. Then the following are equivalent:*

(1) (right split) there exists $g' : P \to M$ such that $g \circ g' = \mathrm{id}_P$;

(2) (left split) there exists $f' : M \to N$ such that $f' \circ f = \mathrm{id}_N$;

(3) this short exact sequence is isomorphic to $0 \to N \to N \oplus P \to P \to 0$.

Proof. (1) $\implies$ (2) Let $h : M \to M$ be given by $h = \mathrm{id}_M - g' \circ g$. Then $g \circ h = g - g \circ g' \circ g = 0$, so $\operatorname{Im} h \subset \operatorname{Ker} g = \operatorname{Im} f = N$, so we can view h as a homomorphism $f' : M \to N$ with $f'(m) = h(m)$. Then $(f' \circ f)(n) = f'(n) = h(n) = n - g'(g(n)) = n$.

(2) $\implies$ (3) Given f' as in (2), the isomorphisms are shown below.

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "f"] \arrow[d, "1_N"] & M \arrow[r, "g"] \arrow[d, "{(f',g)}"] & P \arrow[r] \arrow[d, "1_P"] & 0 \\
0 \arrow[r] & N \arrow[r] & N \oplus P \arrow[r] & P \arrow[r] & 0
\end{tikzcd}$$

(3) $\implies$ (1) Obvious. □

A short exact sequence is *split* if any of these conditions hold.

Example 2.2.4. Consider the sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0.$$

If $n = 0$, then the sequence is not exact. If $n = \pm 1$, then the sequence is a split exact sequence. Otherwise, the sequence is exact but not split.

The functors $\operatorname{Hom}_R(X, -)$ and $\operatorname{Hom}_R(-, X)$ are additive. In particular, there is a canonical isomorphism (of groups)

$$\operatorname{Hom}_R\left(\bigoplus_{i=1}^{n} M_i, \bigoplus_{j=1}^{m} N_j\right) \cong \{\operatorname{Hom}_R(M_i, N_j)\}$$

with the right being an (additive) group of matrices and the composition of homomorphisms being given by matrix multiplication.

2.3 Free, projective, and injective modules

Definition 2.3.1 (Basis / free module)**.** Let M be a (left) R-module. A subset $X \subset M$ is a *basis* for M if every element $m \in M$ can be uniquely written in the form $m = \sum_x r_x x$ for $r_x \in R$ with all but finitely many equal to zero. We say that M is *free* if M has a basis.

Example 2.3.2. 1. If R is a field, every R-module is free.

2. R is free as an R-module with basis $\{1\}$. More generally, $R^n = R \oplus \cdots \oplus R$ is free with basis $\{e_1, \ldots, e_n\}$ (defined in the obvious way).

3. Let X be a set and define $R^X = \prod_x R = \{\text{functions } X \to R\}$. This may not be free, but $R^{(X)} := \bigoplus_x R \subset R^X$ is free with basis $\{e_x\}$ defined by $e_x(x') = \delta_{x,x'}$. The module $R^{(X)}$ consists of all functions $f \in R^X$ such that $f(x) = 0$ for almost all $x \in X$. Identifying x with the function e_x we may assume that $X \subset R^{(X)}$. Every element in $R^{(X)}$ can be written in the form $\sum_{x \in X} r_x x$ for a unique family $(r_x)_{x \in X}$ of elements in R, almost all zero.

Suppose M is free and $X \subset M$ is a basis. Then $R^{(X)} \to M$ given by $[f : X \to R] \mapsto \sum_x f(x) \cdot x$ is an isomorphism, so $M \cong R^{(X)}$.

Proposition 2.3.3. $R^{(X)} \oplus R^{(Y)} \cong R^{(X \sqcup Y)}$.

Theorem 2.3.4 (Universal property of free modules)**.** *Let M be a free R-module with basis $X \subset M$. If N is another R-module, then any set function $X \to N$ extends to a unique homomorphism $M \to N$.*

Proof. We may assume that $M = R^{(X)}$. A function $g : X \to N$ extends uniquely to an R-module homomorphism $R^{(X)} \to N$ taking a function $f : X \to R$ in $R^{(X)}$ to $\sum_{x \in X} f(x)g(x)$. □

Categorically, this tells us that the forgetful functor R-**Mod** → **Set** is a right adjoint to the functor $X \mapsto R^{(X)}$.

Elements of $\operatorname{Hom}_R(R^n, R^m)$ can be written as $m \times n$ matrices in R.

Remark 2.3.5. There are rings R for which $R^n \cong R^m$ as R-modules even when $n \neq m$, so dimension is not well-defined in general. However, when R is commutative, $R^n \cong R^m$ does imply that $n = m$.

Proposition 2.3.6. *Every left R-module is isomorphic to a quotient of a free module.*

Proof. Let X be a generating set of a left R-module M (for example, we can take $X = M$). The inclusion of X into M extends to a surjective R-module homomorphism $h : R^{(X)} \to M$. We have $M \simeq R^{(X)}/\operatorname{Ker}(h)$. □

Proposition 2.3.7. *Let P be a (left) R-module. The following are equivalent:*

(1) the functor $\operatorname{Hom}_R(P, -)$ *is exact;*

(2) for every diagram of the form below, there exists $h : P \to B$ such that $f \circ h = g$;

$$\begin{tikzcd}
 & P \arrow[d, "g"] \arrow[dl, dashed, "h"'] \\
B \arrow[r, two heads, "f"] & C
\end{tikzcd}$$

(3) every short exact sequence $0 \to N \to M \to P \to 0$ *is split.*

Proof. (1) $\iff$ (2) Let $0 \to A \to B \to C \to 0$ be a short exact sequence. Then

$$0 \longrightarrow \operatorname{Hom}_R(P, A) \longrightarrow \operatorname{Hom}_R(P, B) \xrightarrow{\alpha} \operatorname{Hom}_R(P, C) \longrightarrow 0$$

is exact if and only if α is surjective, or equivalently, for all $g \in \operatorname{Hom}_R(P, C)$, there exists $h \in \operatorname{Hom}_R(P, B)$ such that $\alpha(h) = f \circ h = g$.

(2) $\implies$ (3) Given such a short exact sequence, we construct the diagram

$$\begin{tikzcd}
& & & P \arrow[ld, dashed, "h"'] \arrow[d, "1_P"] & \\
0 \arrow[r] & N \arrow[r] & M \arrow[r, "f"'] & P \arrow[r] & 0
\end{tikzcd}$$

Then $f \circ h = 1_P$, so h gives the required splitting.

(3) $\implies$ (2) Suppose we have such a diagram, which equivalently is a diagram of the below form with $B \to C \to 0$ exact.

$$\begin{tikzcd}
& P \arrow[d, "g"] & \\
B \arrow[r, "f"] & C \arrow[r] & 0
\end{tikzcd}$$

Consider the fiber product

$$M = B \times_C P = \{(b,p) \in B \oplus P \mid f(b) = g(p)\}.$$

This comes with projections to $i : M \to B$ and $k : M \twoheadrightarrow P$. Let $N = \operatorname{Ker} k$. We then have the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] & M \arrow[r, two heads, shift left, "k"] \arrow[d, "i"] & P \arrow[l, shift left, "l"] \arrow[r] \arrow[d, "g"] \arrow[ld, dashed, "h"] & 0 \\
& & B \arrow[r, two heads, "f"] & C \arrow[r] & 0
\end{tikzcd}$$

The upper row is split, so there exists $l : P \to M$ with $k \circ l = 1_P$. Take $h = i \circ l$. Then

$$f \circ h = f \circ i \circ l = g \circ k \circ l = g \circ 1_P = g. \qquad \square$$

Definition 2.3.8 (Projective module)**.** We say that P is a *projective* (left) R-module if P satisfies any of the conditions above.

Example 2.3.9. Free modules are projective.

Definition 2.3.10 (Direct summand)**.** Suppose $N \subset M$ is a submodule. We say that N is a *direct summand* of M if there is a submodule $N' \subset M$ with $N \oplus N' = M$.

Theorem 2.3.11. *A (left) R-module P is projective if and only if P is a direct summand of a free R-module.*

Proof. ($\implies$) Every module P is a quotient module of a free module F, so we have an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] & F \arrow[r, two heads] & P \arrow[r] & 0
\end{tikzcd}$$

which is split since P is projective. Then $F \cong N \oplus P$.

($\impliedby$) Suppose $P \oplus P'$ is free. Then $P \oplus P'$ is projective, so $\operatorname{Hom}_R(P \oplus P', -) = \operatorname{Hom}_R(P, -) \oplus \operatorname{Hom}_R(P', -)$ is exact. Thus both $\operatorname{Hom}_R(P, -)$ and $\operatorname{Hom}_R(P', -)$ are exact, so P is projective. $\square$

Example 2.3.12. 1. If $R = R_1 \times R_2$, then R_1 and R_2 are R-modules and $R = R_1 \oplus R_2$ as R-modules. Since R is a free R-module, R_1 and R_2 are projective R-modules which are generally not free.

2. Let $R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$. Consider the R-module homomorphism $R^3 \xrightarrow{(x,y,z)} R$, i.e. $(f, g, h) \mapsto xf + yg + zh$. This has left inverse $f \mapsto (xf, yf, zf)$, so if P is the kernel of the map $R^3 \to R$, then we have a split short exact sequence

$$0 \longrightarrow P \longrightarrow R^3 \xrightarrow{(x,y,z)} R \longrightarrow 0$$

Thus $P \oplus R \cong R^3$, so P is projective. (In fact, it is *stably free*, meaning that it is possible to take the other summand in the theorem to be free.) We claim that P is not free. Suppose $(f, g, h) \in P$, i.e. $xf + yg + zh = 0$. Then for each p on the sphere, $(f(p), g(p), h(p))$ is in the tangent space at p, so (f, g, h) is a vector field on the sphere.

If P were free, then $P \cong R^2$ (as rank is uniquely defined for commutative rings), so P has a basis $\{k, l\}$ of two vector fields. For every point p on the sphere, $\{k(p), l(p)\}$ is a basis for the tangent plane at p, so in particular $k(p) \neq 0$ for all p. This contradicts the hairy ball theorem.

We have similar results for the left exact contravariant functor $\mathrm{Hom}_R(-, X)$.

Proposition 2.3.13. *Let N be a (left) R-module. The following are equivalent:*

(1) the functor $\mathrm{Hom}_R(-, N)$ is exact;

(2) for a diagram of the below form, there exists $h : B \to N$ such that $h \circ f = g$;

$$\begin{tikzcd} A \arrow[r, hook, "f"] \arrow[d, "g"] & B \arrow[dl, dashed, "h"] \\ N & \end{tikzcd}$$

(3) every short exact sequence $0 \to N \to M \to P \to 0$ is split.

Definition 2.3.14 (Injective module)**.** We say that N is an *injective* (left) R-module if N satisfies any of these conditions.

Example 2.3.15. For $R = \mathbb{Z}$, so N is an abelian group, N is injective if and only if N is *divisible*, meaning that $N = aN$ for all non-zero $a \in \mathbb{Z}$. Specific examples include $\mathbb{Q}, \mathbb{Q}/\mathbb{Z}, \mathbb{R}/\mathbb{Z}$.

2.4 Tensor products

Let R be a ring, M a right R-module and N a left R-module (we simply write $(M_R, {}_RN)$). A map $B : M \times N \to A$ to an abelian group A is called a *bilinear map* if

1. $B(m_1 + m_2, n) = B(m_1, n) + B(m_2, n)$ for all $m_1, m_2 \in M$ and $n \in N$,
2. $B(m, n_1 + n_2) = B(m, n_1) + B(m, n_2)$ for all $m \in M$ and $n_1, n_2 \in N$,
3. $B(mr, n) = B(m, rn)$ for all $m \in M$, $n \in N$ and $r \in R$.

All bilinear maps $B : M \times N \to P$ form an abelian group $\mathrm{Bil}(M, N; P)$.

For given $(M_R,\ {}_RN)$ the assignment $P \mapsto \mathrm{Bil}(M,N;P)$ gives rise to a functor

$$\mathbf{AbGroups} \to \mathbf{AbGroups}.$$

The *tensor product* $M \otimes_R N$ of M and N over R is an abelian group representing this functor. In other words, for every abelian group P there is an isomorphism

$$\mathrm{Bil}(M,N;P) \simeq \mathrm{Hom}(M \otimes_R N, P)$$

natural in P. Thus, $M \otimes_R N$ is an abelian group defined uniquely up to canonical isomorphism. Equivalently, there is a *universal* bilinear form

$$B_{univ} : M \times N \to M \otimes_R N$$

such that for every bilinear form $B : M \times N \to P$ with values in an abelian group P there exists a unique homomorphism $f : M \otimes_R N \to P$ such that $B(m,n) = f(m \otimes n)$, where

$$m \otimes n = B_{univ}(m,n) \in M \otimes_R N.$$

We have the following relations:

1. $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$ for all $m_1, m_2 \in M$ and $n \in N$,
2. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$ for all $m \in M$ and $n_1, n_2 \in N$,
3. $mr \otimes n = m \otimes rn$ for all $m \in M$, $n \in N$ and $r \in R$.

Proposition 2.4.1. *Tensor products exist.*

Proof. Consider the free abelian group $F := \mathbb{Z}^{(M \times N)}$ with basis $M \times N$. Let $H \subset F$ be the subgroup generated by the following elements:

1. $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$ for all $m_1, m_2 \in M$ and $n \in N$,
2. $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$ for all $m \in M$ and $n_1, n_2 \in N$,
3. $(mr, n) - (m, rn)$ for all $m \in M$, $n \in N$ and $r \in R$.

We set $M \otimes_R N := F/H$. For an abelian group A, to give a group homomorphism $M \otimes_R N \to A$ is the same as to give a map $B : M \times N \to A$ satisfying $B(H) = 0$, i.e., to give a bilinear form in $\mathrm{Bil}(M,N;A)$. □

It follows from the proof that the group $M \otimes_R N$ is generated by the elements $m \otimes n$ for all $m \in M$ and $n \in N$.

Example 2.4.2. $M \otimes_R R \simeq M$ with $m \otimes r \mapsto mr$ and $R \otimes_R N \simeq N$ with $r \otimes n \mapsto rn$. Indeed, every bilinear form $R \times N \to A$ is of the form $(r,n) \mapsto rf(n)$ for a unique group homomorphism $f : M \to A$, i.e.,

$$\mathrm{Bil}(R,N;A) \simeq \mathrm{Hom}(N,A).$$

Let $f : M \to M'$ and $g : N \to N'$ be homomorphisms of right (respectively, left) R-modules. The map

$$B : M \times N \to M' \otimes N', \quad B(m,n) = f(m) \otimes g(n)$$

is a bilinear form. Hence, there is a unique group homomorphism

$$f \otimes g : M \otimes_R N \to M' \otimes_R N'$$

such that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$. The correspondence $(M, N) \mapsto M \otimes_R N$, $(f, g) \mapsto f \otimes g$ gives rise to a functor

$$(\textbf{Mod-}R) \times (R\textbf{-Mod}) \to \textbf{AbGroups}.$$

Fixing a left R-module N, we get a functor

$$\textbf{Mod-}R \to \textbf{AbGroups}, \quad M \mapsto M \otimes_R N, \quad f \mapsto f \otimes 1_N.$$

Since $(f + f') \otimes g = f \otimes g + f' \otimes g$, this functor is additive. In particular, there are natural isomorphisms

$$(M_1 \oplus M_2) \otimes_R N \simeq (M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$$

and similarly,

$$M \otimes_R (N_1 \oplus N_2) \simeq (M \otimes_R N_1) \oplus (M \otimes_R N_2).$$

Let

$$N' \to N \to N'' \to 0$$

be an exact sequence of left R-modules. Then for an abelian group P the sequence

$$0 \to \operatorname{Bil}(M, N''; P) \to \operatorname{Bil}(M, N; P) \to \operatorname{Bil}(M, N'; P)$$

is exact. Equivalently, the sequence

$$0 \to \operatorname{Hom}(M \otimes_R N'', P) \to \operatorname{Hom}(M \otimes_R N, P) \to \operatorname{Hom}(M \otimes_R N', P)$$

is also exact. It follows that the sequence

$$M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$$

is exact. In other words, the tensor product functor (when one argument is fixed) is right exact.

Example 2.4.3. Let R be a ring and $r \in R$. Then the sequence of left R-module homomorphisms

$$R \xrightarrow{\cdot r} R \to R/Rr \to 0$$

is exact. Applying the functor $M \otimes_R -$ for a right R-module M we get an exact sequence

$$M \xrightarrow{\cdot r} M \to M \otimes_R (R/rR) \to 0,$$

where the first map of right multiplication by r may not be injective. Thus, the functor $M \otimes_R -$ is not left exact in general and $M \otimes_R (R/Rr) \simeq M/Mr$.

Let N be a left R-module. Suppose that N has the structure of a right module over a ring S such that $(rn)s = r(ns)$ for all $r \in R$, $n \in N$ and $s \in S$. We denote this structure as ${}_RN_S$. We call N an *R-S bimodule.*

Example 2.4.4. 1. If R is a commutative ring, then every R-module M is an R-R bimodule.
2. We can view every ring R as an R-R bimodule.

In the situation $(M_R, {}_R N_S)$ for every $s \in S$, the map

$$M \times N \to M \otimes_R N, \quad (m, n) \mapsto m \otimes ns$$

is a bilinear form. By the definition of the tensor product, there is a unique homomorphism $f_s : M \otimes_R N \to M \otimes_R N$ such that $f_s(m \otimes n) = m \otimes (ns)$. The maps f_s allow us to introduce the structure of a right S-module on the group $M \otimes_R N$ via $(m \otimes n)s = m \otimes (ns)$.

Example 2.4.5. If R is a commutative ring and M and N are R-modules, then $M \otimes_R N$ is an R-module.

Consider the situation $(M_R, {}_R N_S, P_S)$. We just learned that $M \otimes_R N$ is a right S-module. The group $\mathrm{Hom}_S(N, P)$ has the structure of a right R-module via $(fr)(n) = f(rn)$ for $f \in \mathrm{Hom}_S(N, P)$, $r \in R$ and $n \in N$.

Proposition 2.4.6. *In the situation $(M_R, {}_R N_S, P_S)$ there is a natural isomorphism*

$$\mathrm{Hom}_S(M \otimes_R N, P) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P)).$$

Proof. We define a map

$$\alpha : \mathrm{Hom}_S(M \otimes_R N, P) \to \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P))$$

by $\alpha(f)(m)(n) = f(m \otimes n)$, where $f : M \otimes_R N \to P$ is an S-module homomorphism. One checks that α is a well defined homomorphism.
We define a map

$$\beta : \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P)) \to \mathrm{Hom}_S(M \otimes_R N, P)$$

as follows. Let $g \in \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, P))$. Then the map

$$B : M \times N \to P, \quad (m, n) \mapsto g(m)(n)$$

is a bilinear map. By the definition of the tensor product, there is a unique homomorphism $h : M \otimes_R N \to P$ such that $h(m \otimes n) = B(m, n)$. We define β by $\beta(g) = h$. Precisely,

$$\beta(g)(m \otimes n) = g(m)(n).$$

One checks that α and β are inverse to each other isomorphisms. □

Corollary 2.4.7. *In the situation $(M_R, {}_R N)$, for an abelian group P there is a natural isomorphism*

$$\mathrm{Hom}(M \otimes_R N, P) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}(N, P)).$$

Proof. Set $S = \mathbb{Z}$. □

If we fix a left R-module N, then the corollary asserts that the tensor product functor

$$\textbf{Mod-}R \to \textbf{AbGroups}, \quad M \mapsto M \otimes_R N$$

has the right adjoint functor

$$\textbf{AbGroups} \to \textbf{Mod-}R, \quad P \mapsto \operatorname{Hom}(N, P).$$

In particular, the functor $M \mapsto M \otimes_R N$ (as well as $N \mapsto M \otimes_R N$ if M is fixed) commutes with colimits (in particular, commutes with arbitrary direct sums).

Let $f : R \to S$ be a ring homomorphism and M a right R-module. We can view S as a left and right R-module. Considering the situation $(M_R, {}_R S_S)$ we see that $M \otimes_R S$ is a right S-module. Moreover, we have an additive *change of ring* functor

$$\textbf{Mod-}R \to \textbf{Mod-}S, \quad M \mapsto M \otimes_R S.$$

Example 2.4.8. Let M be a right R-module and $I \subset R$ and ideal. Then M/IM is an R/I-module. In fact, $M/IM \simeq M \otimes_R (R/I)$, so M/IM is the R/I-module obtained by the ring change with respect to $R \to R/I$.

We also have the pull-back functor (with respect to f):

$$\textbf{Mod-}S \to \textbf{Mod-}R, \quad P_S \mapsto P_R.$$

By Proposition 2.4.6, in the situation (M_R, P_S), we have an isomorphism

$$\operatorname{Hom}_S(M \otimes_R S, P) \simeq \operatorname{Hom}_R(M, \operatorname{Hom}_S(S, P)) = \operatorname{Hom}_R(M, P)).$$

It follows that the change of ring functor is left adjoint to the pull-back functor.

2.5 Modules over a PID

Throughout, let R be a PID, F be its quotient field, and M be an R-module.

Definition 2.5.1 (Torsion)**.** An element $m \in M$ is a *torsion element* if there exists $r \neq 0$ in R for which $rm = 0$.

The *torsion part* of M is the submodule of torsion elements, denoted M_{tors}.

We say that M is *torsion free* if $M_{\text{tors}} = 0$ and M is *torsion* if $M_{\text{tors}} = M$.

Lemma 2.5.2. *M/M_{tors} is torsion free.*

Proof. Let $m + M_{\text{tors}} \in M/M_{\text{tors}}$ with $m \notin M_{\text{tors}}$ and suppose $r(m + M_{\text{tors}}) = rm + M_{\text{tors}} = M_{\text{tors}}$ for some $r \in R$. Then $rm \in M_{\text{tors}}$, so there exists $s \in R$ with $s \neq 0$ such that $s(rm) = (sr)m = 0$. Hence $sr = 0$, so $r = 0$. □

We have a short exact sequence

$$0 \longrightarrow M_{\text{tors}} \hookrightarrow M \longrightarrow M/M_{\text{tors}} \longrightarrow 0 \tag{†}$$

Definition 2.5.3 (Rank)**.** The *rank* of M is the dimension of FM as an F-vector space.

If M is finitely generated, then $\operatorname{rank} M < \infty$.

Example 2.5.4. If $M = R^n$, then $\operatorname{rank} M = n$.

There is a canonical map $M \to FM$ given by $m \mapsto m/1$ which is also an R-module homomorphism, with kernel M_{tors}. In particular, if M is torsion free, then $M \hookrightarrow FM$ as R-modules.

Proposition 2.5.5. *Let M be a free R-module of rank n and $N \subset M$ be a submodule. Then N is free of rank at most n.*

Proof. We apply induction on n. When $n = 1$, so $M = R$, then $N \subset R$ is an ideal. Every ideal is principal by assumption, so N is free of rank 0 (if $N = 0$) or 1 (otherwises).

For the induction step, let $\{m_1, \dots, m_n\}$ be a basis for $M = R^n$. Define $f : M \to R$ by $\sum_i a_i m_i \mapsto a_n$. This is a surjective R-module homomorphism with kernel M' free with basis $\{m_1, \dots, m_{n-1}\}$. Let $N \subset M$ be a submodule and let $I = f(N)$. Then I is an ideal in R, so we have the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M' \cap N \arrow[r] & N \arrow[r, "f"] & I \arrow[r] & 0. \end{tikzcd}$$

By induction, $M' \cap N \subset M'$ is free of rank at most $n-1$, while I is free of rank at most 1. In particular, it is projective, so the short exact sequence is split. Hence $N \cong (M' \cap N) \oplus I$ is free of rank at most n. □

Free R-modules are torsion free.

Remark 2.5.6. The converse of this statement is false. For example, $\mathbb{Q}$ is torsion free but not a free module over $\mathbb{Z}$.

Theorem 2.5.7. *Every finitely generated torsion-free R-module is free.*

Proof. Let M be finitely generated and take its embedding $M \hookrightarrow FM$, which is a vector space of dimension $n = \operatorname{rank} M$ over F. Let $\{x_1, \dots, x_n\}$ be a basis for FM, so then

$$FM = \bigoplus_{i=1}^n F x_i.$$

Let

$$P = \bigoplus_{i=1}^n R x_i$$

be the free R-module with basis $\{x_1, \dots, x_n\}$. Given any $m \in M$, we can write $m = \sum_i \alpha_i x_i$ with $\alpha_i \in F$. Clearing denominators, $am = \sum_i a\alpha_i x_i$ with $a\alpha_i \in R$ for all i, so then $am \in P$. Since M is finitely generated by some $\{m_1, \dots, m_s\}$, we can find a common a with $am_j \in P$ for all j. This means that $am \in P$ for all P. Since P is free and $aM \subset P$ is a submodule, aM is free. Multiplication by a is an isomorphism $M \to aM$ since $a \neq 0$ and M is torsion-free, so M is free. □

Let M be a finitely generated R-module and consider the short exact sequence (†). Then M/M_{tors} is finitely generated and torsion-free, so it is free and $M/M_{\text{tors}} \cong R^n$ with $n = \operatorname{rank} M$. Thus the short exact sequence is split and $M \cong M_{\text{tors}} \oplus R^n$. From this decomposition, M_{tors} is finitely generated.

Now suppose that M is a finitely generated torsion module, i.e. $M = M_{\text{tors}}$. Let $\mathfrak{p} \neq 0$ be a prime ideal in R.

Definition 2.5.8 ($\mathfrak{p}$-primary)**.** We say that $m \in M$ is *$\mathfrak{p}$-primary* if $\mathfrak{p}^n m = 0$ for some $n > 0$.

M is a *$\mathfrak{p}$-primary module* if $\mathfrak{p}^n M = 0$ for some $n > 0$, or equivalently, if all $m \in M$ are $\mathfrak{p}$-primary.

M is *primary* if M is *$\mathfrak{p}$-primary* for some $\mathfrak{p}$.

Example 2.5.9. $M = R/\mathfrak{p}^n$ is $\mathfrak{p}$-primary.

Notation. Let $M(\mathfrak{p})$ be the submodule of all $\mathfrak{p}$-primary elements of M, called the *$\mathfrak{p}$-primary part of M*.

Lemma 2.5.10. *Let $a_1, \dots, a_n \in R$ be relatively prime (not necessarily pairwise) in the sense of having no non-unit common divisor. Then there exist $b_1, \dots, b_n \in R$ such that $\sum a_i b_i = 1$.*

Proof. The ideal generated by $(a_1, \dots, a_n)$ is principal, hence equal to (c) for some $c \in R$. Then $c \mid a_i$ for all i, so c must be a unit. □

Corollary 2.5.11. *Let $m \in M$ and suppose $a_1 m = \cdots = a_n m = 0$ for relatively prime $a_1, \dots, a_n$. Then $m = 0$.*

Theorem 2.5.12. *Let M be a finitely generated torsion R-module. Then $M(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$, and*

$$M = \bigoplus_{\mathfrak{p}} M(\mathfrak{p}).$$

Proof. There exists a non-zero $a \in R$ such that $aM = 0$. Suppose $M(\mathfrak{p}) \neq 0$ for $\mathfrak{p} = (p)$ and let $m \in M(\mathfrak{p})$ be non-zero, so $p^n m = 0$. Since $m \neq 0$, it must be that $p \mid a$ by Corollary 2.5.11. There are only finitely many prime divisors of a, hence only finitely many $\mathfrak{p}$ with $M(\mathfrak{p}) \neq 0$, and all such $\mathfrak{p}$ contain a.

Factor $a = u p_1^{k_1} \cdots p_n^{k_n}$ with p_i, p_j not associates for $i \neq j$. Let $a_i = a/p_i^{k_i}$. Then $a_1, \dots, a_n$ are relatively prime, so $\sum_i a_i b_i = 1$ for some b_i. Then $m = \sum_i a_i b_i m$ and for each i, we have $a_i b_i m \in M(\mathfrak{p})$, so $M = \sum M(\mathfrak{p})$. To show that we have a direct sum, we show that if $m_1 + \cdots + m_n = 0$, then each $m_i = 0$. Multiply through to get $b_i m_i = 0$ for $b_i = \prod_{j \neq i} p_j^{s_j}$. We also have $p_i^{s_i} m_i = 0$, and so $m_i = 0$ since b_i and $p_i^{s_i}$ are relatively prime. □

Definition 2.5.13 (Cyclic module)**.** We say that M is *cyclic* if M is generated by one element.

Example 2.5.14. If $I \subset R$ is an ideal, then R/I is cyclic.

If $\mathfrak{p} = pR \neq 0$ is a prime ideal, then $R/\mathfrak{p}^n = R/p^n R$ is $\mathfrak{p}$-primary cyclic.

Proposition 2.5.15. *Every cyclic R-module M is isomorphic to one of the form R/I for some ideal $I \subset R$.*

Example 2.5.16. Let $\mathfrak{p} \subset R$ be non-zero prime. Then $R/\mathfrak{p} = k$ is a field since every nonzero prime ideal in a PID is maximal.

If M is a $\mathfrak{p}$-primary module with $\mathfrak{p}^n M = 0$, then M is an $R/\mathfrak{p}^n$-module. In particular, if $\mathfrak{p}M = 0$, then M is a k-module, i.e. a vector space over k.

Notation. If M is an R-module and $P = pR$, we write ${}_pM = \{m \in M \mid pm = 0\} \subset M$. This is a submodule with $\mathfrak{p} \cdot {}_pM = 0$, so it is also a k-vector space.

Lemma 2.5.17. *Let M be an R-module and $\mathfrak{p} = pR$ be a prime ideal such that $\mathfrak{p}^n M = 0$ and $\mathfrak{p}^{n-1}M \neq 0$. If $\dim_k({}_pM) = 1$, then $M \cong R/\mathfrak{p}^n R$.*

Proof. There exists $x \in M$ for which $p^n x = 0$ but $p^{n-1}x \neq 0$. We prove the following

Claim: If $rx = 0$ for some $r \in R$, then p^n divides r. Indeed, write $r = p^m q$ with $p \nmid q$. We claim that $m \geq n$. Suppose otherwise, so then $q(p^m x) = 0 = p^{n-m}(p^m x)$. Since q and p^{n-m} are relatively prime, $p^m x = 0$, contradicting the choice of n.

We prove the statement of the lemma by induction on n. If $n = 1$, then $\mathfrak{p}M = 0$, so $M = {}_pM \cong k = R/\mathfrak{p}$.

For the inductive step, define a map $R \to M$ by $r \mapsto rx$. This induces a map $f : R/\mathfrak{p}^n \to M$, which we claim is an isomorphism. The map f is injective by the claim. To see that f is surjective, it suffices to show that x generates M. Let $y \in M$ and find the smallest m such that $p^m y = 0$. If $m = 1$, then $y \in {}_pM$ and $p^{n-1}x \in {}_pM$ with $p^{n-1}x \neq 0$. Since ${}_pM$ is of dimension 1, $y = sp^{n-1}x$ for some $s \in R$. Inducting on m, if $p^m y = 0$, then $p^{m-1}(py) = 0$, so py is a multiple of x, say $py = sx$ for some $s \in R$. Then $p^{m-1}sx = 0$, so $p^n \mid p^{m-1}s$ by the claim. This means that $p \mid s$ since $m \leq n$, so write $s = pt$. Then $p(y - tx) = 0$, so $y - tx \in {}_pM$. We already know that everything in ${}_pM$ is a multiple of x, so y is a multiple of x. □

Let M be a finitely generated $\mathfrak{p}$-primary module with $\mathfrak{p}^n M = 0$. We have a descending chain

$$M \supset \mathfrak{p}M \supset \cdots \supset \mathfrak{p}^n M = 0.$$

For each i, we have that $\mathfrak{p}(\mathfrak{p}^{i-1}M/\mathfrak{p}^i M) = 0$. Since $\mathfrak{p}^i M = p^i M$ for each i, it follows that $\mathfrak{p}^{i-1}M/\mathfrak{p}^i M$ is finitely generated, so a k-vector space of finite dimension.

Definition 2.5.18 (Length)**.** The *length* of a finitely generated $\mathfrak{p}$-primary module with $\mathfrak{p}^n M = 0$ is

$$l(M) = \sum_{i=1}^{n} \dim_k(\mathfrak{p}^{i-1}M/\mathfrak{p}^i M).$$

Example 2.5.19. We have $l(R/\mathfrak{p}^n) = n$, as for $i \leq n$,

$$\mathfrak{p}^{i-1}(R/\mathfrak{p}^n)/\mathfrak{p}^i(R/\mathfrak{p}^n) \cong \mathfrak{p}^{i-1}R/\mathfrak{p}^i R \cong R/\mathfrak{p}R = k.$$

Proposition 2.5.20. *1. $l(M \oplus N) = l(M) + l(N)$.*

2. If $0 \neq N \subset M$, then $l(M/N) < l(M)$.

Proof. 1. Clear.

2. Let $\overline{M} = M/N$. For each i, projection gives a surjective map $\varphi_i \mathfrak{p}^{i-1}M/\mathfrak{p}^i M \twoheadrightarrow \mathfrak{p}^{i-1}\overline{M}/\mathfrak{p}^i\overline{M}$. To show strict inequality, we must show that for some i, this map has non-trivial kernel. There is a unique i such that $\mathfrak{p}^i M \subsetneq N \subset \mathfrak{p}^{i-1}M$. Then the image of N in $\mathfrak{p}^{i-1}\mathfrak{m}/\mathfrak{p}^i M$ is not zero, but is in the kernel of φ_i. □

Proposition 2.5.21. *Let M be a finitely generated R-module and $\mathfrak{p} \subset R$ be a non-zero prime ideal such that $\mathfrak{p}^n M = 0$ and $\mathfrak{p}^{n-1}M \neq 0$ for some $n > 0$. Then there exists a surjective R-module homomorphism $M \twoheadrightarrow R/\mathfrak{p}^n$.*

Proof. There exists $x \in M$ for which $p^n x = 0$ and $p^{n-1}x \neq 0$, where $\mathfrak{p} = pR$. Then $p^{n-1}x \in {}_pM$ is non-zero, so $\dim_k({}_pM)$ is non-zero. If $\dim_k({}_pM) = 1$, then $M \cong R/\mathfrak{p}^n$. Otherwise, $p^{n-1}x$ does not span ${}_pM$ as a k-vector space, so we can find $y \in {}_pM$ and let $N = ky$. This N is a k-vector subspace of ${}_pM$, so it is also a submodule of M. Let $\overline{M} = M/N$. Since $N \neq 0$, we have $l(\overline{M}) < l(M)$ and $\mathfrak{p}^n\overline{M} = 0$, while $p^{n-1}\overline{x} \neq 0$ since $p^{n-1}x \neq N$, so $\mathfrak{p}^{n-1}\overline{M} \neq 0$. By strong induction on $l(M)$, there is a surjective homomorphism $\overline{M} \twoheadrightarrow R/\mathfrak{p}^n$, so we can compose this with the quotient map. □

Theorem 2.5.22. *Let M be a finitely generated R-module. Then M is a finite direct sum of cyclic modules of the form R and $R/\mathfrak{p}^n$ for $\mathfrak{p} \subset R$ non-zero prime.*

Proof. We induct on the length of M. If $l(M) = 0$, then $M = 0$. For the induction step, write $M = M_{\text{tors}} \oplus R^n$ and suppose that $\mathfrak{p}^n M = 0$ for some non-zero prime $\mathfrak{p} \subset R$, with $\mathfrak{p}^{n-1}M \neq 0$. There is a surjective map $M \twoheadrightarrow R/\mathfrak{p}^n$, which is free as an $R/\mathfrak{p}^n$-module, so we have $M \cong N \oplus R/\mathfrak{p}^n$ for some $R/\mathfrak{p}^n$-submodule $N \subset M$. Apply induction to N. □

By a similar computation to that for $l(R/\mathfrak{p}^n)$,

$$l_n(\mathfrak{p}) = \dim_k(\mathfrak{p}^{n-1}M(\mathfrak{p})/\mathfrak{p}^n M(\mathfrak{p})) = \text{number of cyclic summands } R/\mathfrak{p}^m \text{ in } M(p) \text{ with } m \geq n.$$

Remark 2.5.23. The number of cyclic summands R is equal to the rank of M, and the number of cyclic summands $R/\mathfrak{p}^n$ is $l_n(\mathfrak{p}) - l_{n+1}(\mathfrak{p})$. Hence the decomposition is unique up to re-ordering.

Let M be a finitely generated R-module. Then we can write

$$\begin{aligned} M_{\text{tors}} \cong R/\mathfrak{p}_1^{\alpha_{11}} &\oplus \cdots \oplus R/\mathfrak{p}_1^{\alpha_{1r}} \\ \oplus R/\mathfrak{p}_2^{\alpha_{21}} &\oplus \cdots \oplus R/\mathfrak{p}_2^{\alpha_{2r}} \\ &\cdots \\ \oplus R/\mathfrak{p}_s^{\alpha_{s1}} &\oplus \cdots \oplus R/\mathfrak{p}_s^{\alpha_{sr}}, \end{aligned}$$

with $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ distinct non-zero prime ideals and $\alpha_{i1} \geq \alpha_{i2} \geq \cdots \geq \alpha_{ir} \geq 0$ for each i. The powers of prime ideals $\{P_i^{\alpha_{ij}}\}$ different from R are *elementary divisors* of M. Denote this family by $\mathrm{ED}(M)$.

Theorem 2.5.24 (Elementary divisor form)**.** *Two finitely generated modules M and N over a PID R are isomorphic if and only if* $\operatorname{rank} M = \operatorname{rank} N$ *and* $\mathrm{ED}(M) = \mathrm{ED}(N)$.

By the Chinese remainder theorem, if $I_j = \mathfrak{p}_1^{\alpha_{1j}} \cdots \mathfrak{p}_s^{\alpha_{sj}}$, then

$$R/\mathfrak{p}_1^{\alpha_{1j}} \oplus \cdots \oplus R/\mathfrak{p}_s^{\alpha_{sj}} \cong R/I_j.$$

We may thus write

$$M = R/I_1 \oplus \cdots \oplus R/I_r,$$

with the family $\mathrm{IF}(M) = \{I_1, \ldots, I_r\}$ consisting of *invariant factors*. These are unique and satisfy $I_1 \subset \cdots \subset I_r$.

Theorem 2.5.25 (Invariant factor form)**.** *Two finitely generated modules M and N over a PID R are isomorphic if and only if* $\operatorname{rank} M = \operatorname{rank} N$ *and* $\mathrm{IF}(M) = \mathrm{IF}(N)$.

Let M be a finitely generated R-module and $M \cong F/N$ with F free of rank n. Let $\{x_1, \ldots, x_n\}$ be a basis for F and $\{y_1, \ldots, y_n\}$ be generators for N. We can write

$$\begin{aligned} y_1 &= a_{11}x_1 + \cdots + a_{n1}x_n \\ y_2 &= a_{12}x_1 + \cdots + a_{n2}x_n \\ &\vdots \\ y_m &= a_{1m}x_1 + \cdots + a_{nm}x_n \end{aligned}$$

and let $A = (a_{ij})$.
Suppose

$$A = \left(\begin{array}{ccc} r_1 & & \\ & \ddots & \\ & & r_m \\ \hline & 0 & \end{array}\right) \tag{†}$$

with $r_1 \mid \cdots \mid r_m \neq 0$. Then

$$M \cong F/N \cong R^{n-m} \oplus \bigoplus_{i=1}^{m} Rx_i/Rr_ix_i \cong R^{n-m} \oplus \bigoplus_{i=1}^{m} R/r_iR.$$

The invariant factors are $\{r_1R, \ldots, r_mR\}$, but with r_iR removed if r_i is a unit.
To put a general A into this form, we have the following elementary operations:

(I) permutation of rows (columns);

(II) addition to one row (column) a multiple of another row (column);

(III) multiplication of a row (column) by a unit in R.

These correspond to changing the generators for F and N.
When R is a Euclidean domain, we can use the Euclidean algorithm to systematically put A into the form of (†).

Example 2.5.26. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}^2/((4,2),(2,4))$. The coefficient matrix is

$$A = \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix} \to \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 4 \\ 0 & -6 \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 0 & -6 \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix},$$

so $M \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. Thus $\mathrm{IF}(M) = \{2\mathbb{Z}, 6\mathbb{Z}\}$ and $\mathrm{ED}(M) = \{2\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}\}$.

2.6 Abelian groups

Abelian groups are equivalent to $\mathbb{Z}$-modules, so the classification theorems apply.

Theorem 2.6.1 (ED form)**.** *Every finitely generated abelian group is isomorphic to a direct sum of cyclic groups $\mathbb{Z}$ and $\mathbb{Z}/p^n\mathbb{Z}$ for p prime. Two finitely generated abelian groups M and N are isomorphic if and only if* $\operatorname{rank} M = \operatorname{rank} N$ *and* $\mathrm{ED}(M) = \mathrm{ED}(N)$*.*

Theorem 2.6.2 (IF form)**.** *Every finitely generated abelian group is isomorphic to $\mathbb{Z}^n \oplus \mathbb{Z}/r_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/r_k\mathbb{Z}$ with $r_i > 1$ and $r_1 \mid \cdots \mid r_k$. Two finitely generated abelian groups M and N are isomorphic if and only if* $\operatorname{rank} M = \operatorname{rank} N$ *and* $\mathrm{IF}(M) = \mathrm{IF}(N)$*.*

Example 2.6.3.

1. $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \not\cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$ since they have different invariant factors.
2. $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/90\mathbb{Z} \cong \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$ since they both have elementary divisors $\{2, 3, 4, 5, 9\}$. In invariant factor form, they are isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z}$.

2.7 Modules over $F[x]$

Let F be a field and $R = F[x]$. We will be considering the following three languages and the dictionaries between them:

1) R-modules;

2) Linear operators of vector spaces over F;

3) Matrices.

Suppose V is an R-module. Since $F \subset R$ is a subring, we can also regard V as an F-module, i.e. a vector space over F. The map $S : V \to V$ given by $S(v) = x \cdot v$ is a linear operator on V. Conversely, given a vector space V and a linear operator $S : V \to V$, we can define an R-module structure on V by setting

$$(\sum a_i x^i)v = \sum a_i S^i(v).$$

Thus $F[x]$-modules correspond to vector spaces V over F together with a linear operator $S : V \to V$. If S is a linear operator in a vector space V, the choice of a basis B for V yields a square matrix $[S]_B$ of S over F.

Let $D : V \to W$ be an R-module homomorphism, in particular $D(xv) = vD(v)$. Let S and T be the linear operators on V and W respectively. We have $D \circ S = TD$. In particular, if D is an automorphism of V, then $T = DSD^{-1}$. Choosing bases we see that the matrices $[S]$ and $[T]$ are conjugate or *similar*.

Given two R-modules V and W specified by linear operators S and T, the direct sum $V \oplus W$ is given by the operator $S \oplus T$ with matrix $\begin{pmatrix} [S] & 0 \\ 0 & [T] \end{pmatrix}$.

Note that every nonzero ideal of $R = F[x]$ is generated by a unique monic polynomial. Suppose that $V = R/fR$ is a cyclic R-module for some $f = a_0 + \cdots + a_{n-1}x^{n-1} + x^n \in R$. Then V has a basis $(v_0, \ldots, v_{n-1})$ corresponding to $(1, x, \ldots, x^{n-1})$, so $x \cdot v_i = v_{i+1}$ for $0 \le i < n-1$ and $x \cdot v_{n-1} = -a_0 v_0 - \cdots - a_{n-1} v_{n-1}$. The matrix of the corresponding S is the *companion matrix* for

f,

$$C(f) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & -a_{n-3} \\ 0 & 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Theorem 2.7.1. *Let $S : V \to V$ be a linear operator. Then the matrix of S in some basis for V is similar to a unique matrix of the form*

$$\begin{pmatrix} C(f_1) & & \\ & \ddots & \\ & & C(f_r) \end{pmatrix},$$

where $f_1 \mid f_2 \mid \cdots \mid f_r$ are nonzero monic polynomials. Moreover, $\mathrm{IF}(S) = \{f_1, f_2, \ldots, f_r\}$ *are the invariant factors.*

Definition 2.7.2 (Rational canonical form of an operator)**.** This matrix is the *rational canonical form* for S.

Theorem 2.7.3. *Let A be a square matrix over F. Then A is similar to a unique matrix of the form*

$$\begin{pmatrix} C(f_1) & & \\ & \ddots & \\ & & C(f_r) \end{pmatrix},$$

where $\mathrm{IF}(A) = \{f_1, f_2, \ldots, f_r\}$ *are the invariant factors.*

Definition 2.7.4 (Rational canonical form of a square matrix)**.** This matrix is the *rational canonical form* for A.

Proposition 2.7.5. *Two matrices are similar if and only if they have the same rational canonical form.*

How to compute the invariant factors of a linear operator $S : V \to V$? Choose a basis $B = \{v_1, v_2, \ldots, v_n\}$ for S and let $A = (a_{ij})$ be the matrix $[S]_B$ of S in the basis B. Consider the matrix

$$xI_n - A = \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \vdots & \ddots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix}$$

The determinant $P_S(x)$ of this matrix is a monic polynomial of degree $n = \dim(V)$, called the *characteristic polynomial of S*.

Consider the R-submodule N of R^n generated by the columns of this matrix.

Lemma 2.7.6. *The factor module R^n/N is a vector space of dimension n.*

Proof. We write the generators of N (the columns of $xI_n - A$) as linear combinations of the standard basis of R^n. The matrix of the coefficient is $xI_n - A$. In order to compute the invariant factors of the R-module R^n/N we transform the matrix $xI_n - A$, using the elementary operations, to the diagonal matrix with monic polynomials $f_1 \mid f_2 \mid \dots \mid f_n$ on the diagonal. Comparing the determinants we see that $P_S(x)$ is the product of all f_i, in particular, $\sum \deg(f_i) = n$. Since $R^n/N \simeq \coprod R/f_iR$, we have $\dim(R^n/N) = n$. □

Consider an R-module homomorphism

$$g : R^n \to V$$

defined by

$$g(h_1, h_2, \dots, h_n) = h_1(S)(v_1) + h_2(S)(v_2) + \cdots + h_n(S)(v_n).$$

Clearly, g is surjective. We claim that $N \subset \operatorname{Ker}(g)$. Indeed, computing the image of the k-th column of the matrix $xI_n - A$ under g, we have

$$g(-a_{k1}, \cdots, -a_{k,k-1}, x - a_{kk}, -a_{k,k+1}, -a_{kn}) = S(v_k) - \sum_i a_{ki}v_i = 0$$

by the definition of the matrix A of the operator S in the basis B. Therefore, g factors through a surjective linear map $\overline{g} : R^n/N \to V$. By Lemma 2.7.6, $\dim(R^n/N) = n = \dim(V)$. It follows that $\overline{g}$ is an isomorphism. In particular, the nonconstant polynomials f_i in the proof of Lemma 2.7.6 are the invariant factors of S. Precisely, if k is the largest index such that $f + 1 = \cdots f_k = 1$, then $\mathrm{IF}(S) = \{f_{k+1}, \dots, f_n\}$. Note that the product of all invariant factors of S is equal to $P_S(x)$.

Let M be a finitely generated torsion R-module. The ideal of all $g \in R$ such that $gM = 0$ is nonzero, hence it is generated by a unique monic polynomial m_S, called the *minimal polynomial of S*. Similarly, we defined the minimal polynomial of a linear operator and a square matrix. For example, the minimal polynomial of R/fR, where f is a monic polynomial is equal to f. If the invariant factors of an R-module (linear operator or matrix) are $f_1 \mid f_2 \mid \cdots \mid f_s$, then the minimal polynomial coincides with f_s.

Example 2.7.7. 1. Let $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. Then reducing $x \cdot I - A$ gives

$$\begin{pmatrix} x-2 & -1 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & x-2 \end{pmatrix} \to \begin{pmatrix} 1 & x-2 & 0 \\ 0 & (x-2)^2 & 0 \\ 0 & 0 & x-2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)^2 \end{pmatrix},$$

so the invariant factors are $x-2$ and $(x-2)^2$. Hence $\mathrm{RCF}(A) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & 4 \end{pmatrix}$.

2. Let p be prime and consider elements of $GL_2(\mathbb{Z}/p\mathbb{Z})$, a matrix group of size $(p^2-1)(p^2-p)$. The number of classes is equal to the number of possible rational canonical forms, which is

determined by the possible invariant factors. These must have total degree 2, so there are two cases. If $\mathrm{IF}(A) = \{f\}$, so that $f = x^2 + ax + b$, then $C(f) \in GL_2(\mathbb{Z}/p\mathbb{Z})$ if and only if $b \neq 0$, so this case gives $p(p-1)$ classes. If $\mathrm{IF}(A) = \{f, g\}$, then $f \mid g$ and both have degree 1, so $g = f = x + a$ for some $a \neq 0$. Hence we have $p - 1$ classes in this case, so in total, there are $p(p-1) + (p-1) = p^2 - 1$ conjugacy classes in $GL_2(\mathbb{Z}/p\mathbb{Z})$.

3. Let A be an $n \times n$ matrix over F and K be a field containing F. The invariant factors of A over F are the same as those over K, so $A \sim B$ in F if and only if $A \sim B$ in K.

4. We classify (up to similarity) all 3×3 matrices A over $\mathbb{Q}$ such that $A^4 + 2A^3 + A^2 = 0$ but $A + A^2 \neq 0$. The minimal polynomial of A satisfies $m_A \mid x^4 + 2x^3 + x^2 = x^2(x+1)^2$ but $m_A \nmid x^2 + x = x(x+1)$, so the possible minimal polynomials are x^2, $(x+1)^2$, $x(x+1)^2$, and $x^2(x+1)$.

   If $m_A = x^2$, then $\mathrm{IF}(A) = \{x, x^2\}$, and the RCF is $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

   If $m_A = (x+1)^2$, then $\mathrm{IF}(A) = \{x+1, x^2+2x+1\}$, and the RCF is $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -2 \end{pmatrix}$.

   If $m_A = x(x+1)^2$, then $\mathrm{IF}(A) = \{x^3 + 2x^2 + x\}$, and the RCF is $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & -2 \end{pmatrix}$.

   If $m_A = x^2(x+1)$, then $\mathrm{IF}(A) = \{x^3 + x^2\}$, and the RCF is $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & -1 \end{pmatrix}$.

5. We classify (up to similarity) all 4×4 matrices A over $\mathbb{R}$ such that $(A - 2I)^2 = 0$. Since $m_A \mid (x-2)^2$, we have $m_A = x - 2$ or $m_A = (x-2)^2$. As the minimal polynomial is the largest invariant factor, the possibilities for $\mathrm{IF}(A)$ are

   $$\{x-2, x-2, x-2, x-2\}, \qquad \{x-2, x-2, (x-2)^2\}, \qquad \{(x-2)^2, (x-2)^2\}.$$

   There are three similarity classes.

Proposition 2.7.8. *Let $S : V \to V$ be a linear operator. Then the following are equivalent:*

(1) V is cyclic as an R-module;

(2) the matrix of S in some basis is $C(f)$ for some (monic) $f \in R$;

(3) $\mathrm{IF}(S) = \{P_S\}$;

(4) $m_S = P_S$;

(5) the elementary divisors of S are pairwise coprime.

Proof. (1) $\implies$ (3) If V is cyclic, then $V \cong R/fR$ for some $f \in R$, so $\mathrm{IF}(S) = \{f\}$, in which case $f = P_S$.

(3) $\implies$ (2) If $\mathrm{IF}(S) = \{f\}$, then $V \cong R/fR$, so $[S] = C(f)$ in some basis.

(2) $\implies$ (1) If $[S] = C(f)$ in some basis, then $V \cong R/fR$ is cyclic.

(3) $\iff$ (4) Since P_S is the product of all invariant factors and m_S is always an invariant factor, $P_S = m_S$ if and only if $\mathrm{IF}(s) = \{P_S\}$.

(5) $\implies$ (1) Let $\mathrm{ED}(S) = \{p_i^{\alpha_i}\}$. Then by the Chinese remainder theorem, if $f = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $V \cong R/fR$ is cyclic.

(3) $\implies$ (5) The elementary divisors are the primary divisors of $\mathrm{IF} = \{P_S\}$. □

If $V = R/(x-\lambda)^k R$ for some $\lambda \in F$ and $S : V \to V$ is the corresponding operator, consider the *Jordan basis* $\{1, \overline{x} - \lambda, \dots, (\overline{x} - \lambda)^{k-1}\}$. Then

$$S((\overline{x} - \lambda)^i) = \overline{x(x-\lambda)^i} = (\overline{x} - \lambda)^{i+1} + \lambda(\overline{x} - \lambda)^i.$$

In particular, when $i = k-1$, then the first term vanishes. Therefore, the matrix of S with respect to this basis, restricted to M, is

$$[S] = \begin{pmatrix} \lambda & 0 & \cdots & 0 & 0 \\ 1 & \lambda & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 1 & \lambda & 0 \\ 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}.$$

This is a *Jordan block* $J(\lambda, k)$.

Definition 2.7.9 (Splitting). A monic polynomial f is *split over F* if $f = (x - \lambda_1) \cdots (x - \lambda_n)$ for some $\lambda_1, \dots, \lambda_n \in F$.

Theorem 2.7.10. *Let $S : V \to V$ be a linear operator over F. Assume that the characteristic polynomial P_S is split over F. Then there is a basis of V such that*

$$[S] = \begin{pmatrix} J_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & J_t \end{pmatrix}$$

for some Jordan blocks $J_1, \dots, J_t$. These are unique up to permutation, and this form of S is the Jordan form, *denoted $J(S)$.*

Proof. Every elementary divisor of S divides P_S, hence it is of the form $(x-\lambda)^k$ for some $\lambda \in F$ and k since P_S is split. Then V is a direct some of cyclic modules of the form $R/(x-\lambda)^k R$. Now apply the Jordan bases to each cyclic summand. □

Proposition 2.7.11. *Let $S : V \to V$ be a linear operator. The following are equivalent:*

(1) there exists a basis such that $[S]$ is diagonal;

(2) there exists a basis consisting of eigenvectors of S;

(3) V is a direct sum of eigenspaces of S;

(4) all elementary divisors of S are linear;

(5) all invariant factors of S are products of distinct linear polynomials;

(6) m_S is a product of distinct linear polynomials.

Proof. Linear algebra. □

3 Fields

3.1 Field extensions

Proposition 3.1.1. *Every field homomorphism is injective.*

Proof. If $f : F \to K$ is a field homomorphism, then $\operatorname{Ker} f \subset F$ is an ideal which does not contain 1, so $\operatorname{Ker} f = 0$. □

Given a homomorphism of fields $f : F \to K$, we can identify F with $\operatorname{Im} f \subset K$.

Definition 3.1.2 (Extension)**.** If $F \subset K$ is a subfield (subring), we say that K is a *field extension* (ring extension) of F, written K/F.

Notation. Given a field F, the category of field extensions of F is denoted $\mathbf{Field}/F$. The morphisms are field homomorphisms $f : K \to L$ for which $f(x) = x$ for all $x \in F$, i.e. *F-homomorphisms.*

If K/F is a field extension, then K is a vector space over F and F-homomorphisms are also linear maps of vector spaces over F. However, not every F-linear map defines an F-homomorphism.

Definition 3.1.3 (Degree)**.** The *degree* of a field extension K/F is $[K : F] = \dim_F K$.

Example 3.1.4.

1. $[K : F] = 1$ if and only if $K = F$.
2. $[\mathbb{C} : \mathbb{R}] = 2$ since $\{1, i\}$ is a basis for $\mathbb{C}$ as a real vector space.
3. $[\mathbb{Q} : \mathbb{R}]$ is (uncountably) infinite.

Proposition 3.1.5 (Tower law)**.** *Let $L/K/F$ be a tower of field extensions. Then $[L : F] = [L : K][K : F]$.*

Proof. Let (x_i) be a basis for K/F and (y_j) be a basis for L/K. We claim that $(x_i y_j)$ is a basis for L/F. For linear independence, suppose that $\sum_{i,j} a_{ij} x_i y_j = 0$ with $a_{ij} = 0$ for all but finitely many i, j. Then $\sum_j (\sum_i a_{ij} x_i) y_j = 0$ with each coefficient of y_j in K. Since (y_j) is linearly independent, $\sum_i a_{ij} x_i = 0$ for all j. Since (x_i) is linearly independent, $a_{ij} = 0$ for all i, j.

To see that $(x_i y_j)$ generate L/F, let $z \in L$. Since (y_j) spans L over K, we can find $b_j \in K$ for which $z = \sum_j b_j y_j$. Since (x_i) spans K over L, we can find $a_{ij} \in F$ for which $b_j = \sum_i a_{ij} x_i$ for each j. Then $z = \sum_{i,j} a_{ij} x_i y_j$. □

Corollary 3.1.6. *If $L/K/F$ is a tower of field extensions and $[L : F]$ is finite, then $[L : K]$ and $[K : F]$ divide $[L : F]$.*

Corollary 3.1.7. *If $L/K/F$ is a tower of field extensions and $[L : F]$ is prime, then $K = L$ or $K = F$.*

Let K be a field and $S \subset K$ be a subset. The smallest subfield of K containing S exists and is the intersection of all subfields of K containing S. This is the subfield generated by S.

Let K/F be a field extension and $S \subset K$ be a subset. Denote by $F(S)$ the subfield of K generated by $F \cup S$. Then $K/F(S)/F$ is a tower of field extensions. We say that $F(S)$ is the subfield of K generated by S over F.

Proposition 3.1.8. *Let K/F be a field extension and $\alpha_1, \dots, \alpha_n \in K$. Then*

$$F(\alpha_1, \dots, \alpha_n) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f, g \in F[x_1, \dots, x_n] \text{ and } g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}.$$

Proof. Let L be the right hand side. Then $L \subset K$ is a field and $F \cup \{\alpha_1, \dots, \alpha_n\} \subset L$, so $F(\alpha_1, \dots, \alpha_n) \subset L$. For the other inclusion, by direct computation, $F(\alpha_1, \dots, \alpha_n)$ must contain all polynomials expressions of $\alpha_1, \dots, \alpha_n$, and hence also all rational function expressions, so $F(\alpha_1, \dots, \alpha_n)$ contains L. □

Let K/F be a field extension and $\alpha_1, \dots, \alpha_n \in K$. Write $F[\alpha_1, \dots, \alpha_n] = \{f(\alpha_1, \dots, \alpha_n) \mid f \in F[x_1, \dots, x_n]\}$. This is a subring of K containing F, and $F[\alpha_1, \dots, \alpha_n] \subset F(\alpha_1, \dots, \alpha_n)$. Equality holds if and only if $F[\alpha_1, \dots, \alpha_n]$ is a field.

Example 3.1.9.

1. $\mathbb{R}[i] = \mathbb{C} = \mathbb{R}(i)$.
2. $F(x)$, the quotient field of $F[x]$, is not equal to $F[x]$ since $1/x \notin F[x]$ but $1/x \in F(x)$.

Definition 3.1.10 (Algebraic extension)**.** Let K/F be a field extension. We say that $\alpha \in K$ is *algebraic over F* if there is a non-zero $f \in F[x]$ such that $f(\alpha) = 0$. Otherwise, we say that α is *transcendental over F*. We say that K/F is an *algebraic extension* if every $\alpha \in K$ is algebraic over F.

Example 3.1.11.

1. All elements in F are algebraic over F.
2. All complex numbers are algebraic over $\mathbb{R}$.
3. For $F(x)/F$, the element x is transcendental over F.
4. Let $L/K/F$ be a tower of field extensions. If $\alpha \in L$ is algebraic over F, then α is algebraic over K.
5. If K/F is a field extension and $\alpha \in K$ is transcendental over F, then the ring homomorphism $F[x] \to F[\alpha]$ is an isomorphism. Moreover, $F(x) \cong F(\alpha)$.

Theorem 3.1.12. *Let K/F be a field extension and $\alpha \in K$ be algebraic over F.*

1. *There is a unique monic irreducible polynomial $m_\alpha \in F[x]$ such that $m_\alpha(\alpha) = 0$.*
2. *If $f \in F[x]$ is such that $f(\alpha) = 0$, then $m_\alpha \mid f$ in $F[x]$.*
3. *$F[\alpha] = F(\alpha)$.*
4. *If $n = \deg m_\alpha$, then $[F(\alpha) : F] = n$ with $\{1, \alpha, \dots, \alpha^{n-1}\}$ as a basis for $F(\alpha)$ over F.*

Proof.

1. The set I of all $f \in F[x]$ such that $f(\alpha) = 0$ forms an ideal of $F[x]$, which is a PID. Since α is algebraic, $I \neq 0$, so $I = m_\alpha \cdot F[x]$ for a unique monic polynomial m_α. If $m_\alpha \mid fg$ for some $f, g \in F[x]$, then $f(\alpha) = 0$ or $g(\alpha) = 0$, so m_α divides one of them. This shows that m_α is prime, hence irreducible.
2. If $f(\alpha) = 0$, then $f \in I$, so $m_\alpha \mid f$.

3. Consider the homomorphism $h : F[x] \to K$ given by $f \mapsto f(\alpha)$. Then $\operatorname{Ker} h = m_\alpha \cdot F[x]$, so $F[x]/m_\alpha \cdot F[x] \cong F[\alpha]$. Since m_α is prime and non-zero, $m_\alpha \cdot F[x]$ is prime and non-zero, hence maximal as $F[x]$ is a PID. Thus $F[\alpha]$ is a field, so $F[\alpha] = F(\alpha)$.

4. We have $[F(\alpha) : F] = \dim_F F[\alpha] = \deg m_\alpha$. To see that $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis for $F[\alpha]$, it is enough to show linear independence. Suppose $a_0, \dots, a_{n-1}$ satisfy

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0, \qquad f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}.$$

Then $m_\alpha \mid f$ but $\deg f \leq \deg m_\alpha$, so $f = 0$. □

Definition 3.1.13 (Minimal polynomial)**.** m_α is the *minimal polynomial* of α.

Remark 3.1.14. The proof of the theorem shows that $F(\alpha) \cong F[x]/m_\alpha \cdot F[x]$. If we are not given α in a larger extension, but we have some $f \in F[x]$ which is monic irreducible, then $K = F[x]/f \cdot F[x]$ is a field. Defining a map $F \to K$ by $a \mapsto a + f \cdot F[x]$, we see that K/F is a field extension of degree $\deg f$. If $\alpha = x + f \cdot F[x] \in K$, then $K = F(\alpha)$ and $f = m_\alpha$.

Example 3.1.15. 1. If $\deg m_\alpha = 1$, then $m_\alpha = x - \alpha$, so $\alpha \in F$.

2. If $\alpha = \sqrt{3} \in \mathbb{R}$ as an extension of $\mathbb{Q}$, then $m_\alpha = x^2 - 3$ and $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

3. Let p be prime and $\xi_p = e^{2\pi i/p} \in \mathbb{C}$. Then ξ_p is a root of $x^p - 1 = (x-1)(x^{p-1} + \cdots + 1)$ and $\xi_p \neq 1$, so ξ_p is a root of the second factor. This is irreducible, so $m_{\xi_p} = x^{p-1} + \cdots + 1$. Hence $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$.

4. For $p = 3$, we have $\xi_p = (-1 + \sqrt{-3})/2$, so $\mathbb{Q}(\xi_p) = \mathbb{Q}(\sqrt{-3})$.

Corollary 3.1.16. *Let K/F be a field extension of F. Then α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.*

Proof. ($\Longrightarrow$) If α is algebraic, then $[F(\alpha) : F] = \deg m_\alpha < \infty$.

($\Longleftarrow$) Since $n = [F(\alpha) : F] < \infty$, the elements $1, \alpha, \dots, \alpha^n$ are linearly dependent, so there exist $a_0, \dots, a_n$ not all zero with $\sum_i a_i \alpha^i = 0$. If $f = \sum_i a_i x^i$, then $f(\alpha) = 0$ and $f \neq 0$, so α is algebraic. □

Corollary 3.1.17. *Finite field extensions are algebraic.*

Proof. Let K/F be a finite field extension and $\alpha \in K$. Then $[F(\alpha) : F] \leq [K : F] < \infty$, so α is algebraic. □

Corollary 3.1.18. *Let K/F be a field extension and $\alpha_1, \dots, \alpha_n \in K$ be algebraic over F. Then $[F(\alpha_1, \dots, \alpha_n) : F] < \infty$.*

Proof. We induct on n. The case $n = 1$ is known. Then, let $E = F(\alpha_1, \dots, \alpha_{n-1})$. By induction, E/F is finite. Since α_n is algebraic over F, it is also algebraic over E, so $F(\alpha_1, \dots, \alpha_n) = E(\alpha_n)$ is a finite extension over E. Hence

$$[F(\alpha_1, \dots, \alpha_n) : F] = [E(\alpha_n) : E][E : F] < \infty.$$ □

Theorem 3.1.19. *Let K/F be a field extension. The set of all elements of K algebraic over F is a subfield of K.*

Proof. Let $\alpha, \beta \in K$ be algebraic over F. Then $F(\alpha,\beta)/F$ is algebraic, so $\alpha+\beta, \alpha\beta, -\alpha, \alpha^{-1} \in F(\alpha,\beta)$ are algebraic. □

Theorem 3.1.20. *If K/F and L/K are algebraic, then L/F is algebraic.*

Proof. Let $\alpha \in L$. Since α is algebraic over K, there exists $f = x^n + \beta_{n-1}x^{n-1} + \cdots + \beta_0$ with $\beta_i \in K$ for which $f(\alpha) = 0$. Then $E = F(\beta_0, \ldots, \beta_{n-1})$ is a finite extension of F since β_i is algebraic over F for each i, and α is algebraic over E by construction, so $E(\alpha)/E$ is finite. Hence $E(\alpha)/F$ is finite, so α is algebraic over F. □

Let $\mathcal{P}$ be a property of field extensions. One could say that $\mathcal{P}$ is *good* if, for a tower of field extensions $L/K/F$, the extension L/F has property $\mathcal{P}$ if and only if both L/K and K/F do. We have proved that the property to be algebraic (respectively, finite) is good.

3.2 Splitting fields

Theorem 3.2.1. *Let $f \in F[x]$ be non-constant of degree n. Then there is a field extension K/F such that $[K : F] \leq n$ and f has a root in K.*

Proof. Since f is non-constant, it has a monic irreducible divisor g. Set $K = F[x]/g \cdot F[x]$. □

Recall that a nonconstant polynomial $f \in F[x]$ is split (over F) if f is a product of linear factors in $F[x]$, i.e., $f = a(x-a_1)\cdots(x-a_n)$ with $a, a_1, \ldots, a_n \in F$. Note that a is the highest coefficient of f and $a_1, \ldots, a_n$ are all roots of f in F as well as in every field extension of F.

Corollary 3.2.2. *Let $f \in F[x]$ be non-constant of degree n Then there is a field extension K/F such that $[K : F] \leq n!$ and f is split over K, i.e. f is a product of linear factors in $K[x]$.*

Definition 3.2.3 (Extension of homomorphisms)**.** Let $\varphi : F \to F'$ be a field homomorphism, K/F be a field extension, and $\psi : K \to K'$ be another homomorphism. We say that ψ is an *extension* of φ if $\psi(x) = \varphi(x)$ for all $x \in F$.

If ψ is an extension of id_F, so that $\psi(x) = x$ for all $x \in F$, then ψ is an *F-homomorphism*, i.e. a morphism in the category of field extensions of F.

$$\begin{tikzcd}
 & K' \arrow[dd, dash] \\
K \arrow[ur, "\psi"] \arrow[dd, dash] & \\
 & F' \\
F \arrow[ur, "\varphi"] &
\end{tikzcd}$$

Proposition 3.2.4. *Let $K = F(\alpha)/F$ be a finite extension, $\varphi : F \to F'$ be a field homomorphism, and K'/F' be a field extension.*

1. *If $\psi : K \to K'$ is an extension of φ, then $\psi(\alpha)$ is a root of $\varphi(m_\alpha) \in F'[x]$.*

2. *For every root $\beta \in K'$ of $\varphi(m_\alpha)$, there exists a unique extension $\psi : K \to K'$ of φ with $\psi(\alpha) = \beta$.*

Proof. 1. Since $m_\alpha(\alpha) = 0$, we have $0 = \psi(m_\alpha(\alpha)) = \varphi(m_\alpha)(\psi(\alpha))$ since ψ extends φ and $m_\alpha \in F[x]$.

2. Define a map $\sigma : F[x] \to K'$ by $g \mapsto \varphi(g)(\beta)$. Then σ is a homomorphism that factors through $F[x]/m_\alpha \cdot F[x] \cong F(\alpha)$ to give a homomorphism $\psi : F(\alpha) \to K'$ with $\psi(\alpha) = \sigma(x) = \beta$. For $a \in F$, we have $\psi(a) = \sigma(a) = \varphi(a)$, so ψ extends φ.

   Uniqueness is clear since K is generated by α, so any extension is determined by the image of α. □

Corollary 3.2.5. *For $K = F(\alpha)$, the number of extensions $\psi : K \to K'$ of $\varphi : F \to F'$ is at most $[K : F]$.*

Definition 3.2.6 (Splitting field)**.** Let $f \in F[x]$ be non-constant of degree n. A field extension K/F is a *splitting field* of f over F if

(i) f is split over K, i.e., $f = a(x - \alpha_1) \cdots (x - \alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in K$;

(ii) $K = F(\alpha_1, \ldots, \alpha_n)$.

Example 3.2.7. Let $f \in F[x]$ be a non-constant polynomial and L/F a field extension of F such that f is split over L. Then the field $K := F(\alpha_1, \ldots, \alpha_m)$, where $\alpha_1, \ldots, \alpha_m$ are all roots of f in L is a splitting field of f.

Theorem 3.2.8. *Let $f \in F[x]$ be non-constant of degree n. Then f admits a splitting field of degree at most $n!$ over F.*

Proof. There is a field extension L/F of degree at most $n!$ such that f splits in $L[x]$. Set $K := F(\alpha_1, \ldots, \alpha_m)$, where $\alpha_1, \ldots, \alpha_m$ are all roots of f in L. □

Example 3.2.9. Let $f = x^2 - 3 \in \mathbb{Q}[x]$. Then $\mathbb{Q}(\sqrt{3})$ is a splitting field of f.

Theorem 3.2.10. *Let K/F be a splitting field of a non-constant $f \in K[x]$ and $\varphi : F \to F'$ be a field isomorphism. Let K'/F' be a splitting field of $\varphi(f) \in F'[x]$. Then there is an isomorphism $\psi : K \to K'$ extending φ.*

Proof. We induct on $n = \deg f$. If $n = 1$, then $K = F$ and $K' = F'$, so we can take $\psi = \varphi$.

Let $\alpha \in K$ be a root of f and write $f = (x - \alpha) \cdot g$ for some $g \in F(\alpha)[x]$. Since $m_\alpha \mid f$, we have $\varphi(m_\alpha) \mid \varphi(f)$ in $F'[x]$. As $\varphi(f)$ splits in $K'[x]$, we also have that $\varphi(m_\alpha)$ splits in $K'[x]$. Let β be a root of $\varphi(m_\alpha)$. There is a unique extension $\rho : F(\alpha) \to F'(\beta)$ of φ such that $\rho(\alpha) = \beta$, and since ρ

is surjective, it is an isomorphism.

$$\begin{tikzcd}
K \arrow[r, dashed, "\psi"] \arrow[d, dash] & K' \arrow[d, dash] \\
F(\alpha) \arrow[r, "\rho"] \arrow[d, dash] & F'(\beta) \arrow[d, dash] \\
F \arrow[r, "\varphi"] & F'
\end{tikzcd}$$

Since K is a splitting field of f, one can check that $K/F(\alpha)$ is a splitting field of g and $K'/F'(\beta)$ is a splitting field for $\varphi(g)$. The result follows by induction. □

Corollary 3.2.11. *If K and K' are splitting fields for a non-constant $f \in F[x]$, then K and K' are F-isomorphic.*

3.3 Finite fields

Definition 3.3.1 (Characteristic)**.** Let R be a ring. The kernel of the unique homomorphism $\mathbb{Z} \to R$ has the form $n\mathbb{Z}$ for some $n \geq 0$. The *characteristic* of R, denoted $\operatorname{char} R$, is n.

Proposition 3.3.2. *The characteristic of a field F is 0 or p for a prime p.*

Proof. Let $f : \mathbb{Z} \to F$ be the unique homomorphism and let $\operatorname{Ker} f = n\mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z} \cong \operatorname{Im} f \subset F$, and since F is a domain, $n\mathbb{Z} \subset \mathbb{Z}$ is a prime ideal. Hence $n = 0$ or $n = p$ for a prime p. □

Definition 3.3.3 (Prime subfield)**.** Let F be a field. The *prime subfield* of F is the smallest subfield of F.

Proposition 3.3.4. 1. *If $\operatorname{char} F = 0$, then the prime subfield of F is isomorphic to $\mathbb{Q}$.*

2. *If $\operatorname{char} F = p$ for $p > 0$ prime, then the prime subfield of F is isomorphic to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Corollary 3.3.5. *If $\operatorname{char} F = 0$, then F is infinite.*

Definition 3.3.6 (Multiplicity)**.** Let $f \in F[x]$ and $a \in F$ be a root of f. Write $f = (x-a)^k \cdot g$ for some $g \in F[x]$ with $g(a) \neq 0$. The *multiplicity* of a is k. We say that a is a *simple root* if $k = 1$.

Definition 3.3.7 (Formal derivative)**.** If $f = a_n x^n + \cdots + a_1 x + a_0$, the *(formal) derivative* of f is

$$f' = n a_n x^{n-1} + \cdots + a_1.$$

Proposition 3.3.8. *If $f, g \in F[x]$ and $a \in F$, then $(f+g)' = f' + g'$, $(af)' = af'$, and $(fg)' = f'g + fg'$.*

Proposition 3.3.9. *Let $a \in F$ be a root of $f \in F[x]$. Then a is a simple root of f if and only if $f'(a) \neq 0$.*

Proof. Write $f = (x-a)^k \cdot g$, with $k \geq 1$ and $g(a) \neq 0$. Then $f' = k(x-a)^{k-1} \cdot g + (x-a)^k \cdot g'$, so $f'(a) \neq 0$ if and only if $k - 1 = 0$ and $k \cdot g(a) \neq 0$, which holds for $k = 1$. □

Corollary 3.3.10. *If* $\gcd(f, f') = 1$*, then* f *has no multiple roots.*

Let F be a finite field with $\operatorname{char} F = p > 0$ prime. Then F is a vector space over $\mathbb{F}_p$ of dimension $n = [F : \mathbb{F}_p]$, and $|F| = p^n$.

Theorem 3.3.11. *Let* p *be a prime,* $n > 0$*, and* $q = p^n$*. There is a field* $\mathbb{F}_q$*, unique up to isomorphism, with* $|\mathbb{F}_q| = q$*.*

Proof. For existence, let K be the splitting field of $f = x^q - x \in \mathbb{F}_p[x]$, and suppose $f = (x - \alpha_1) \cdots (x - \alpha_q) \in K[x]$. Since $f' = qx^{q-1} - 1 = -1$, the roots α_i are distinct. We claim that $K = \{\alpha_1, \ldots, \alpha_q\}$; it suffices to show that $\{\alpha_1, \ldots, \alpha_q\}$ is a field. It is clear that $0, 1 \in F$, so for closure under addition and multiplication, since $\alpha_i^q = \alpha_i$ for each i,

$$(\alpha_i + \alpha_j)^q - (\alpha_i + \alpha_j) = \alpha_i^q + \alpha_j^q - \alpha_i - \alpha_j = 0,$$
$$(\alpha_i \alpha_j)^q - \alpha_i \alpha_j = \alpha_i^q \alpha_j^q - \alpha_i \alpha_j = 0.$$

For uniqueness, it suffices to show that any field L with $|L| = q$ is a splitting field for $x^q - x \in \mathbb{F}_p[x]$. If $|L| = q$, then $|L^\times| = q - 1$, so $\alpha^{q-1} = 1$ for any $\alpha \in F^\times$. This shows that α is a root of $x^q - x$ for $\alpha \neq 0$, and it is clear that 0 is a root of the same polynomial, so L is a splitting field for $x^q - x$. □

Example 3.3.12. 1. $\mathbb{F}_p = \mathbb{Z}/p$, but $\mathbb{F}_{p^2} \neq \mathbb{Z}/p^2$.

2. To construct $\mathbb{F}_4$, which is a quadratic extension of $\mathbb{F}_2$, we must find an irreducible quadratic polynomial in $\mathbb{F}_2[x]$. The only such polynomial is $x^2 + x + 1$, so $\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2 + x + 1)$.

Notation. For an abelian group $(A, \cdot)$ and $n > 0$, write ${}_nA = \{a \in A \mid a^n = 1\} \subset A$.

Proposition 3.3.13. *Let* A *be a finite abelian group such that* $|{}_nA| \leq n$ *for all* n*. Then* A *is cyclic.*

Proof. Let $\mathrm{IF}(A) = \{f_1, \ldots, f_s\}$ with $f_1 \mid \cdots \mid f_s$. Then $|{}_{f_1}A| = f_1^s$, so $s = 1$. □

Corollary 3.3.14. *If* F *is a field, then every finite subgroup of* $F^\times$ *is cyclic.*

Proof. If $A \subset F^\times$ and $n > 0$, then ${}_nA = \{x \in F \mid x^n - 1\} \cap A$, so $|{}_nA| \leq n$. □

Example 3.3.15. $(\mathbb{F}_q)^\times$ is cyclic of order $q - 1$, in particular $(\mathbb{Z}/p)^\times$ is cyclic of order $p - 1$.

Definition 3.3.16 (Simple extension)**.** A field extension K/F is *simple* if $K = F(\alpha)$ for some $\alpha \in K$.

Corollary 3.3.17. *Every extension of finite fields is simple.*

Proof. Let K/F be an extension of finite fields. Since K is finite, $K^\times$ is cyclic, so if $\alpha \in K^\times$ is a generator, then $K = F(\alpha)$. □

Corollary 3.3.18. *For every* n*, there is an irreducible polynomial* $f \in \mathbb{F}_p[x]$ *of degree* n*.*

Proof. Let $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, where $q = p^n$. Then m_α is irreducible of degree n. □

3.4 Normal extensions

Lemma 3.4.1. *Let E/F be a finite field extension and $\varphi : F \to L$ be a homomorphism. Then there is a finite field extension M/L and a homomorphism $\psi : E \to M$ extending φ.*

$$\begin{tikzcd}
 & M \arrow[dd, dashed] \\
E \arrow[ur, dashed, "\psi"] \arrow[dd, dash] & \\
 & L \\
F \arrow[ur, "\varphi"] &
\end{tikzcd}$$

Proof. Since E/F is finite, we can write $E = F(\alpha_1, \dots, \alpha_n)$ and induct on n. For $n = 0$, we have $E = F$, so we can take $M = L$ and $\psi = \varphi$.

For the general step, let $F_1 = F(\alpha_1)$ and $f = m_{\alpha_1} \in F[x]$, then let L_1 be the splitting field of $\varphi(f)$, which is a finite extension of L. In L_1, we have that $\varphi(\alpha_1) \in L_1$ is a root of $\varphi(f)$. Hence there is a unique extension $\varphi_1 : F_1 \to L_1$ of φ such that $\varphi_1(\alpha_1) = \varphi(\alpha_1)$. Since $E = F_1(\alpha_2, \dots, \alpha_n)$, by induction, there is a finite field extension M/L_1 and homomorphism $\psi : E \to M$ extending φ_1. Then ψ extends φ and M/L is finite. □

Proposition 3.4.2. *Let E/F be a finite field extension. The following are equivalent:*

(1) E is a splitting field of some polynomial in $F[x]$;

(2) for any field extension M/E and F-homomorphism $\sigma : E \to M$, we have $\sigma(E) = E$;

(3) if $f \in F[x]$ is irreducible and f has a root in E, then f splits in $E[x]$.

Proof. (1) $\implies$ (2) Let E be the splitting field of $f \in F[x]$, so $f = (x - \alpha_1) \cdots (x - \alpha_n)$ with $\alpha_i \in E$ and $E = F(\alpha_1, \dots, \alpha_n)$. For all i,

$$0 = (\sigma f)(\sigma(\alpha_i)) = f(\sigma(\alpha_i)),$$

so $\sigma(\alpha_i) = \alpha_{j(i)} \in E$. Since the α_i generate E over F, we have $\sigma(E) \subset E$. Since $\sigma : E \to E$ is F-linear, E/F is finite, and σ is injective, σ is an isomorphism, so $\sigma(E) = E$.

(2) $\implies$ (3) Suppose $f \in F[x]$ is irreducible and $f(\alpha) = 0$ for some $\alpha \in E$. Let L/E be a splitting field for f over E and $\beta \in L$ be any root of f. Then there is a unique F-homomorphism $\varphi : F(\alpha) \to L$ with $\varphi(\alpha) = \beta$. By the lemma, there is a finite extension M/L and $\psi : E \to M$ extending φ.

$$\begin{tikzcd}
 & M \arrow[d, dash] \\
 & L \arrow[d, dash] \\
E \arrow[uur, "\psi"] \arrow[d, dash] & E \arrow[dd, dash] \\
F(\alpha) \arrow[uur, "\varphi"] \arrow[d, dash] & \\
F \arrow[r, equal] & F
\end{tikzcd}$$

Since $\psi(E) = E$, we have $\beta = \psi(\alpha) \in E$. Hence all roots of f are in E, so f splits in $E[x]$.

(3) $\Longrightarrow$ (1) Let $E = F(\alpha_1, \dots, \alpha_n)$ and $f_i = m_{\alpha_i} \in F[x]$. Each f_i is split over E, so $f = f_1 \cdots f_n \in F[x]$ is split over E. As all roots of f are in E, and E is generated by the roots $\alpha_1, \dots, \alpha_n$, in fact E is generated by all roots of f, so E is the splitting field of f. □

Definition 3.4.3 (Normal extension)**.** A finite extension E/F is *normal* if all these conditions (1), (2) and (3) hold.

Corollary 3.4.4 (Test for normality)**.** *If $E = F(\alpha_1, \dots, \alpha_n)$, then E/F is normal if and only if m_{α_i} splits in $E[x]$ for all i.*

Example 3.4.5.

1. F/F is normal.

2. If $[E : F] = 2$, then $E = F(\alpha)$ for any $\alpha \in E \backslash F$. Then $m_\alpha = (x - \alpha)(x - \beta)$ is split over E, so E/F is normal.

3. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal, as the minimal polynomial $x^3 - 2$ of $\sqrt[3]{2}$ does not split in $\mathbb{Q}(\sqrt[3]{2})[x]$. More generally, $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ is not normal for $n \geq 3$.

4. The extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are normal, as both are quadratic, but $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal. Thus, the property to be normal is not good.

5. The extension $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$, where $\omega = e^{2\pi i/3}$, is normal, as it is the splitting field for $x^3 - 2$. While $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})$ is quadratic, hence normal, the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.

Proposition 3.4.6. *Let $L/E/F$ be a tower of extensions. If L/F is normal, then L/E is normal.*

Proof. If L is the splitting field of $f \in F[x]$, then it is also the splitting field of $f \in E[x]$. □

Definition 3.4.7 (Normal closure)**.** Let E/F be a finite extension. A finite extension L/E is a *normal closure* of E/F if L/F is normal and, for any L' with $E \subset L' \subset L$, if L'/F is normal, then $L' = L$.

Example 3.4.8.

1. If E/F is normal, then its normal closure is itself.

2. $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a normal closure of $\mathbb{Q}(\sqrt[3]{2})$.

Proposition 3.4.9. *The normal closure of a finite extension E/F exists and is unique up to E-isomorphism.*

Proof. Let L/E be an extension with L/F normal, $E = F(\alpha_1, \dots, \alpha_n)$, and $f = m_{\alpha_1} \cdots m_{\alpha_n} \in F[x]$. Then f is split over L, as L contains the root α_1 of f, so L contains the splitting field K of f. Hence K is the normal closure of E/F, which is unique up to E-isomorphism, as K is also the splitting field of f over E. □

3.5 Separable extensions

Lemma 3.5.1. *Let $f \in F[x]$ be non-constant. Then the following are equivalent:*

(1) f and f' are relatively prime;

(2) f has no multiple roots over any extension K/F;

(3) there is an extension K/F such that f splits in $K[x]$ and f has no multiple roots in K.

Proof. (1) $\implies$ (2) If f, f' are relatively prime in $F[x]$, they are also relatively prime in $K[x]$, so f has no multiple roots in K.

(2) $\implies$ (3) Take K to be the splitting field of f.

(3) $\implies$ (1) If f splits in $K[x]$ and has no multiple roots in K, then f, f' are relatively prime in $K[x]$, hence in $F[x]$. □

Definition 3.5.2 (Separable polynomial)**.** A non-constant $f \in F[x]$ is *separable* over F if f satisfies any of these conditions.

Corollary 3.5.3. *1. Let K/F be an extension and $f \in F[x]$ be non-constant. Then f is separable over F if and only if f is separable over K.*

2. If f is separable and $g \mid f$ is non-constant, then g is separable.

3. An irreducible $f \in F[x]$ is separable if and only if $f' \neq 0$.

Example 3.5.4. If $\operatorname{char} F = p > 0$ and $a \in F \backslash F^p$, so $a \neq b^p$ for some $b \in F$, then $f = x^p - a$ is irreducible over F and $f' = 0$, so f is not separable. To see this explicitly, let K/F be a splitting field and suppose $\alpha \in K$ is a root, so $\alpha^p = a$. Then $(x - \alpha)^p = x^p - \alpha^p = x^p - a$.

Definition 3.5.5 (Perfect field)**.** A field F is *perfect* if either $\operatorname{char} F = 0$ or $\operatorname{char} F > 0$ and $F^p = F$.

Proposition 3.5.6. *If F is perfect and $f \in F[x]$ is irreducible, then f is separable.*

Proof. If $\operatorname{char} F = 0$, then this is clear. Otherwise, let $\operatorname{char} F = p > 0$ and suppose $f = \sum a_k x^k$ with $f' = 0$. For each non-zero term $a_k x^k$ in f, the corresponding term in f' is $k a_k x^{k-1}$, so $p \mid k$. Then $f(x) = g(x^p)$ for $g = \sum b_l x^l$, where $b_l = a_{pl}$. If $b_l = c_l^p$ for some $c_l \in F$, then $f(x) = g(x^p) = (\sum c_l x^l)^p$, contradicting irreducibility of f. □

Example 3.5.7. 1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are perfect.

2. $\mathbb{F}_q$ is perfect for $q = p^n$.

3. $\mathbb{F}_q(x)$ is not perfect.

Definition 3.5.8 (Separable element)**.** Let E/F be an extension and $\alpha \in E$ be algebraic. We say that α is *separable* over F if m_α is separable.

Example 3.5.9. If F is perfect, then every algebraic $\alpha \in E$ is separable.

Lemma 3.5.10. *Let $L/K/F$ be a tower of extensions and suppose $\alpha \in L$ is separable over F. Then α is separable over K.*

Proof. If $m_\alpha \in K[x]$ is the minimal polynomial of α over K, then m_α divides the minimal polynomial of α over F, which is separable, so m_α is separable. □

Lemma 3.5.11. *Let E/F be a finite extension and $\varphi : F \to L$ be a homomorphism. Then φ has at most $[E : F]$ extensions $\psi : E \to L$.*

$$\begin{tikzcd}
 & L \arrow[dd, equal] \\
E \arrow[ru, dashed, "\psi"] \arrow[dd, dash] & \\
 & L \\
F \arrow[ru, "\varphi"] &
\end{tikzcd}$$

Proof. Let $E = F(\alpha_1, \dots, \alpha_n)$ and induct on n. If $n = 1$, so $E = F(\alpha_1)$, there is a bijection between the set of extensions of φ and the set of roots of m_{α_1} in L, of which there are at most $[E : F]$.

For the induction step, any extension $\psi : E \to L$ restricts to an extension $\rho : F(\alpha_1) \to L$. For a given ρ, the number of extensions ψ of ρ is at most $[E : F(\alpha_1)]$, while the number of extensions ρ of φ is at most $[F(\alpha_1) : F]$. Hence the number of extensions ψ of φ is at most $[E : F(\alpha_1)][F(\alpha_1) : F] = [E : F]$. □

Definition 3.5.12 (Separable extension)**.** A finite extension E/F is *separable* if there is a field homomorphism $\varphi : F \to L$ that has exactly $[E : F]$ extensions $\psi : E \to L$.

Proposition 3.5.13. *Let $E = F(\alpha)/F$ be a finite extension. Then E/F is separable if and only if α is separable over F.*

Proof. ($\Longrightarrow$) Let $\varphi : F \to L$ have $[E : F] = \deg m_\alpha$ extensions $\psi : E \to L$. Then $\varphi(m_\alpha)$ has $\deg m_\alpha$ roots in L, so $\varphi(m_\alpha)$ splits in $L[x]$ into distinct linear factors, hence α is separable.

($\Longleftarrow$) Let L be the splitting field of m_α over F. Since m_α is split over L and has exactly $[E : F] = \deg m_\alpha$ roots in L, any $\varphi : F \to L$ has exactly $[E : F]$ extensions $\psi : E \to L$, so E/F is separable. □

Example 3.5.14. The extension $F(x)/F(x^p)$ is finite of degree p, so $F(x,y)/F(x^p, y^p)$ has degree p^2. If $\operatorname{char} F = p$ and $\varphi \in F(x, y)$, then $\varphi^p \in F(x^p, y^p)$, then $\deg m_\varphi \leq p$. Hence $F(x, y)/F(x^p, y^p)$ is finite and not simple.

Lemma 3.5.15. *Let F be an infinite field, L/F be a field extension, and $g \in L[x_1, \dots, x_n]$ be non-zero. Then there exist $a_1, \dots, a_n \in F$ such that $g(a_1, \dots, a_n) \neq 0$.*

Proof. We induct on n. For $n = 1$, since g has finitely many roots and F is infinite, we can find $a \in F$ with $g(a) \neq 0$. For the inductive step, since $g \neq 0$, we can write $g = g_0 + g_1 x_n + \cdots + g_m x_n^m$ for $g_i \in L[x_1, \dots, x_{m-1}]$ with $g_m \neq 0$. By induction, there exist $a_1, \dots, a_{n-1} \in F$ with $g_m(a_1, \dots, a_{m-1}) \neq 0$. Then $g(a_1, \dots, a_{n-1}, x_n)$ is non-zero in $L[x_n]$, so by the $n = 1$ case, there exists $a_n \in F$ with $g(a_1, \dots, a_n) \neq 0$. □

Remark 3.5.16. This result does not hold if F is finite. If $F = \mathbb{F}_q$, then $\alpha^{q^n} - \alpha = 0$ for all $\alpha \in \mathbb{F}_q$, but $x^{q^n} - x \neq 0$.

Corollary 3.5.17. *Let $f_1, \dots, f_m \in L[x_1, \dots, x_n]$ be distinct. Then there exist $a_1, \dots, a_n \in F$ such that the values $f_i(a_1, \dots, a_n)$ are distinct for $i = 1, \dots, m$.*

Proof. Apply the lemma to $g = \prod_{i<j}(f_i - f_j)$. □

Theorem 3.5.18. *Every (finite) separable field extension is simple.*

Proof. Let E/F be separable with $E = F(\alpha_1, \dots, \alpha_n)$. Then there exist a field L and a homomorphism $\varphi : F \to L$ with exactly $m = [E : F]$ extensions $\psi_i : E \to L$. Let $f = \alpha_1 x_1 + \cdots + \alpha_n x_n \in E[x_1, \dots, x_n]$ and $f_i = \psi_i(f) \in L[x_1, \dots, x_n]$. These are distinct, so if F is infinite, then there exist $a_1, \dots, a_n \in F$ such that the values $\beta_i = f_i(a_1, \dots, a_n) \in L$ are distinct. Let $\beta = \alpha_1 a_1 + \cdots + \alpha_n a_n$. By construction, $\psi_i(\beta) = \beta_i$ for each i, and these values are distinct, so there are at least m extensions $\psi_i|_{F(\beta)} : F(\beta) \to L$ of φ. Since $[F(\beta) : F] \leq [E : F] = m$, we must have equality, so $F(\beta) = E$. If F is finite, then every finite extension of F is simple. □

Now we prove that the property to be separable is good.

Theorem 3.5.19. *Let $E/K/F$ be a tower of finite extensions. Then E/F is separable if and only if E/K and K/F are separable.*

Proof. ($\Longrightarrow$) If E/F is separable, then so is E/K. For some field L and homomorphism $\varphi : F \to L$, there are exactly $[E : F]$ extensions $\psi : E \to L$ of φ. There are at most $[K : F]$ extensions $\rho : K \to L$ of φ, and for any such ρ, there are at most $[E : K]$ extensions $\psi : E \to L$ of ρ, hence at most $[E : K][K : F] = [E : F]$ extensions $\psi : E \to L$ of φ. Since we know there are exactly this many, we must have equality, so there are exactly $[K : F]$ extensions $\rho : K \to L$ of φ, hence K/F is separable.

($\Longleftarrow$) Let $E = K(\alpha)$ for some $\alpha \in E$. Since K/F is separable, there exists $\varphi : F \to L$ with exactly $m = [K : F]$ extensions $\psi_i : K \to L$. If $f = m_\alpha \in K[x]$ and $f_i = \psi(f) \in L[x]$, then let M/L be a splitting field of $f_1 \cdots f_m$.

$$\begin{tikzcd}
E = K(\alpha) \arrow[dd, dash] \arrow[dr, dashed] & \\
& M \arrow[dd, dash] \\
K \arrow[dd, dash] \arrow[dr, "\psi_i"] & \\
& L \\
F \arrow[ur, "\varphi"] &
\end{tikzcd}$$

The number of extensions $E \to M$ of ψ_i is the number of roots of f_i in M, which is $\deg f_i = [E : K]$ since M is a splitting field. Hence there are $[E : K][K : F] = [E : F]$ extensions of φ, so E/F is separable. □

Corollary 3.5.20. *Let E/F be a finite extension. The following are equivalent:*

(1) E/F is separable;

(2) every $\alpha \in E$ is separable over F;

(3) $E = F(\alpha_1, \dots, \alpha_n)$ for some α_i separable over F;

(4) $E = F(\alpha)$ for some α separable over F.

Proof. (1) $\implies$ (2) If $\alpha \in E$, then $F \subset F(\alpha) \subset E$ and E/F is separable, so $F(\alpha)/F$ is separable, which implies α is separable over F.

(2) $\implies$ (3) Since E/F is finite, $E = F(\alpha_1, \dots, \alpha_n)$ for some α_i, which must all be separable.

(3) $\implies$ (1) Each of the extensions $F(\alpha_1, \dots, \alpha_k)/F(\alpha_1, \dots, \alpha_{k-1})$ is separable, since α_k is separable over F, hence also over $F(\alpha_1, \dots, \alpha_{k-1})$. Thus E/F is separable.

(1) $\implies$ (4) Since E/F is separable, $E = F(\alpha)$ for some $\alpha \in E$ which is separable.

(4) $\implies$ (3) Trivial. □

Corollary 3.5.21. *Every finite extension of a perfect field is separable.*

Proof. Let F be perfect and E/F be a finite extension. For any $\alpha \in E$, the minimal polynomial m_α is irreducible, hence separable, so α is separable. Thus E/F is separable. □

3.6 Galois extensions

Definition 3.6.1 (Galois group)**.** Let E/F be a finite extension. The group of all field automorphisms of E over F is called the *Galois group of* E/F, denoted $\mathrm{Gal}(E/F)$.

Proposition 3.6.2. *1.* $|\mathrm{Gal}(E/F)| \le [E : F]$.

2. $|\mathrm{Gal}(E/F)| = [E : F]$ *if and only if* E/F *is normal and separable.*

Proof. 1. Every $\sigma \in \mathrm{Gal}(E/F)$ is an extension of the embedding $F \hookrightarrow E$, and there are at most $[E : F]$ such extensions.

2. ($\implies$) If $|\mathrm{Gal}(E/F)| = [E : F]$, then there are exactly $[E : F]$ extensions of $F \hookrightarrow E$, so E/F is separable. For normality, it suffices to show that for any extension M/E and F-homomorphism $\varphi : E \to M$, we have $\varphi(E) = E$. For $\sigma \in \mathrm{Gal}(E/F)$, if $\rho : E \hookrightarrow M$ is the inclusion, then $\{\rho \circ \sigma \mid \sigma \in \mathrm{Gal}(E/F)\}$ is the set of all extensions of id_F (by counting). Hence $\varphi \in \mathrm{Gal}(E/F)$ and $\varphi = \rho \circ \sigma$, so $\varphi(E) = \rho(\sigma(E)) = \rho(E) = E$.

($\impliedby$) By separability, there exists $\alpha \in E$ such that $E = F(\alpha)$. The minimal polynomial m_α of α is separable (since E/F is separable) and m_α is split (since E/F is normal). Hence the identity of F has exactly $\deg(m_\alpha) = [E : F]$ extensions $E \to E$, therefore, $|\mathrm{Gal}(E/F)| = [E : F]$. □

Definition 3.6.3 (Galois extension)**.** We say that the extension E/F is *Galois* if $|\mathrm{Gal}(E/F)| = [E : F]$, or equivalently if E/F is normal and separable.

Example 3.6.4. 1. $\mathbb{C}/\mathbb{R}$ is Galois with $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, z \mapsto \overline{z}\}$

2. If $\operatorname{char} F \neq 2$ and $a \in F \backslash F^2$, then $f = x^2 - a$ is irreducible and separable. The splitting field E/F of f is $E = F(\alpha) = F(\sqrt{a})$, where $\alpha^2 = a$, so $[E : F] = \deg f = 2$. By construction, E/F is separable and normal, hence Galois, so $\mathrm{Gal}(E/F) = \{\mathrm{id}_E, \sigma\}$ for some σ. Since $\sigma(f) = f$, we have that $\sigma(\alpha)$ is a root of f, so $\sigma(\alpha) = \pm\alpha$. If $\sigma(\alpha) = \alpha$, then $\sigma = \mathrm{id}_F$, so the non-identity element is determined by $\sigma(\alpha) = -\alpha$. A general element of E is of the form $a + b\alpha$, and $\sigma(a + b\alpha) = a - b\alpha$.

3. If $\operatorname{char} F = 2$ and $a \in F$, consider $f = x^2 + x + a$. This is separable, so if f is irreducible, its splitting field E/F is a Galois extension of F of degree 2. If α is a root of f, then the roots of f are α and $1 + \alpha$, so $E = F(\alpha)$. We have $\mathrm{Gal}(E/F) = \{\mathrm{id}_E, \sigma\}$ with $\sigma(\alpha) = 1 + \alpha$.

4. Let p be prime, $k \geq 1$, and $q = p^k$. The splitting field of $f = x^{q^n} - x$ over $\mathbb{F}_q$ is $\mathbb{F}_{q^n}$ This is normal and separable, hence Galois, so $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a group of order n. It is in fact cyclic, generated by $\sigma(x) = x^q$ (called the *Frobenius automorphism*). Indeed, if $\sigma^i = 1$, then $x^{q^i} = x$ for all $x \in \mathbb{F}_{q^n}$, hence $i \geq n$. It follows that σ is of order n.

Let E/F be Galois. Then E/F is separable, so $E = F(\alpha)$ for some $\alpha \in E$ and $\deg m_\alpha = [E : F] = n$. Since E/F is also normal, m_α is split over E, so m_α has exactly n distinct roots. Let $X = \{\alpha_1 = \alpha, \ldots, \alpha_n\}$ be the roots of m_α. Then $G = \mathrm{Gal}(E/F)$ acts on X, so there is a homomorphism $\rho : G \to S_n$. This is injective, as if $\sigma(\alpha_i) = \alpha_i$ for all i, then $\sigma = \mathrm{id}_E$ since $E = F(\alpha_1)$. Furthermore, for each i, there is a unique $\sigma \in G$ with $\sigma(\alpha) = \alpha_i$, so G acts transitively on X. The stabilizer of any root α_i is trivial by this uniqueness, so the action is simply transitive.

Example 3.6.5. 5. Consider $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ and let $\alpha = \sqrt{2+\sqrt{2}}$. The minimal polynomial of α is $(x^2-2)^2 - 2 = x^4 - 4x^2 + 2$, which is irreducible by Eisenstein. The extension is normal by computation (see homework problem), and any finite extension of $\mathbb{Q}$ is separable, so it is Galois. The Galois group G has order 4, and it contains the element $\sigma(\alpha) = \sqrt{2-\sqrt{2}}$. Then $\sigma(\sqrt{2}) = \sigma(\alpha^2 - 2) = -\sqrt{2}$, and

$$\sigma^2(\alpha) = \sigma(\sqrt{2-\sqrt{2}}) = \sigma\left(\frac{\sqrt{2}}{\alpha}\right) = \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = -\alpha,$$

so σ has order 4, hence generates G as a cyclic group.

6. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Then $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ by a contradiction argument, so $E/\mathbb{Q}$ is a separable extension of degree 4. Since it is the splitting field of $(x^2-2)(x^2-3)$, we have that $E/\mathbb{Q}$ is Galois, so $G = \mathrm{Gal}(E/\mathbb{Q})$ has order 4. It is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$, with $\sigma \in G$ determined by $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(\sqrt{3}) = \pm\sqrt{3}$.

7. Let $E = \mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$, a Galois extension of degree 6. Let $\sigma \in G = \mathrm{Gal}(E/\mathbb{Q})$ be given by $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ and $\sigma(\omega) = \omega$, and let $\tau \in G$ be complex conjugation. Then $\sigma\tau(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ while $\tau\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$, so G is not commutative. Therefore, $G \cong S_3$.

Definition 3.6.6 (Galois group of polynomial)**.** Let $f \in F[x]$ be separable and let E/F be a splitting field for f. Then E/F is Galois, and the *Galois group* of f is $\mathrm{Gal}(f) = \mathrm{Gal}(E/F)$.

If $\deg f = n$, then $\mathrm{Gal}(f) \hookrightarrow S_n$ by acting on the roots. Since splitting fields are unique up to F-isomorphism, the Galois group of f is well-defined.

Example 3.6.7. If f splits in $F[x]$, then $\mathrm{Gal}(f)$ is trivial.

Theorem 3.6.8 (Artin)**.** *Let E be a field and G be a finite group of automorphisms of E. Let $F = E^G$ be the fixed field of G, i.e. the set of all $x \in E$ such that $\sigma(x) = x$ for all $\sigma \in G$. Then F is a subfield of E and E/F is Galois with* $\mathrm{Gal}(E/F) = G$.

Proof. That F is a subfield of E is clear. We claim that if $\alpha \in E$, then α is separable over F and $[F(\alpha) : F] \leq |G|$. Consider $S = \{\sigma(\alpha) \mid \sigma \in G\} \subset E$ and let $f = \prod_{\beta \in S}(x - \beta) \in E[x]$. For $\beta \in S$ and $\sigma \in G$, we have $\sigma(\beta) \in S$, so

$$\sigma(f) = \prod_{\beta \in S}(x - \sigma(\beta)) = \prod_{\beta \in S}(x - \beta) = f.$$

Thus $f \in F[x]$ is separable and α is a root of f, so α is separable. Moreover, $[F(\alpha) : F] \leq |S| \leq |G|$. Since every $\alpha \in E$ is separable over F, we have that E/F is separable.

Next we show that $[E : F] \leq |G|$. Suppose otherwise, and let $\alpha_1, \dots, \alpha_n \in E$ be linearly independent over F with $n > |G|$. Then $[F(\alpha_1, \dots, \alpha_n) : F] \geq n > |G|$. Each α_i is separable over F, so $F(\alpha_1, \dots, \alpha_n)/F$ is separable. Hence there exists $\beta \in E$ with $F(\alpha_1, \dots, \alpha_n) = F(\beta)$. However, $[F(\beta) : F] \leq |G|$, a contradiction.

Finally, note that $G \subset \mathrm{Aut}_F E$, so

$$|G| \leq |\mathrm{Aut}_F E| \leq [E : F] \leq |G|.$$

This gives equality everywhere, so E/F is Galois and $G = \mathrm{Aut}_F E = \mathrm{Gal}(E/F)$. □

Example 3.6.9. 1. Let K be a field and $E = K(x_1, \dots, x_n)$. The group $G = S_n$ acts on E by permuting the x_i's, so if $F = E^{S_n}$, then E/F is Galois with $\mathrm{Gal}(E/F) = S_n$. In fact, $F = K(\phi_1, \dots, \phi_n)$, where

$$\phi_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k}$$

is the standard symmetric polynomial of degree k in n variables.

2. Let G be a finite group and embed $G \hookrightarrow S_n$. For $E = K(x_1, \dots, x_n)$ and $F = E^G$, we have that E/F is Galois and $\mathrm{Gal}(E/F) = G$. Since E/F is normal, it is the splitting field of some polynomial $f \in F[x]$, and $\mathrm{Gal}(f) = G$.

3. Let $\mathbb{Q} = F$. The *inverse Galois problem* asks whether there is a Galois extension $E/\mathbb{Q}$ with $\mathrm{Gal}(E/\mathbb{Q}) \cong G$ for any finite group G. It is known that every finite abelian group and every symmetric group can be realized.

Let E/F be a Galois extension and $G = \mathrm{Gal}(E/F)$. We construct the two maps between the following sets:

- The set of all fields L such that $F \subset L \subset E$;
- The set of all subgroups of G;

Given a field L with $F \subset L \subset E$, we obtain a subgroup of G given by $\{\sigma \in G \mid \sigma(x) = x \text{ for all } x \in L\} = \mathrm{Gal}(E/L)$. Conversely, given $H \in G$, we obtain a subfield L with $F \subset L \subset E$ by setting $L = E^H$.

Theorem 3.6.10. *The two maps are inverses to each other. (In particular, they are bijections.)*

Proof. Let L be an intermediate subfield of E/F. If $H = \mathrm{Gal}(E/L)$, then clearly $L \subset E^H$. Since E/E^H is Galois with $\mathrm{Gal}(E/E^H) = H$, we have $[E^H : L] = [E : L]/[E : E^H] = |H|/|H| = 1$, so $L = E^H$. Now let $H \leq G$ be a subgroup. Then the composition of maps gives $H \mapsto E^H \mapsto \mathrm{Gal}(E/E^H)$, which is H. □

Proposition 3.6.11. *Let E/F be a Galois extension and $G = \mathrm{Gal}(E/F)$.*

1. *$E^1 = E$ and $E^G = F$.*
2. *If $H_1 \leq H_2 \leq G$ are subgroups, then $E^{H_2} \subset E^{H_1}$.*
3. *If $H \leq G$ and $L = E^H$, then $[L : F] = [G : H]$.*
4. *If $\sigma \in G$ and $L = E^H$, then $E^{\sigma H \sigma^{-1}} = \sigma(L)$.*
5. *$H \trianglelefteq G$ if and only if $L = E^H/F$ is normal. In this case, L/F is Galois and $\mathrm{Gal}(L/F) \cong G/H$.*

Proof. 1, 2 and 3 are clear.
4. For any $\alpha \in E$ we have $\alpha \in E^{\sigma H \sigma^{-1}} \Leftrightarrow \sigma h \sigma^{-1}(\alpha) = \alpha$ for all $h \in H \Leftrightarrow h\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha)$ for all $h \in H \Leftrightarrow \sigma^{-1}(\alpha) \in E^H \Leftrightarrow \alpha \in \sigma(E^H)$.
5. If H in normal in G, then $L = \sigma(L)$ for all $\sigma \in G$ by 4. We get a homomorphism $G \to \mathrm{Gal}(L/F)$ by restriction, with kernel $H = \mathrm{Gal}(E/L)$, so G/H is isomorphic to a subgroup of $\mathrm{Gal}(L/F)$. We have the following inequalities:

$$|\mathrm{Gal}(L/F)| \geq |G/H| = [L : F] \geq |\mathrm{Gal}(L/F)|.$$

It follows that all these are equalities. In particular, L/F is Galois (hence normal) and the restriction homomorphism yields an isomorphism $G/H \xrightarrow{\sim} \mathrm{Gal}(L/F)$.
Conversely, if L/F is normal, then $\sigma(L) = L$ for all $\sigma \in G$, so $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$, hence H is normal. □

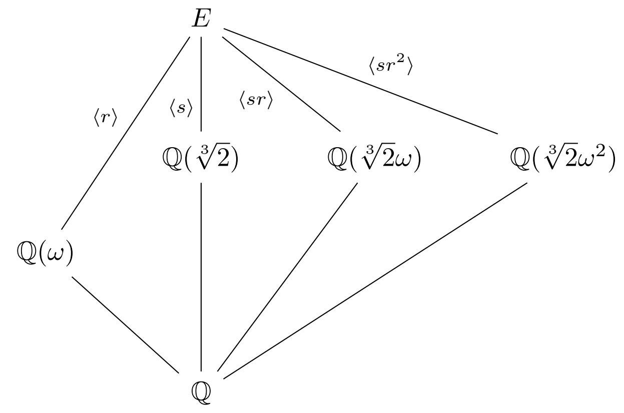
Example 3.6.12. 1. Let $E = \mathbb{Q}(\sqrt{2+\sqrt{2}})$, so $G = \mathrm{Gal}(E/\mathbb{Q}) = \langle \sigma \rangle$ is cyclic of order 4.

$$\begin{tikzcd}
E \arrow[d, dash, "2"] & & 1 \arrow[d, dash, "2"] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] & & \langle \sigma^2 \rangle \arrow[d, dash, "2"] \\
\mathbb{Q} & & G
\end{tikzcd}$$

2. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so $G = \mathrm{Gal}(E/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$.

$$\begin{tikzcd}
 & E \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & & & & 1 \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash, "2"] & & \langle \sigma \rangle \arrow[dr, dash, "2"'] & \langle \tau \rangle \arrow[d, dash, "2"] & \langle \sigma\tau \rangle \arrow[dl, dash, "2"] \\
 & \mathbb{Q} & & & & G &
\end{tikzcd}$$

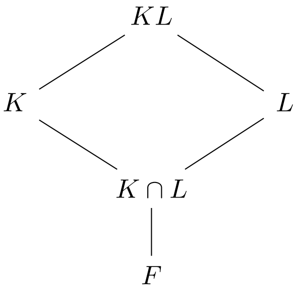
3. Let $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$, so $G = S_3 = \langle r, s \mid r^3, s^2, rsrs \rangle$. Suppose $s(\omega) = \omega^2$ and $s(\sqrt[3]{2}) = \sqrt[3]{2}$.



Definition 3.6.13 (Compositum)**.** Let $F \subset K, L \subset M$ be fields. The *compositum* KL of K and L is the smallest subfield of M containing K and L.

Proposition 3.6.14. *If $K = F(\alpha_1, \ldots, \alpha_n)$, then $KL = L(\alpha_1, \ldots, \alpha_n)$.*

Theorem 3.6.15. *If K/F is Galois, then KL/L is Galois. The restriction homomorphism r : $\mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/F)$ is injective with image $\mathrm{Gal}(K/K \cap L)$.*



Proof. Write $K = F(\alpha_1, \ldots, \alpha_n)$. Since K/F is separable, each α_i is separable over F. Then $KL = L(\alpha_1, \ldots, \alpha_n)$ with $\alpha_i \in KL$ separable over L, so KL/L is separable. Since K/F is normal, it is the splitting field of some $f \in F[x]$. Then KL/L is a splitting field of $f \in L[x]$. Hence KL/L is Galois.

Since K/F is normal, for any $\sigma \in \mathrm{Gal}(KL/L)$, the restriction of σ to a map $K \to KL$ must have $\sigma(K) = K$, so restriction gives $\sigma \in \mathrm{Gal}(K/F)$. To see that restriction is injective, suppose $\sigma \in \mathrm{Gal}(KL/L)$ acts as the identity on K. In particular $\sigma(\alpha_i) = \alpha_i$ for each α_i above, so σ acts as the identity on L. Finally, let $\tau \in H = \mathrm{Im}\, r$, so τ is the restriction of σ for some $\sigma \in \mathrm{Gal}(KL/L)$. Then σ fixes L, so τ fixes $K \cap L$, so $\tau \in \mathrm{Gal}(KL/L)$ and $H \subset \mathrm{Gal}(K/K \cap L)$. To get the reverse inclusion, note that $K^H \subset K \cap L$, as if $x \in K^H$, then $\sigma(x) = x$ for all $\sigma \in \mathrm{Gal}(KL/L)$, so $x \in (KL)^{\mathrm{Gal}(KL/L)} = L$. By the Galois correspondence, $H \supset \mathrm{Gal}(K/K \cap L)$. □

Definition 3.6.16 (Linearly disjoint extensions)**.** We say that K and L are *linearly disjoint* over F if $K \cap L = F$.

Corollary 3.6.17. *If K and L are linearly disjoint over F, then $r : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/F)$ is an isomorphism.*

Theorem 3.6.18. *If K/F and L/F are Galois, then KL/F is Galois and the restriction map $r : \mathrm{Gal}(KL/F) \to \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$ is injective. If K and L are linearly disjoint over F, then r is an isomorphism.*

Proof. Clearly, KL/F is separable. If K/F and L/F are splitting fields of polynomials f and g in $F[x]$ respectively, then KL/F is a splitting field of fg, hence KL/F is normal and therefore Galois. By Theorem 3.6.15, r is injective.

Suppose K and L are linearly disjoint over F and let $\sigma \in \mathrm{Gal}(K/F)$ and $\tau \in \mathrm{Gal}(L/F)$. By Theorem 3.6.15, there are $\overline{\sigma} \in \mathrm{Gal}(KL/L)$ and $\overline{\tau} \in \mathrm{Gal}(KL/K)$ such that $\overline{\sigma}|K = \sigma$ and $\overline{\tau}|L = \tau$. Then $r(\overline{\sigma}\overline{\tau}) = (\sigma, \tau)$, i.e., r is surjective. □

In fact, $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(KL/L)$ and $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(KL/K)$, both of which are subgroups of $\mathrm{Gal}(KL/F)$, satisfy

$$\mathrm{Gal}(KL/F) = \mathrm{Gal}(KL/L) \times \mathrm{Gal}(KL/K)$$

as an internal direct product.

3.7 Cyclotomic extensions

Let $n > 0$ and F be a field with $\operatorname{char} F \nmid n$. Since $f_n = x^n - 1$ and $f_n' = nx^{n-1}$ are relatively prime, f_n is separable. Therefore, the splitting field F_n of f_n is a Galois extension of F, the *n-th cyclotomic extension* of F. The set of roots μ_n in F_n, the n-th roots of unity, is a finite subgroup of $F^\times$, hence cyclic of order n, and the generators of μ_n are primitive n-th roots of unity. Let $\zeta_n \in \mu_n$ be primitive, so then $\mu_n = \{\zeta_n^k \mid 0 \leq k < n\}$. Therefore, $F_n = F(\zeta_n)$. Elements of the Galois group $G_n = \mathrm{Gal}(F_n/F) = \mathrm{Gal}(f_n)$ are of the form $\sigma(\zeta_n) = \zeta_n^k$ for $k \in \mathbb{Z}/n\mathbb{Z}$. Since ζ_n^k must be a primitive n-th root of unity in order for σ to be an automorphism, we must have $\gcd(k, n) = 1$. Thus we get a group homomorphism $\chi_n : G_n \to (\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 3.7.1. *χ_n is injective.*

Proof. If $\sigma \in \operatorname{Ker} \chi_n$, then $\chi_n(\sigma) = 1 + n\mathbb{Z}$, so $\sigma(\zeta_n) = \zeta_n^1 = \zeta_n$, hence $\sigma = \mathrm{id}_{F_n}$. □

Remark 3.7.2. By the proposition, G_n may be identified with a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, hence G_n is abelian. It turns out that depending on the choice of F, one can obtain any subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Now let $F = \mathbb{Q}$, and let $\Phi_n \in \mathbb{Q}[x]$ be the minimal polynomial of ζ_n, i.e. the *n-th cyclotomic polynomial* (over $\mathbb{Q}$). For some $\alpha \in \mathbb{Q}^\times$, we have that $\alpha\Phi_n \in \mathbb{Z}[x]$ is primitive. Since $\Phi_n \mid x^n - 1$, we have $x^n - 1 = \Phi_n\Psi_n = (\alpha\Phi_n)(\alpha^{-1}\Psi_n)$, hence $\alpha^{-1}\Psi_n \in \mathbb{Z}[x]$. The leading coefficient of $\alpha\Phi_n$ must then be ± 1, so $\alpha = \pm 1$ as Φ_n is monic. Hence $\Phi_n \in \mathbb{Z}[x]$.

Lemma 3.7.3. *Let p be a prime integer, $p \nmid n$. Then $(\zeta_n)^p$ is a root of Φ_n.*

Proof. Write $x^n - 1 = \Phi_n\Psi_n$ for some $\Psi_n \in \mathbb{Z}[x]$. If $\Phi_n(\zeta_n^p) \neq 0$, then $\Psi_n(\zeta_n^p) = 0$. Define $\Delta_n(x) = \Psi_n(x^p)$, so then $\Delta_n(\zeta_n) = 0$. Hence $\Phi_n \mid \Delta_n$ in $\mathbb{Z}[x]$. As polynomials modulo p, we have $(\overline{\Psi}_n)^p = \overline{\Delta}_n$ and $\overline{\Phi}_n \mid \overline{\Delta}_n$. If g is an irreducible divisor of $\overline{\Phi}_n$ in $\mathbb{F}_p[x]$, then $g \mid \overline{\Psi}_n$. Then $g^2 \mid x^n - 1$, but $x^n - 1$ is separable over $\mathbb{F}_p[x]$ since $p \nmid n$, a contradiction. □

Corollary 3.7.4. *Every primitive n-th root of unity is a root of Φ_n.*

Proof. Every primitive n-th root of unity has the form ζ_n^k with $\gcd(k, n) = 1$. The result follows by induction and writing k as a product of primes, none of which divide n. □

Theorem 3.7.5. $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ *and* $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Proof. Since every primitive n-th root of unity is a root of Φ_n,

$$\varphi(n) \le \deg \Phi_n = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| \le |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n).$$ □

Every $\zeta \in \mu_n$ has $\operatorname{ord} \zeta = d$ for some $d \mid n$. Therefore,

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta) = \prod_{d \mid n} \prod_{\zeta \in \mu_d \text{ primitive}} (x - \zeta) = \prod_{d \mid n} \Phi_d.$$

From this, we can inductively compute Φ_n.

$$\begin{aligned} \Phi_1 &= x - 1 & \Phi_4 &= x^2 + 1 \\ \Phi_2 &= x + 1 & \Phi_5 &= x^4 + x^3 + x^2 + x + 1 \\ \Phi_3 &= x^2 + x + 1 & \Phi_6 &= x^2 - x + 1 \end{aligned}$$

Remark 3.7.6. The first several cyclotomic polynomials have coefficients 0 and ±1. One can show that this holds for any n of the form $2^a p^k q^m$ where p, q are odd primes and $a, k, m \ge 0$. The first positive integer not of this form is 105, and it turns out that

$$\Phi_{105} = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} + \cdots - 2x^7 + \cdots.$$

3.8 Algebraically closed fields

Proposition 3.8.1. *Let F be a field. The following are equivalent:*

(1) every finite extension of F is trivial;

(2) every irreducible $f \in F[x]$ is linear;

(3) every non-constant $f \in F[x]$ has a root in F;

(4) every non-constant $f \in F[x]$ splits in $F[x]$.

Proof. (1) $\Longrightarrow$ (2) If f is irreducible, then $F[x]/fF[x]$ is an extension of F of degree $\deg f = 1$, so f is linear.

(2) $\Longrightarrow$ (3) If $f \in F[x]$ is non-constant, then f factors in $F[x]$ as a product of linear factors, hence has a root in F.

(3) $\Longrightarrow$ (4) If $f \in F[x]$ is non-constant, then it has a root $\alpha \in F$, so $f = (x - \alpha)g$ for some $g \in F[x]$. Induct on degree.

(4) $\implies$ (1) Let K/F be finite, $\alpha \in K$, and m_α be the minimal polynomial of α over F. Then m_α splits into linear factors and is irreducible, so $m_\alpha = x - \alpha$, so $\alpha \in F$. □

Definition 3.8.2 (Algebraically closed field)**.** A field F satisfying these properties is said to be *algebraically closed.*

Theorem 3.8.3. *$\mathbb{C}$ is algebraically closed.*

Proof. First we show that $\mathbb{R}$ has no non-trivial odd degree extensions. If $K/\mathbb{R}$ has odd degree, then $K = \mathbb{R}(\alpha)$ for some $\alpha \in K$ as K is separable. Then m_α has irreducible over $\mathbb{R}$ and has odd degree, so m_α has a root in $\mathbb{R}$ by the intermediate value theorem. Therefore, $m_\alpha = x - \alpha$, so $\alpha \in \mathbb{R}$ and $K = \mathbb{R}$.

Next we show that $\mathbb{C}$ has no quadratic extensions. If $K/\mathbb{C}$ is quadratic, say $K = \mathbb{C}(\alpha)$, then m_α is quadratic, but all quadratics are solvable over $\mathbb{C}$, a contradiction.

Now let $E/\mathbb{C}$ be any finite extension. It suffices to show that $E = \mathbb{C}$. By taking a normal closure if needed, we may assume that $E/\mathbb{R}$ is normal, hence Galois.

$$\begin{tikzcd}
E \arrow[d, dash] \\
\mathbb{C} \arrow[d, dash] \\
\mathbb{R}
\end{tikzcd}$$

Since $|G|$ is even, there is a non-trivial Sylow 2-subgroup $H \leq G$, so $[G : H] = [K^H : \mathbb{R}]$ is odd. Therefore, $E^H = \mathbb{R}$, so $H = G$ is a 2-group. Now let $N = \operatorname{Gal}(E/\mathbb{C})$. We have $N \leq G$ and $[G : N] = 2$. If N is a non-trivial 2-group, then N has a subgroup N' of index 2, and then $E^{N'}/\mathbb{C}$ has degree 2, a contradiction. If N is trivial, then $E = \mathbb{C}$. □

Definition 3.8.4 (Algebraic closure)**.** An extension F_{alg}/F is an *algebraic closure* of F if F_{alg} is algebraically closed and F_{alg}/F is algebraic.

Theorem 3.8.5. *Every field F admits an algebraic closure F_{alg}/F.*

Proof. Let x_f be a variable for $f \in F[x]$ non-constant monic, and let $A = F[\{x_f\}]$. Define an ideal $I \subset A$ generated by the polynomials $f(x_f)$.

We claim that $I \neq A$. To see this, suppose otherwise, and write $1 = \sum f(x_f) \cdot g_f$ for $g_f \in A$ with $g_f = 0$ for all but finitely many S. Let L/F be a finite extension for which all f with $g_f \neq 0$ have roots, so then $f(\alpha_f) = 0$ for some $\alpha_f \in L$. Substituting (α_f), the right hand side is 0, a contradiction.

Let $\mathfrak{m} \subset A$ be a maximal ideal containing I. Then $F_1 = A/\mathfrak{m}$ is an algebraic field extension of F, as it is generated by algebraic elements. Furthermore, every polynomial $f \in F[x]$ has a root in F_1. Now construct a sequence $F = F_0 \subset F_1 \subset \cdots$ inductively in this way, then take $F_{\text{alg}} = \bigcup_n F_n$. □

3.9 Galois groups of polynomials

Let $f \in F[x]$ be a non-constant separable polynomial, E/F be a splitting field of f, and $G = \mathrm{Gal}(f) = \mathrm{Gal}(E/F)$. Let $S = \{\alpha_1, \ldots, \alpha_n\}$ be the roots of f in E. Then G acts on S, so G embeds into S_n.

Lemma 3.9.1. *Let E/F be Galois, $G = \mathrm{Gal}(E/F)$, and $\alpha \in E$. If $T = \{\sigma(\alpha) \mid \sigma \in G\}$, then $\deg m_\alpha = |T|$ and $m_\alpha = \prod_{\beta \in T}(x - \beta)$.*

Proof. Consider the tower $E/F(\alpha)/F$ and let $H = \mathrm{Gal}(E/F(\alpha))$. Then $\deg m_\alpha = [F(\alpha) : F] = [G : H]$. Since G acts transitively on T, we have $|T| = [G : \mathrm{stab}\,\alpha] = [G : H]$.

Let $g = \prod_{\beta \in T}(x - \beta)$. Then $\sigma(g) = g$ for all $\sigma \in G$, so $g \in F[x]$. Furthermore, $g(\alpha) = 0$ and $\deg g = \deg m_\alpha$, so $g = m_\alpha$. □

Example 3.9.2. Let $\alpha = \sqrt{2} + \sqrt[3]{5}$. Then α lies in the extension $E = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}, \omega)/\mathbb{Q}$, the splitting field of $(x^2 - 2)(x^3 - 5)$. Since $E = \mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(\sqrt[3]{5}, \omega)$ as the compositum and these are linearly disjoint, so $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/2 \times S_3$. One can check that the orbit of α has size 6, so $\mathbb{Q}(\alpha)/\mathbb{Q}$ is of degree 6. By direct computation,

$$m_\alpha = (x^3 + 6x - 5)^2 - 2(3x^2 + 2)^2.$$

3.10 Radical extensions

Let $\mathrm{char}\, F = 0$ and $n > 0$. A finite extension E/F is *n-radical* if $E = F(\alpha)$ and $\alpha^n \in F$.

Example 3.10.1. Let E be the splitting field of $x^n - 1$, so $E = F(\zeta_n)$. Then E/F is n-radical, as $\zeta_n^n = 1 \in F$.

An extension E/F is *cyclic* if E/F is Galois with $\mathrm{Gal}(E/F)$ cyclic.

Proposition 3.10.2. *Suppose $\zeta_n \in F$, so F contains every n-th root of unity. Then every n-radical extension is cyclic.*

Proof. Since $\mu_n \in F$ and $E = F(\alpha)$ for some α with $\alpha^n = a \in F$, the roots of $x^n - a$ are $\zeta_n^k \alpha \in E$. Thus E/F is normal, hence Galois. Define $f : G = \mathrm{Gal}(E/F) \to \mu_n$ by $\sigma \in G \mapsto \sigma(\alpha)/\alpha \in \mu_n$. Then f is an injective homomorphism, so G is isomorphic to a subgroup of the cyclic group μ_n, hence cyclic. □

Let E/F be Galois with $G = \mathrm{Gal}(E/F)$. The vector space $\mathrm{End}_F(E)$ is also a vector space over E. Every element of G is an endomorphism of E over F, so G is a subset of $\mathrm{End}_F(E)$.

Lemma 3.10.3. *$G \subset \mathrm{End}_F(E)$ is linearly independent over E.*

Proof. Let $G = \{\sigma_1, \ldots, \sigma_n\}$ and suppose $\sum_i x_i \sigma_i = 0$ with $x_i \in E$. Without loss of generality, suppose $x_1, x_2 \neq 0$ and that the number of non-zero coefficients is at its minimum. For all $y \in E$, we have $\sum x_i \sigma_i(y) = 0$, so then $\sum x_i \sigma_i(yz) = (\sum_i x_i \sigma_i(y) \sigma_i)(z) = 0$ for any z. Multiplying the initial linear dependence by $\sigma_1(y)$, and choosing y so that $\sigma_1(y) \neq \sigma_2(y)$, we get by subtracting

$$\sum_{i=2}^{n} x_i(\sigma_i(y) - \sigma_1(y))\sigma_i = 0.$$

The number of non-zero coefficients is smaller, but not zero since $x_2(\sigma_2(y) - \sigma_1(y)) \neq 0$, so we have the required contradiction. □

Theorem 3.10.4 (Hilbert 90)**.** *Let E/F be cyclic of degree n. If $\zeta_n \in F$, then E/F is n-radical.*

Proof. Let $G = \mathrm{Gal}(E/F)$ be generated by σ of order n, then consider $\sum_{k=0}^{n-1} \zeta_n^{-k} \sigma^k \neq 0$. There exists $y \in E$ such that $\alpha = \sum_{k=0}^{n-1} \zeta_n^{-k} \sigma^k(y) \neq 0$, and we claim that $E = F(\alpha)$. To see this, note that $\sigma(\alpha) = \zeta_n \alpha$, so $\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n$. Hence $\alpha^n \in F$, so $F(\alpha)/F$ is n-radical. Moreover, the values $\sigma^k(\alpha) = \zeta_n^k \alpha$ are distinct, so $\deg \alpha = n$. Since $[E : F] = [F(\alpha) : F] = n$, we have $E = F(\alpha)$. □

Definition 3.10.5 (Radical extension)**.** An extension L/F is *radical* if there is a tower of extensions $F = E_0 \subset E_1 \subset \cdots \subset E_m = L$ for which each E_i/E_{i-1} is n_i-radical for some n_i.

Proposition 3.10.6. *1. If L/E and E/F are radical, then so is L/F.*

2. If L/F is radical, then for every K/F with K, L both in some larger field, KL/K is radical.

3. If $L = F(\alpha_1, \ldots, \alpha_k)$ with $\alpha_i^{n_i} \in F$, then L/F is radical.

Lemma 3.10.7. *Every radical extension L/F can be embedded in a normal radical extension E/F.*

Proof. Let $L = F(\alpha_1, \ldots, \alpha_m)$ with $\alpha_i^{n_i} \in E_{i-1} = F(\alpha_1, \ldots, \alpha_{i-1})$ for each i, and let $L = E_m$. We induct on m. When $m = 0$, we take $E = L = F$.

Suppose the result holds for $m - 1$. Then we can embed E_{m-1}/F into a normal radical extension K_{m-1}/F.

$$\begin{tikzcd}
 & K_m \arrow[dd, dash] \\
E_m \arrow[ur, dashed, "\psi"] \arrow[dd, dash] & \\
 & K_{m-1} \arrow[dl, dash] \arrow[ddl, dash] \\
E_{m-1} \arrow[d, dash] & \\
F &
\end{tikzcd}$$

Let K_{m-1} be the splitting field of $g \in F[x]$ over F, so K_{m-1}/F is Galois with $G = \mathrm{Gal}(K_{m-1}/F)$. Let $L = E_{m-1}(\alpha)$ with $\alpha^n = a \in E_{m-1}$ for some n and a. Let $h = \prod_\sigma \sigma(m_\alpha) \in F$. Define K_m to be the splitting field of h over K_{m-1}. Then gh splits in $K_m[x]$ and $gh \in F[x]$, and K_m is generated over F by all roots of gh, as the roots of g generate K_{m-1} over F and the roots of h generate K_m over K_{m-1}. Hence K_m/F is normal, so it remains to find an embedding of E_m into K_m. Since $f = m_\alpha \mid h$ and h is split over K_m, in particular f has a root in K_m. Using this root, we embed E_m into K_m. To see that K_m/F is radical, we have that K_m is generated over K_{m-1} by the roots of h. If β is a root of h, then $h(\beta) = 0$, so $(\psi f)(\beta) = 0$, hence $f(\psi^{-1}\beta) = 0$. Since $f \mid x^n - a$, we have $\psi^{-1}(\beta)^n = a$, so $\beta^n = \psi(a) \in K_{n-1}$. Thus $K_m = K_{m-1}(\beta)$ is n-radical. □

A polynomial $f \in F[x]$ is *solvable by radicals* if there is a radical extension E/F in which f splits.

Theorem 3.10.8. *Let $f \in F[x]$ be a non-constant polynomial. Then f is solvable by radicals if and only if $\mathrm{Gal}(f)$ is solvable.*

Proof. ($\Longrightarrow$) If f is solvable by radicals, then there is a radical extension L/F such that f is split in L. Replacing L with a normal closure if necessary, we can suppose that L/F is Galois. Let $E \subset L$ be the splitting field of f, so $\mathrm{Gal}(E/F) = \mathrm{Gal}(f)$. Let $n = [L : F]$, then define $F' = F(\zeta_n)$ and $L' = L(\zeta_n)$. Since L/F is radical, L'/F' is radical. Write $F' = L_0 \subset L_1 \subset \cdots \subset L_m = L'$, and set $G_i = \mathrm{Gal}(L'/L_i)$ for $i = 0, 1, \ldots, m$. Since $\zeta_n \in F'$, each L_i/L_{i-1} is Galois cyclic, so $G_i \trianglelefteq G_{i-1}$ with $\mathrm{Gal}(L_i/L_{i-1}) = G_{i-1}/G_i$ cyclic. Hence $\mathrm{Gal}(L'/F')$ is solvable. The extension F'/F is cyclotomic, hence abelian, so L'/F is solvable. Then E/F is solvable.

($\Longleftarrow$) If $G = \mathrm{Gal}(f) = \mathrm{Gal}(E/F)$ is solvable, where E/F is the splitting field of f, then let $n = |G|$. Set $F' = F(\zeta_n)$ and $E' = E(\zeta_n)$. Since $\mathrm{Gal}(E/F)$ is solvable, $\mathrm{Gal}(E'/F') \hookrightarrow \mathrm{Gal}(E/F)$ is solvable. Take a descending sequence of subgroups $\mathrm{Gal}(E'/F') = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = 1$ with G_{i-1}/G_i cyclic. Setting $E_i = (E')^{G_i}$, we obtain a tower of cyclic extensions, so E'/F' is radical. Since F'/F is cyclotomic, E'/F is radical. Hence E/F is radical. □

Example 3.10.9. Let $E = K(x_1, \ldots, x_n)$. Then S_n acts on E, and if $F = E^{S_n}$, then $\mathrm{Gal}(E/F) = S_n$. Consider $f = \prod_i (t - x_i) \in F[t]$. Then E/F is the splitting field of f, so f is not solvable by radicals for $n \geq 5$.

Proposition 3.10.10. *Let p be a prime and $f \in \mathbb{Q}[x]$ be irreducible of degree p such that f has exactly two non-real complex roots. Then $\mathrm{Gal}(f) = S_p$.*

Proof. Let $E \subset \mathbb{C}$ be a splitting field for f. If $\alpha \in \mathbb{C}$, then $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree p, so $p \mid |G|$ for $G = \mathrm{Gal}(E/\mathbb{Q})$. Since $G \hookrightarrow S_p$, we know that G has an element of order p, i.e. a p-cycle. Complex conjugation is also in G, and in S_p, it is a transposition since f has exactly two non-real complex roots, which are conjugate. Hence G has a p-cycle and a transposition, which generate all of S_p. □

Example 3.10.11. The polynomial $x^5 - 4x + 2$ is not solvable by radicals over $\mathbb{Q}$.

Lemma 3.10.12. *For every finite abelian group G, there exists n such that there is a surjective homomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \twoheadrightarrow G$.*

Proof. Write $G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}$. Find distinct primes $p_1, \ldots, p_s$ such that $p_i \equiv 1 \pmod{m_i}$. Take $n = p_1 \cdots p_s$. □

Corollary 3.10.13. *For every finite abelian group G, there is an extension $E/\mathbb{Q}$ with Galois group G.*