1 Groups 3
  1.1 Definitions and basic properties .............................................. 3
  1.2 Examples of groups .............................................................. 4
  1.3 Homomorphisms ................................................................. 6
  1.4 Cyclic groups ................................................................. 6
  1.5 Subgroups ................................................................. 7
  1.6 Normal subgroups ............................................................ 9
  1.7 Isomorphism theorems ....................................................... 10
  1.8 Group actions .............................................................. 12
  1.9 Sylow theorems ............................................................ 15
  1.10 Direct products ............................................................. 16
  1.11 Nilpotent and solvable groups ........................................... 18
  1.12 Symmetric and alternating groups ...................................... 20
  1.13 Semidirect products ....................................................... 22
  1.14 Groups of small order .................................................... 22
  1.15 Exact sequences .......................................................... 24
  1.16 Free groups ............................................................... 25

2 Categories and Functors 29
  2.1 Definitions and basic properties ......................................... 29
  2.2 Products and coproducts ................................................... 30
  2.3 Functors ................................................................. 33
  2.4 Natural transformations .................................................. 35
  2.5 Limits ................................................................. 37

3 Rings 39
  3.1 Definitions and basic properties ......................................... 39
  3.2 Ideals ................................................................. 41
  3.3 Euclidean rings .......................................................... 43
  3.4 Factorization in domains .................................................. 44
  3.5 Factorization in polynomial rings ..................................... 46
  3.6 Factorization in quadratic fields ..................................... 48
  3.7 The spectrum of a commutative ring .................................. 50
4 Modules

4.1 Definitions and basic examples ........................................ 53
4.2 Exact sequences of modules ............................................ 54
4.3 Free, projective, and injective modules ................................ 57
4.4 Modules over a PID ....................................................... 60
4.5 Abelian groups ............................................................ 65
4.6 Modules over $F[x]$ ...................................................... 65

5 Fields

5.1 Field extensions ............................................................ 71
5.2 Splitting fields ............................................................ 74
5.3 Finite fields ............................................................... 76
5.4 Normal extensions ........................................................ 78
5.5 Separable extensions ...................................................... 80
5.6 Galois extensions .......................................................... 84
5.7 Cyclotomic extensions ..................................................... 88
5.8 Algebraically closed fields .............................................. 89
5.9 Galois groups of polynomials .......................................... 91
5.10 Radical extensions ....................................................... 91
1 GROUPS

1.1 DEFINITIONS AND BASIC PROPERTIES

Definition 1.1.1 (Group). A group is a set $G$ together with a binary operation $\cdot$ such that

(i) $(ab)c = a(bc)$ for all $a, b, c \in G$;

(ii) there exists an identity element $1 \in G$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in G$;

(iii) for all $a \in G$, there exists an inverse $a^{-1} \in G$ of $a$ such that $aa^{-1} = a^{-1}a = 1$.

Initially, it is not obvious that inverses are well-defined, as if the identity is not unique, then we are required to make an arbitrary choice in (iii). Furthermore, it may be that inverses are not unique, in which case the notation $a^{-1}$ would not be well-defined. We resolve these concerns now.

Proposition 1.1.2 (Uniqueness of identity / inverse). Let $G$ be a group.

1. There is exactly one identity element in $G$.

2. If $a \in G$, then $a$ has exactly one inverse in $G$.

Proof. 1. If $1$ and $1'$ are identities, then $1' = 1 \cdot 1' = 1$.

2. Let $b$ and $b'$ be inverses of $a$. Then $b = 1 \cdot b = (b'a)b = b'(ab) = b' \cdot 1 = b'$.

Definition 1.1.3 (Abelian group). If $G$ is a group and $ab = ba$ for all $a, b \in G$, then $G$ is said to be abelian (or commutative). The following notation, depending on context, may be used for an abelian group:

1. the binary operation is $+$ instead of $\cdot$;
2. the identity element is $0$ instead of $1$;
3. the inverse of $a \in G$ is $-a$ instead of $a^{-1}$.

Proposition 1.1.4 (Cancellation). 1. If $ab = ac$, then $b = c$.

2. If $ac = bc$, then $a = b$.

Notation. For $n \geq 0$, write $a^n$ for the $n$-fold product of $a$ with itself.

Proposition 1.1.5. 1. If $ab = 1$ or $ba = 1$, then $b = a^{-1}$.

2. $(a^{-1})^{-1} = a$.

3. $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

4. $(a^{-1})^n = (a^n)^{-1}$ for $n \geq 0$. (Write $a^{-n}$ for either of these expressions.)

Proposition 1.1.6 (Homework A2 Problem 1). For $n, m \in \mathbb{Z}$, $a^n a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.
1.2 Examples of groups

**Definition 1.1.7** (Order of a group element). Let \( a \in G \). The order of \( a \), denoted \( \text{ord } a \), is the minimum \( n > 0 \) such that \( a^n = 1 \). If such an \( n \) does not exist, then \( \text{ord } a = \infty \).

**Definition 1.1.8** (Order of a group). The order of a group \( G \) is the cardinality \( |G| \) of \( G \) as a set. We say that \( G \) is finite if \( |G| \) is finite.

**Proposition 1.1.9.**

1. If \( G \) is finite and \( a \in G \), then \( \text{ord } a \) is finite.

2. If \( \text{ord } a = n \) is finite and \( a^m = 1 \) for some \( m \in \mathbb{Z} \), then \( n \mid m \).

### 1.2 EXAMPLES OF GROUPS

**Example 1.2.1** (Trivial group). Any singleton set \( G = \{g\} \) can be made into an abelian group of order 1 with the operation \( gg = g \). A generic trivial group may be written as \( 1 = \{1\} \).

If we are only working with abelian groups, then we may write \( 0 = \{0\} \) for a generic trivial group.

**Example 1.2.2** (Numbers with addition).

1. \( (\mathbb{N}, +) \) is not a group, as 1 \( \in \mathbb{N} \) has no inverse.

2. \( (\mathbb{R}, +) \) is an abelian group for \( R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \).

**Example 1.2.3** (Addition modulo \( n \)). Let \( n \) be a positive integer. For \( a \in \mathbb{Z} \), the congruence class of \( a \) modulo \( n \) is

\[
[a]_n = \{ a + nk \mid k \in \mathbb{Z} \} \subset \mathbb{Z}.
\]

The relation \( \sim \) on \( \mathbb{Z} \) given by \( a \sim b \iff [a]_n = [b]_n \) is an equivalence relation whose equivalence classes are precisely the congruence classes modulo \( n \), so these congruence classes partition \( \mathbb{Z} \). The set of congruence classes modulo \( n \) is denoted \( \mathbb{Z}/n\mathbb{Z} \), for reasons that will be seen later.

The natural way to give \( \mathbb{Z}/n\mathbb{Z} \) an additive group structure is to say that \( [a]_n + [b]_n = [a + b]_n \), but it needs to be shown that this is well-defined. Suppose that \( [a]_n = [a']_n \) and \( [b]_n = [b']_n \), so there exist \( k, l \in \mathbb{Z} \) with \( a' = a + nk \) and \( b' = b + nl \). Then

\[
[a' + b']_n = [(a + b) + n(k + l)]_n = \{(a + b) + n(k + l) + nm \mid m \in \mathbb{Z}\}
\]

\[=
\{(a + b) + nm' \mid m' \in \mathbb{Z}\} = [a + b]_n,
\]

so the addition is, in fact, well-defined. The group \( (\mathbb{Z}/n\mathbb{Z}, +) \) is an abelian group of order \( n \). For convenience, we may denote this additive group as \( \mathbb{Z}/n \).

**Example 1.2.4** (Fields). If \( K \) is a field, then the set \( K^\times = K \setminus \{0\} \) with multiplication is an abelian group with identity 1. Familiar examples include \( \mathbb{Q}^\times, \mathbb{R}^\times, \) and \( \mathbb{C}^\times \).

With the language of groups, one could define a field to be a set \( K \) with distinct elements \( 0, 1 \in K \) and operations \(+, \cdot\) such that

(i) (addition) \( (K, +) \) is an abelian group with identity 0;

(ii) (multiplication) \( (K^\times, \cdot) \) is an abelian group with identity 1;

(iii) (distributive law) \( a(b + c) = ab + ac \) for all \( a, b, c \in K \).

The first two axioms describe the separate structures of addition and multiplication, while the third axiom describes how they interact.
Example 1.2.5 (Units modulo $n$). Define multiplication on the set $\mathbb{Z}/n\mathbb{Z}$ by

$$[a]_n \cdot [b]_n = [ab]_n.$$ 

By a similar argument to the one for addition, this is well-defined, but it does not define a group structure on $\mathbb{Z}/n\mathbb{Z}$ (unless $n = 1$), as $[0]_n$ has no inverse. To fix this, we can restrict multiplication to the subset

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \gcd(a, n) = 1\}.$$ 

To see that this is well-defined, suppose $[a]_n = [a']_n$, so that $a' = a + mn$ for some $m \in \mathbb{Z}$, and $\gcd(a, n) = 1$. If $c \mid a'$ and $c \mid n$, then $c \mid a = a' - mn$, so $c \mid \gcd(a, n) = 1$. Thus $\gcd(a', n) = 1$.

We claim that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group. To prove this, we use Bézout’s lemma in elementary number theory, which tells us that $\gcd(a, n) = 1$ if and only if there exist $b, m \in \mathbb{Z}$ such that $ab + mn = 1$.

(0) If $[a]_n, [a']_n \in (\mathbb{Z}/n\mathbb{Z})^\times$, then there exist $b, m, b', m' \in \mathbb{Z}$ with $ab + mn = a'b' + m'n = 1$, so

$$1 = (ab + mn)(a'b' + m'n) = aa'(bb') + n(a'b'm + abm' + m'm').$$

Thus $\gcd(aa', n) = 1$, so $[a]_n[a']_n = [aa']_n \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(i) Associativity follows from associativity of ordinary integer multiplication.

(ii) The identity element is $[1]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(iii) If $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $ab + mn = 1$, then the inverse of $[a]_n$ is $[b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$.

The group $(\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, and its order is (essentially by definition) $\varphi(n)$, where $\varphi$ is the Euler totient function.

Example 1.2.6. Given a set $G$ with a small number of elements, we can define a group structure on $G$ by writing down a full multiplication table which satisfies the group axioms. This is shown for the Klein four-group $V_4$ (also denoted $V$ or $K_4$) below.

<table>
<thead>
<tr>
<th>$V_4$</th>
<th>1</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>1</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>1</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>1</td>
</tr>
</tbody>
</table>

Example 1.2.7. Let $X$ be any set. A permutation of $X$ is a bijection from $X$ to itself. The symmetric group of $X$, denoted $S(X)$, is the group of permutations of $X$ with function composition as the group operation. If $X$ is finite with $|X| = n$ and the exact nature of the elements of $X$ is not important, then we may assume $X = \{1, \ldots, n\}$. In this case, we write $S_n$ for $S(X)$. This is a group of order $n!$, and for $n \geq 3$, $S_n$ is not abelian.

Example 1.2.8. Let $R$ be a ring (with $1 \neq 0$). The set $GL_n(R)$ of invertible $n \times n$ matrices with entries in $R$ is the general linear group of $R$ of $n \times n$ matrices with matrix multiplication as the group operation. This is not commutative for $n \geq 2$, even if $R$ is, as

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$
1.3 HOMOMORPHISMS

**Definition 1.3.1** (Group homomorphism / isomorphism). Let $G$ and $H$ be groups. A (group) homomorphism from $G$ to $H$ is a function $f : G \to H$ such that $f(ab) = f(a)f(b)$ for all $a, b \in G$. If $f : G \to H$ is a bijective homomorphism, then we say that $f$ is an isomorphism. Groups $G$ and $H$ are isomorphic, written $G \cong H$, if there exists an isomorphism $f : G \to H$.

**Proposition 1.3.2.** Let $f : G \to H$ be a homomorphism. Then

1. $f(1) = 1$;
2. $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$;
3. if $f$ is an isomorphism, then so is $f^{-1} : H \to G$.

**Proof.**

1. We have $1 \cdot f(1) = f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$, so $f(1) = 1$.

2. Since $f$ is a homomorphism, $f(a)f(a^{-1}) = f(aa^{-1}) = f(1) = 1$.

3. The inverse of a bijective function is bijective, hence it is enough to show that $f^{-1} : H \to G$ is a homomorphism. Since $f$ is a homomorphism,

$$f(f^{-1}(ab)) = ab = f(f^{-1}(a))f(f^{-1}(b)) = f(f^{-1}(a)f^{-1}(b)).$$

As $f$ is bijective, it is injective, so $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$.

**Proposition 1.3.3.** If $f : G \to H$ and $g : H \to K$ are homomorphisms, then so is $g \circ f : G \to K$. If $f$ and $g$ are isomorphisms, then so is $g \circ f$.

**Example 1.3.4.**

1. Let $G = \{g\}$ and $H = \{h\}$ be trivial groups. The unique map $f : G \to H$ with $f(g) = h$ is an isomorphism, so there is only one trivial group up to isomorphism.

2. Two groups with the same multiplication tables, up to relabeling of elements, are isomorphic.

3. As additive groups, $\mathbb{C} \cong \mathbb{R}^2$ with $a + bi \leftrightarrow (a, b)$.

4. The map $x \mapsto e^x$ is a homomorphism $\mathbb{R} \to \mathbb{R}^\times$.

**Lemma 1.3.5** (†). Let $f : G \to H$ be an isomorphism and $a \in G$. Then $\text{ord } f(a) = \text{ord } a$.

1.4 CYCLIC GROUPS

**Definition 1.4.1** (Generator / cyclic group). Let $G$ be a group and $a \in G$. We say that $a$ is a generator of $G$ if every element of $G$ is of the form $a^n$ for some $n \in \mathbb{Z}$. If $G$ has a generator, we say that $G$ is cyclic.

**Example 1.4.2.**

1. The additive group $\mathbb{Z}$ is an infinite cyclic group with generators $\pm 1$.

2. The additive group $\mathbb{Z}/n\mathbb{Z}$ is a finite cyclic group. Its generators are $[a]_n$ for $\gcd(a, n) = 1$. There are $\varphi(n)$ such generators.
3. The multiplicative group \((\mathbb{Z}/5\mathbb{Z})^\times\) is cyclic. The elements \([2]_5\) and \([3]_5\) are generators, while \([1]_5\) and \([4]_5\) are not.

**Theorem 1.4.3** (Classification of cyclic groups). *Every cyclic group is isomorphic to \(\mathbb{Z}\) or \(\mathbb{Z}/n\mathbb{Z}\) for some \(n > 0\).*

*Proof.* Deferred (see Example 1.7.5).

1.5 SUBGROUPS

**Definition 1.5.1** (Subgroup). Let \(G\) be a group and \(H \subseteq G\) be a subset. We say that \(H\) is a *subgroup* of \(G\) if it is a group with the operation inherited from \(G\).

**Notation.** We write \(H \leq G\) to mean that \(H\) is a subgroup of \(G\), and \(H < G\) to mean that \(H\) is a subgroup of \(G\) and \(H \neq G\).

**Proposition 1.5.2.** Let \(G\) be a group and \(H \subseteq G\). Then \(H \leq G\) if and only if

(i) \(1 \in H\);

(ii) if \(a, b \in H\), then \(ab \in H\);

(iii) if \(a \in H\), then \(a^{-1} \in H\).

**Corollary 1.5.3** (†). Let \(G\) be a group and \(H \subseteq G\). Then \(H \leq G\) if and only if

(i) \(H\) is nonempty;

(ii) if \(a, b \in H\), then \(ab^{-1} \in H\).

**Example 1.5.4.**

1. Every group \(G\) has \(1 \leq G\) and \(G \leq G\).

2. Every subgroup of \(\mathbb{Z}\) is of the form \(n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}\) for \(n \geq 0\).

3. As additive groups, \(\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}\).

4. As multiplicative groups, \(\mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times\).

5. If \(\{H_i\}\) is a family of subgroups of \(G\), then \(\bigcap_i H_i\) is a subgroup of \(G\).

6. Let \(G\) be a group and \(a \in G\). The *cyclic subgroup generated by* \(a\) is \(\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}\). It is the smallest subgroup of \(G\) containing \(a\).

7. Let \(G\) be a group and \(S \subseteq G\) be any subset. The *subgroup generated by* \(S\) is the smallest subgroup \((S)\) of \(G\) containing \(S\). It is equivalently the subgroup of all finite products \(s_1 \cdots s_n\) with \(s_i \in S\) or \(s_i^{-1} \in S\) for each \(i\).

**Definition 1.5.5** (Kernel / image). Let \(f : G \to H\) be a homomorphism.

1. The *kernel of* \(f\) is 

\[
\ker f = f^{-1}(1) = \{a \in G \mid f(a) = 1\} \subseteq G.
\]
2. The image of $f$ is

$$\text{im } f = f(G) = \{ f(a) \mid a \in G \} \subset H.$$ 

**Proposition 1.5.6.** $\ker f \leq G$ and $\text{im } f \leq H$.

*Proof.* For $\ker f \subset G$, since $f(1) = 1$, we have $1 \in \ker f$. If $a, b \in \ker f$, then

$$f(ab^{-1}) = f(a)f(b)^{-1} = 1 \cdot 1^{-1} = 1,$$

so $ab^{-1} \in \ker f$. Thus $\ker f \leq G$.

For $\text{im } f \subset H$, it is clear that $\text{im } f$ is non-empty. If $x, y \in \text{im } f$ with $f(a) = x$ and $f(b) = y$ for some $a, b \in G$, then

$$xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in \text{im } f,$$

so $\text{im } f \leq H$. 

**Theorem 1.5.7.** Let $f : G \to H$ be a homomorphism. Then $f$ is injective if and only if $\ker f = 1$.

*Proof.* ($\implies$) Omitted.

($\impliedby$) Suppose $\ker f = 1$ and $f(a) = f(b)$ for $a, b \in G$. Then $f(ab^{-1}) = 1$, so $ab^{-1} = 1$.

**Theorem 1.5.8.** Let $f : G \to H$ be an injective homomorphism. Then $G \cong \text{im } f \leq H$.

*Proof.* The homomorphism $f : G \to \text{im } f$ is injective and surjective.

**Definition 1.5.9** (Embedding). If $f : G \to H$ is injective, we say that $f$ is an embedding of $G$ into $H$, written $f : G \hookrightarrow H$. That $G$ embeds into $H$ means that $G$ is isomorphic to a subgroup of $H$.

**Example 1.5.10** (Cayley’s theorem). Let $G$ be a group. For $a \in G$, define the left multiplication function $f_a : G \to G$ by $f_a(g) = ag$. This is not a homomorphism (unless $a = 1$), but it does satisfy

$$f_a \circ f_b = f_{ab} \quad \text{and} \quad f_1 = \text{id}_G.$$ 

In particular, $f_a \circ f_{a^{-1}} = f_1 = \text{id}_G$, so each $f_a$ is a bijection with $(f_a)^{-1} = f_{a^{-1}}$. Thus $f_a \in S(G)$, and the map $G \hookrightarrow S(G)$ given by $a \mapsto f_a$ is an injective homomorphism. 

*Cayley’s theorem* states that every group $G$ embeds into some symmetric group. Our work here shows that in particular, $G$ embeds into its own symmetric group $S(G)$.

**Definition 1.5.11** (Cosets). If $H \leq G$ is a subgroup and $a \in G$, then $aH = \{ ah \mid h \in H \}$ is a left coset of $H$ in $G$, while $Ha = \{ ha \mid h \in H \}$ is a right coset (of $H$ in $G$).

Given $H \leq G$, say that $a \sim b$ if $b = ah$ for some $h \in H$, or equivalently, if $a^{-1}b \in H$. This is an equivalence relation, and the equivalence class of $a$ is $[a] = aH$. Thus $G$ is partitioned into left cosets of $H$. (These results can be developed similarly for right cosets.)

**Notation.** The set of left cosets of $H$ in $G$ is denoted $G/H$.

**Definition 1.5.12** (Index). The index of $H$ in $G$ is $[G : H] = |G/H|$ (cardinality as a set).
Theorem 1.5.13 (Lagrange). Let \( G \) be a group and \( H \leq G \). Then \(|G| = [G : H] \cdot |H|\).

Proof. Each coset \( X \in G/H \) has cardinality \(|H|\) and \( G = \bigsqcup_{X \in G/H} X \). □

Corollary 1.5.14. Let \( G \) be a finite group.

1. If \( H \leq G \), then \(|H| \) divides \(|G|\).
2. If \( a \in G \), then \( \text{ord } a \) divides \(|G|\).

Proof. 1. Omitted.
2. Apply the first statement to \( H = \langle a \rangle \). □

1.6 NORMAL SUBGROUPS

Definition 1.6.1 (Normal subgroup). A subgroup \( H \leq G \) is normal if \( aH = Ha \) for every \( a \in G \).

In this case we write \( H \trianglelefteq G \).

Example 1.6.2. 1. In any group \( G \), the subgroups 1 and \( G \) are normal.
2. In an abelian group \( G \), every subgroup of \( G \) is normal.

Proposition 1.6.3. \( H \leq G \) is normal if and only if \( ghg^{-1} \in H \) for all \( g \in G \) and \( h \in H \).

Proof. ( \( \Rightarrow \) ) Let \( g \in G \) and \( h \in H \). Since \( gH = Hg \), we have \( gHg^{-1} = H \).

( \( \Leftarrow \) ) If \( ghg^{-1} \in H \) for all \( g \in G \) and \( h \in H \), then \( gHg^{-1} \subset H \), so \( gH \subset Hg \). By the same reasoning applied to \( g^{-1} \) and \( h \), we have \( Hg \subset gH \), so \( gH = Hg \). □

Definition 1.6.4 (Conjugate). Given \( g, h \in G \), the conjugate of \( h \) by \( g \) is \( ghg^{-1} \).

Proposition 1.6.5. If \( N \trianglelefteq G \) and \( H \leq G \) with \( N \subset H \), then \( N \trianglelefteq H \).

Proposition 1.6.6. Let \( f : G \to H \) be a homomorphism. Then \( \ker f \trianglelefteq G \).

Proof. Let \( k \in \ker f \) and \( g \in G \). Then
\[
f(gkg^{-1}) = f(g)f(k)f(g)^{-1} = f(g) \cdot 1 \cdot f(g)^{-1} = 1,
\]
so \( gkg^{-1} \in \ker f \). □

Example 1.6.7. Let \( F \) be a field and fix \( n \geq 1 \). Then \( \text{det} : GL_n(F) \to F^\times \) is a homomorphism, so its kernel is a normal subgroup of \( GL_n(F) \). The kernel of \( \text{det} \) is the special linear group
\[
SL_n(F) = \{ A \in GL_n(F) \mid \text{det } A = 1 \}.
\]

Proposition 1.6.8. If \( H \trianglelefteq G \), then \( G/H \) is a group with operation \( (aH)(bH) = abH \).
Proof. This follows from the calculation

\[(aH)(bH) = aHbH = abHH = abH.\]

Definition 1.6.9 (Quotient group). If \(H \leq G\), then the group \(G/H\) is the quotient group or factor group of \(G\) by \(H\). The map \(\pi : G \to G/H\) defined by \(\pi(a) = aH\) is the canonical homomorphism or quotient homomorphism.

Note that \(\ker \pi = H\) and \(\text{im} \pi = G/H\). Thus every normal subgroup of \(G\) is the kernel of some homomorphism from \(G\) to another group.

Example 1.6.10. 1. For any group \(G\), we have \(G/G \cong 1\) and \(G/1 \cong G\).

2. The subgroup \(n\mathbb{Z} \leq \mathbb{Z}\) is normal since \(\mathbb{Z}\) is abelian, and \(\mathbb{Z}/n\mathbb{Z}\) is the additive group of integers modulo \(n\), in accordance with our earlier use of the notation \(\mathbb{Z}/n\mathbb{Z}\).

3. The elements of \(\mathbb{C}/\mathbb{R}\) are lines \(l_y = \{x + iy \mid y \in \mathbb{R}\}\). This is isomorphic to \(\mathbb{R}\) via \(l_y \mapsto y\).

Theorem 1.6.11 (Correspondence theorem). Let \(H \leq G\). There is a natural bijection

\[
\{\text{subgroups of } G \text{ containing } H\} \longleftrightarrow \{\text{subgroups of } G/H\}
\]

\[
K \mapsto \pi(K)
\]

\[
\pi^{-1}(L) \longleftarrow L.
\]

Furthermore, normal subgroups of \(G\) containing \(H\) are paired with normal subgroups of \(G/H\).

Proof. See Homework 2 Problem 4.

1.7 ISOMORPHISM THEOREMS

Definition 1.7.1 (Factoring through). Let \(f : G \to H\) be a homomorphism and \(N \leq G\) with the canonical homomorphism \(\pi : G \to G/N\). Then \(f\) factors through \(G/N\) if there is a homomorphism \(\overline{f} : G/N \to H\) such that \(f = \overline{f} \circ \pi\).

\[
\begin{array}{ccc}
G & \xrightarrow{f} & H \\
\pi \downarrow & & \downarrow \overline{f} \\
G/N & & 
\end{array}
\]

Theorem 1.7.2. Let \(f : G \to H\) be a homomorphism and \(N \leq G\). Then \(f\) factors through \(G/N\) if and only if \(N \subseteq \ker f\).

Proof. \((\Longrightarrow )\) Suppose \(f\) factors through \(G/N\) as \(f = \overline{f} \circ \pi\). Then

\[f(N) = \overline{f}(NN) = \overline{f}(N) = 1,\]

so \(N \subseteq \ker f\).
(\iffalse) Suppose \( N \subset \ker f \). For \( f \) to factor as \( f \circ \pi \), we must have
\[
\overline{f}(aN) = (\overline{f} \circ \pi)(a) = f(a),
\]
so we take this to define \( \overline{f} \) and show that \( \overline{f} \) is well-defined. If \( aN = bN \), then \( a^{-1}b \in N \subset \ker f \), so \( f(a^{-1}b) = 1 \), hence
\[
\overline{f}(aN) = f(a) = f(b) = \overline{f}(bN).
\]
The proof that \( \overline{f} \) is a homomorphism is omitted.

**Theorem 1.7.3** (First isomorphism theorem). Let \( f : G \to H \) be a group homomorphism. Then \( G/\ker f \cong \text{im } f \), with isomorphism \( \overline{f} \) given by factoring \( f \) through \( G/\ker f \).

**Proof.** Let \( \pi : G \to G/\ker f \) be the canonical homomorphism, so \( f = \overline{f} \circ \pi \). Then \( \text{im } f = \text{im } \overline{f} \), so \( \overline{f} : G/\ker f \to \text{im } f \) is surjective. To see that it is injective, suppose \( a \ker f \in \ker f \). Then
\[
\overline{f}(a \ker f) = (\overline{f} \circ \pi)(a) = f(a) = 1,
\]
so \( a \in \ker f \) and \( a \ker f = \ker f \) is the identity in \( G/\ker f \).

**Corollary 1.7.4.** If \( f : G \to H \) is a surjective homomorphism, then \( G/\ker f \cong H \).

**Example 1.7.5.** We prove Theorem 1.4.3 on the classification of cyclic groups.

Let \( G \) be a cyclic group generated by \( a \), and define the homomorphism \( f : \mathbb{Z} \to G \) by \( n \mapsto a^n \). This is surjective since \( G \) is cyclic, so \( \mathbb{Z}/\ker f \cong G \). Since \( \ker f \leq \mathbb{Z} \), it is of the form \( n\mathbb{Z} \) for some \( n \geq 0 \).

If \( n = 0 \), then \( G \cong \mathbb{Z} \). Otherwise, \( G \cong \mathbb{Z}/n\mathbb{Z} \).

**Theorem 1.7.6** (Second isomorphism theorem). Let \( K \leq G \) and \( N \trianglelefteq G \). Then

1. \( KN \leq G \);
2. \( N \trianglerighteq KN \);
3. \( K \cap N \trianglerighteq K \);
4. \( KN/N \cong K/(K \cap N) \).

**Proof.**
1. Here \( KN \) is non-empty, and
\[
(KN)(KN)^{-1} = KNNK = KNK = KK = KN.
\]
2. Omitted.
3. Omitted.
4. Define \( f : KN \to K/K \) by \( kn \mapsto k(K \cap N) \). This is well-defined, since if \( k'n' = kn \), then \( k^{-1}k' = nn'^{-1} \in K \cap N \), so \( k(K \cap N) = k'(K \cap N) \). Then \( f \) is a surjective homomorphism with kernel \( N \), so \( KN/N \cong K/K \cap N \) by the first isomorphism theorem.
Theorem 1.7.7 (Third isomorphism theorem). Let $K, H \trianglelefteq G$ with $K \subset H$. Then

1. $H/K \trianglelefteq G/K$;
2. $(G/K)/(H/K) \cong G/H$.

Proof. 1. Given $gK \in G/K$ and $hK \in H/K$, 
\[ gK(hK)(gK)^{-1} = gK(hK)Kg^{-1} = ghg^{-1}K \in H/K. \]

2. Define $f : G/K \to G/H$ by $gK \mapsto gH$. This is a well-defined surjective homomorphism with kernel $H/K$, hence $(G/K)/(H/K) \cong G/H$ by the first isomorphism theorem.

\[ \square \]

1.8 GROUP ACTIONS

Definition 1.8.1 (Left group action). Let $G$ be a group and $X$ be a set. A left action of $G$ on $X$ is a map
\[ \theta : G \times X \longrightarrow X \]
\[ (g, x) \mapsto gx \]

such that

(i) $1x = x$ for all $x \in X$;
(ii) $g(hx) = (gh)x$ for all $g, h \in G$ and $x \in X$.

A right action can be defined similarly. When we say “action”, we usually mean “left action”.

Example 1.8.2. Let $X$ be a set. Then $S(X)$ acts on $X$ by $(f, x) \mapsto f(x)$ for $f \in S(X)$ and $x \in X$.

Definition 1.8.3 (Pullback of a group action). Let $f : G \to H$ be a homomorphism and suppose $\theta$ is an action of $H$ on $X$. The pullback of $\theta$ by $f$ is the action of $G$ on $X$ given by $gx = f(g)x$.

Theorem 1.8.4. There is a bijection
\[ \{ \text{actions of } G \text{ on } X \} \longleftrightarrow \{ \text{homomorphisms } G \to S(X) \} \]
\[ \theta \mapsto (g \mapsto \theta(g, -)) \]
\[ ((g, x) \mapsto [f(g)](x)) \longleftrightarrow f. \]

This tells us that every group action is the pullback of the action in Example 1.8.2 for some set $X$. Thus this action may be called the universal action.
**Definition 1.8.5** (Kernel / faithful action, †). Let \( \theta \) be an action of \( G \) on \( X \). The *kernel* of \( \theta \) is the kernel of the induced homomorphism \( G \to S(X) \). We say that \( \theta \) is *faithful* if \( \ker \theta = 1 \).

**Definition 1.8.6** (Orbit / stabilizer). Let \( G \) act on \( X \) and let \( x \in X \).

1. The *orbit* of \( x \), written \( \text{orb} \, x \) or \( GX \), is

\[
\text{orb} \, x = \{gx \mid g \in G\} \subset X.
\]

2. The *stabilizer* of \( x \), written \( \text{stab} \, x \) or \( G_x \), is

\[
\text{stab} \, x = \{g \in G \mid gx = x\} \leq G.
\]

**Proposition 1.8.7.** \( \ker \theta = \bigcap_x \text{stab} \, x \).

Define a relation on \( X \) by \( x \sim y \) if \( \text{orb} \, x = \text{orb} \, y \). Then \( \sim \) is an equivalence relation whose equivalence classes are the orbits of \( \theta \). In particular, the orbits partition \( X \).

**Definition 1.8.8** (Transitive action). An action of \( G \) on \( X \) is *transitive* if the only orbit is \( X \).

**Example 1.8.9** (Trivial action). The *trivial action* of \( G \) on \( X \) is given by \( gx = x \) for all \( g \in G \) and \( x \in X \). This is not faithful (unless \( G = 1 \)) and not transitive (unless \( |X| = 1 \)). We have \( \text{orb} \, x = \{x\} \) and \( \text{stab} \, x = G \).

**Example 1.8.10** (Left regular action). The *left regular action* of \( G \) on \( X = G \) is the action given by \( (g, x) \mapsto gx \). This is faithful and transitive, as \( \text{stab} \, x = 1 \) and \( \text{orb} \, x = G \) for all \( x \in G \). The induced homomorphism \( G \to S(G) \) is the embedding from Example 1.5.10.

**Example 1.8.11** (Left coset action). If \( H \leq G \), then the *left coset action* of \( G \) on \( X = G/H \) is the transitive action given by \( (g, xH) \mapsto gxH \). Given \( gH \in G/H \), we have \( \text{orb}(gH) = G/H \) and \( \text{stab}(gH) = gHg^{-1} \). The kernel of the left coset action is the *normal core* of \( H \) in \( G \), which is the largest normal subgroup of \( G \) contained in \( H \).

**Definition 1.8.12** (Automorphism). An *automorphism* of \( G \) is an isomorphism \( G \to G \). The group of automorphisms of \( G \) is denoted \( \text{Aut} \, G \).

**Example 1.8.13.**

1. \( \text{Aut} \, \mathbb{Z} = \{(n \mapsto n), (n \mapsto -n)\} \).

2. \( \text{Aut} \, (\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \).

**Example 1.8.14.** Any automorphism of \( G \) is also a permutation of \( G \), so \( \text{Aut}(G) \leq S(G) \). Then \( \text{Aut} \, G \) acts on \( G \) as the pullback of the universal action by the inclusion \( \text{Aut}(G) \hookrightarrow S(G) \).

**Example 1.8.15** (Conjugation action on group elements). Let \( G \) act on \( X = G \) by conjugation, i.e. \( (g, x) \mapsto gxg^{-1} \). The orbit of \( x \in G \) is the *conjugacy class* of \( x \) in \( G \), while the stabilizer of \( x \) is the *centralizer* of \( x \) in \( G \). For each \( g \in G \), the map \( x \mapsto gxg^{-1} \) is an automorphism of \( G \).

**Definition 1.8.16** (Center). The *center* of \( G \), denoted \( Z \) or \( Z(G) \), is the kernel of the conjugation action on the elements of \( G \). Equivalently, \( Z = \{g \in G \mid gh = hg \text{ for all } h \in G\} \). In particular, \( Z = G \) if and only if \( G \) is abelian.
Definition 1.8.17 (Inner automorphism). An *inner automorphism* of $G$ is an automorphism of the form $x \mapsto g x g^{-1}$ for some $g \in G$. The group of inner automorphisms is denoted $\text{Inn } G$, and is a subgroup of $\text{Aut } G$.

**Proposition 1.8.18.** $\text{Inn } G \cong G/Z$.

*Proof.* Apply the first isomorphism theorem to the homomorphism induced by the conjugation action on the elements of $G$. 

**Example 1.8.19** (Conjugation action on subgroups). Let $G$ act on the set $X$ of all subgroups of $G$ by conjugation, i.e. $(g, H) \mapsto g H g^{-1}$. The stabilizer of $H$ is the *normalizer* of $H$ in $G$, denoted $N_G(H)$. It is the largest subgroup of $G$ in which $H$ is normal.

**Lemma 1.8.20.** Let $G$ be a finite group and $H \leq G$ such that $|G : H|$ is the smallest prime divisor of $|G|$. Then $H \trianglelefteq G$.

*Proof.* Let $p$ be the smallest prime divisor of $|G|$. Let $G$ act on $G/H$ by left translation and $f : G \to S(X) \cong S_p$ be the induced homomorphism. Let $N = \ker f \leq G$. Then $N \trianglelefteq H$ and $|G/N|$ divides $p!$ by the first isomorphism theorem, so in particular $|G/N|$ has no prime factor greater than $p$. On the other hand, $|G/N|$ divides $|G|$, and $|G|$ has no prime factor less than $p$. Thus $|G/N| = p$, i.e. $|G : N| = p$. Since $G$ is finite, this means that $H = N \subseteq G$.

**Theorem 1.8.21** (Orbit-stabilizer). Let $G$ be a group acting on a set $X$ and let $x \in X$. Then $|\text{orb } x| = |G : \text{stab } x|$. In particular, if $G$ is finite, then $|\text{orb } x| = |G|/|\text{stab } x|$.

*Proof.* Let $y \in \text{orb } x$. Then there exists $g_y$ such that $g_y x = y$. Define a function $\text{orb } x \to G/\text{stab } x$ by $y \mapsto g_y \text{stab } x$. This is well-defined, as if $g$ satisfies $g x = y$, then $g^{-1} g_y x = x$, so $g^{-1} g_y \in \text{stab } x$ and $g_y \text{stab } x = g \text{stab } x$. The inverse of this function is $g \text{stab } x \mapsto g x$. Thus we have a bijection between $\text{orb } x$ and $G/\text{stab } x$.

**Example 1.8.22.** If the group $G$ is finite and $H \leq G$, then the number of subgroups conjugate to $H$ is $|G|/|N_G(H)|$.

**Definition 1.8.23** (Fixed point). Given an action of $G$ on $X$ and $S \subset G$, a *fixed point* of $g$ is an element $x \in X$ with $g x = x$ for all $g \in S$. The set of fixed points of $S$ is denoted $X^S$. When $S = \{g\}$, we write $X^g$ for $X^S$.

**Proposition 1.8.24.** If $H = \langle S \rangle \leq G$, then $X^S = X^H$.

**Lemma 1.8.25** (Burnside, †). Let $G$ be a finite group acting on a finite set $X$. Then the number of orbits of the action is

$$
\frac{1}{|G|} \sum_{g \in G} |X^g|.
$$

*Proof.* The number of orbits can be counted as a weighted sum over all $x \in X$ by $1/|\text{orb } x|$, so we get by orbit-stabilizer

$$
\sum_{x \in X} \frac{1}{|\text{orb } x|} = \sum_{x \in X} \frac{1}{|G|} \frac{\text{stab } x}{|\text{orb } x|} = \frac{1}{|G|} \sum_{x \in X} |\text{stab } x| = \frac{1}{|G|} \sum_{x \in X} \sum_{g \in G} |\{ (g, x) \in G \times X \mid g x = x \}| = \frac{1}{|G|} \sum_{g \in G} |\{ x \in X \mid g x = x \}| = \frac{1}{|G|} \sum_{g \in G} |X^g|.
$$
1.9 SYLOW THEOREMS

Throughout, let $G$ be a finite group and $p$ be a prime.

**Definition 1.9.1** ($p$-group). 1. $G$ is a $p$-group if $|G| = p^n$ for some $n \geq 0$.

2. If $H \leq G$, then $H$ is a $p$-subgroup of $G$ if $H$ is a $p$-group. (Here $G$ need not be a $p$-group.)

**Lemma 1.9.2.** Let a $p$-group $H$ act on a finite set $X$. Then $|X^H| \equiv |X| \pmod{p}$.

**Proof.** If $X^H = \{x_1, \ldots, x_k\}$, then $\text{orb}(x_i) = \{x_i\}$ for each $i$. All other orbits have size divisible by $p$ by orbit-stabilizer, hence the result.

**Theorem 1.9.3** (Cauchy). If $p$ divides $|G|$, then $G$ has an element of order $p$.

**Proof.** Let $X = \{(x_1, \ldots, x_p) \in G^p \mid x_1 \cdots x_p = 1\}$. Then $|X| = |G|^{p-1}$, which is divisible by $p$. Consider the action of $H = \langle \sigma \rangle$ on $X$ with $\sigma(x_1, \ldots, x_p) = (x_p, x_1, \ldots, x_{p-1})$. Since $|H| = p$, it is a $p$-group, so by Lemma 1.9.2, $|X^H| \equiv |X| \equiv 0 \pmod{p}$. Any fixed point (element of $X^H$) is of the form $(x, \ldots, x)$ with $x^p = 1$. Note that $(1, \ldots, 1) \in X^H$, so $|X^H| \geq 1$ and is divisible by $p \geq 2$. Thus there exists $(x, \ldots, x) \in X^H$ with $x \neq 1$, so $x$ is an element of order $p$.

**Theorem 1.9.4.** Let $G$ be a non-trivial $p$-group. Then $Z \neq 1$.

**Proof.** Let $G$ act on $X = G$ by conjugation, so $X^G = Z$. By Lemma 1.9.2, $|Z| \equiv |G| \equiv 0 \pmod{p}$, so $Z$ is non-trivial.

**Lemma 1.9.5.** Let $H$ be a $p$-subgroup of a finite group $G$. Then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

**Proof.** Let $H$ act on $X = G/H$ by left multiplication. If $gH \in X^H$, i.e. $h(gH) = gH$ for all $h \in H$, then $g \in N_G(H)$. Hence $|X^H| = [N_G(H) : H]$. The result follows by Lemma 1.9.2.

**Definition 1.9.6** (Sylow $p$-subgroup). Write $|G| = p^n m$ with $n \geq 0$ and $p \nmid m$. A Sylow $p$-subgroup $H \leq G$ is a subgroup of $G$ with $|H| = p^n$.

**Theorem 1.9.7** (First Sylow theorem). Let $p$ be a prime and $G$ be a finite group with $p$ dividing $|G|$. If $H \leq G$ is a $p$-subgroup, then

1. if $H$ is not a Sylow $p$-subgroup, then $H$ lies in a subgroup $N$ of order $p \cdot |H|$ with $H \leq N$;

2. $H$ is contained in a Sylow $p$-subgroup of $G$.

**Proof.** 1. Let $|H| = p^i$ for some $i < n$. Then $[N_G(H) : H] \equiv [G : H] = p^{n-i}m \equiv 0 \pmod{p}$ by Lemma 1.9.5, so $N_G(H)/H$ has order divisible by $p$. By Cauchy’s theorem, it has an element of order $p$, hence a subgroup $F$ of order $p$. By the correspondence theorem, if $\pi : N_G(H) \to N_G(H)/H$ is the canonical homomorphism, then $N = \pi^{-1}(F)$ is a subgroup of $N_G(H)$ containing $H$ and $[N : H] = p$. Since $H \leq N_G(H)$, we also have $H \leq N$.

2. Apply the first statement repeatedly.
**Theorem 1.9.8** (Second Sylow theorem). Suppose $p \mid |G|$. 

1. If $H \leq G$ is a $p$-subgroup and $P \leq G$ is a Sylow $p$-subgroup, then $gHg^{-1} \leq P$ for some $g \in G$.

2. Any two Sylow $p$-subgroups of $G$ are conjugate.

**Proof.** 1. Let $H$ act on $X = G/P$ by left multiplication. Then $|X^H| \equiv |X| = m \not\equiv 0 \ (\text{mod } p)$, so $|X^H| \geq 1$. Let $gP \in X^H$. Then $hgP = gP$ for all $h \in H$, so $g^{-1}Hg \leq P$.

2. Immediate from the first statement. □

**Corollary 1.9.9.** Let $P \leq G$ be a Sylow $p$-subgroup. Then $P \leq G$ if and only if $P$ is the unique Sylow $p$-subgroup of $G$.

**Notation.** Given a finite group $G$ and prime $p$, write $\text{Syl}_p(G)$ for the set of all Sylow $p$-subgroups of $G$ and $n_p = |\text{Syl}_p(G)|$.

**Theorem 1.9.10** (Third Sylow theorem). Suppose $p \mid |G|$. Then $n_p \mid m$ and $n_p \equiv 1 \ (\text{mod } p)$.

**Proof.** By the second Sylow theorem, $G$ acts transitively on $X = \text{Syl}_p(G)$ by conjugation. Let $P \in X$ be some Sylow $p$-subgroup. Then $\text{orb} P = X$ and $\text{stab} P = N_G(P)$, so by orbit-stabilizer, $n_p = |X| = [G : N_G(P)]$. This divides $|G : P| = m$.

Now let $P$ act on $X$ by conjugation. Since $P$ is a $p$-group, $|X^P| \equiv |X| = n_p \ (\text{mod } p)$ by Lemma 1.9.2. If $Q \in X^P$, then $gQg^{-1} = Q$ for all $g \in P$. Thus $P, Q \leq N_G(Q)$ are Sylow $p$-subgroups. Since $Q \leq N_G(Q)$, this means that $Q = P$. Thus $X^P = \{P\}$ and $n_p \equiv 1 \ (\text{mod } p)$. □

### 1.10 Direct Products

**Definition 1.10.1** (Direct product). Let $G_1, \ldots, G_n$ be groups. Then $G = G_1 \times \cdots \times G_n$ forms a group with componentwise group operations, called the (external) direct product of $G_1, \ldots, G_n$.

**Proposition 1.10.2** (†). If $G_1 \cong G_2$ and $H_1 \cong H_2$, then $G_1 \times H_1 \cong G_2 \times H_2$.

**Example 1.10.3.** 1. $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ has order 4 and is non-cyclic, so it is isomorphic to $V_4$.

2. The direct product of abelian groups is abelian.

**Definition 1.10.4** (Internal direct product). Let $H_1, \ldots, H_n \leq G$. We say that $G$ is the internal direct product of $H_1, \ldots, H_n$ if the multiplication map

$$f : H_1 \times \cdots \times H_n \longrightarrow G$$

$$(h_1, \ldots, h_n) \longmapsto h_1 \cdot h_n$$

is a group isomorphism.

**Proposition 1.10.5.** If $G$ is the internal direct product of $H_1, \ldots, H_n$, then $G \cong H_1 \times \cdots \times H_n$.

**Theorem 1.10.6** (Direct product theorem). Let $G$ be a group and $H_1, \ldots, H_n \leq G$ be subgroups. Then $G$ is the internal direct product of $H_1, \ldots, H_n$ if and only if
1. \( H_i \leq G \);
2. \( G = H_1 \cdots H_n \);
3. if \( 1 = h_1 \cdots h_n \) for \( h_i \in H_i \), then \( h_i = 1 \) for all \( i \).

**Proof.** (\( \implies \)) Let \( f \) be the multiplication isomorphism above. The first condition follows from the fact that \( f^{-1}(H_i) \) is the copy of \( H_i \) embedded in \( H_1 \times \cdots \times H_n \) in the natural way, which is normal. The last two conditions are surjectivity and injectivity of \( f \), respectively.

(\( \impliedby \)) By the third condition, \( H_i \cap H_j = 1 \) for \( i \neq j \). Then if \( h_i \in H_i \) and \( h_j \in H_j \), we have \( h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_j = 1 \) by normality of \( H_i \) and \( H_j \) in \( G \), so \( H_i \) and \( H_j \) commute. This is enough to ensure that the multiplication map \( f \) above is a group homomorphism. That \( f \) is surjective and injective follows from the second and third conditions, respectively. \( \square \)

**Corollary 1.10.7.**
1. If \( n = 2 \), then condition 3 may be replaced by \( H_1 \cap H_2 = 1 \).
2. If \( G \) is finite, then one of conditions 2 or 3 may be replaced by \( |G| = |H_1| \cdots |H_n| \).

**Example 1.10.8** (Chinese remainder theorem). Let \( m \) and \( n \) be relatively prime positive integers, and consider \( \mathbb{Z}/mn\mathbb{Z} \). The subgroups \( m\mathbb{Z}/mn\mathbb{Z} \) and \( n\mathbb{Z}/mn\mathbb{Z} \) satisfy the conditions of the direct product theorem, so (Homework 1 Problem 9(b))

\[
\mathbb{Z}/mn\mathbb{Z} \cong (m\mathbb{Z}/mn\mathbb{Z}) \times (n\mathbb{Z}/mn\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).
\]

**Theorem 1.10.9.** Let \( G \) be a finite group with \( |G| = p_1^{k_1} \cdots p_n^{k_n} \), where the \( p_i \) are distinct primes. For each \( i \), let \( H_i \leq G \) be a Sylow \( p_i \)-subgroup. If \( H_i \leq G \) for all \( i \), then \( G \) is the internal direct product of \( H_1, \ldots, H_n \).

**Proof.** We apply the direct product theorem.

1. This is given.
2. We replace \( G = H_1 \cdots H_n \) with \( |G| = |H_1| \cdots |H_n| \), and this holds since \( |H_i| = p_i^{k_i} \) for each \( i \).
3. Suppose \( 1 = h_1 \cdots h_n = 1 \) with \( h_i \in H_i \) for each \( i \). Since each \( H_i \) is normal in \( G \), the product \( H_1 \cdots H_{n-1} H_n^{-1} \) is a subgroup of \( G \) of order not divisible by \( p_n \), so \( h_1 \cdots h_{n-1} h_n^{-1} \) has order not divisible by \( p_n \). On the other hand, \( h_n \in H_n \), so \( h_n \) has order 1 or order divisible by \( p_n \). Thus we must have \( h_n = 1 \). By the same reasoning, \( h_i = 1 \) for all \( i \), as required. \( \square \)

**Proposition 1.10.10.** Let \( G \) be a group of order \( pq \), where \( p < q \) are primes. If \( q \not\equiv 1 \pmod{p} \), then \( G \) is cyclic.

**Proof.** If \( H_p \) and \( H_q \) are Sylow subgroups, then \( |H_p| = p \) and \( |H_q| = q \). By Sylow’s third theorem, \( H_p \) and \( H_q \) are normal (here we use \( q \not\equiv 1 \pmod{p} \)). Thus

\[
G \cong H_p \times H_q \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}
\]

by the Chinese remainder theorem. \( \square \)
1.11 NILPOTENT AND SOLVABLE GROUPS

**Definition 1.11.1** (Commutator / commutator subgroup). Given $g, h \in G$, the commutator of $g$ and $h$ is $[g, h] = g h g^{-1} h^{-1}$.

If $H, K \leq G$, then the **commutator subgroup** $[H, K]$ of $G$ is the subgroup generated by commutators $[h, k]$ with $h \in H$ and $k \in K$.

**Proposition 1.11.2.**
1. $[g, h]^{-1} = [h, g]$;
2. $[g, [h, k]] = [[g, h], [g, k]]$;
3. $[x, y] = 1$ if and only if $xy = yx$.

**Corollary 1.11.3.** $[G, G] = 1$ if and only if $G$ is abelian.

**Proposition 1.11.4.**
1. If $H, K \unlhd G$, then $[H, K] \unlhd G$.
2. If $H \leq G$, then $[G, H] \unlhd G$.
3. If $H, K \leq G$ and $[H, K] \leq H$, then $K \leq N_G(H)$.

**Proof.** See Homework 3 Problem 7.

**Definition 1.11.5** (Central series / lower central series). A **central series** is a series of subgroups $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$ such that $G_i \unlhd G$ and $[G, G_i] \leq G_{i+1}$ for each $i$, or equivalently, $G_i / G_{i+1} \subset Z(G / G_{i+1})$ for each $i$. The **lower central series** is the series

$$G = G_0 \triangleright G_1 \triangleright \cdots$$

with $G_{i+1} = [G, G_i]$ for each $i$.

**Definition 1.11.6** (Nilpotent group). A group is **nilpotent** if it has a (terminating) central series. Equivalently, the lower central series terminates in the trivial group.

**Example 1.11.7.**
1. Abelian groups are nilpotent.
2. Products of finitely many nilpotent groups are nilpotent.

**Lemma 1.11.8.** If $G / Z$ is nilpotent, then $G$ is nilpotent.

**Proof.** See Homework 3 Problem 8.

**Corollary 1.11.9.** Every $p$-group is nilpotent.

**Lemma 1.11.10.** Let $G$ be a nilpotent group and $H < G$ be a proper subgroup. Then $H \neq N_G(H)$.

**Proof.** Take a central series $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$. There exists $j$ such that $G_j \subseteq H$ but $G_{j+1} \subseteq H$. Then $[H, G_j] \leq [G, G_j] \leq G_{j+1} \leq H$, so $G_j \leq N_G(H)$, which means $N_G(H) \neq H$. 

**Lemma 1.11.11.** Let $P$ be a Sylow $p$-subgroup of $G$ and $H = N_G(P)$. Then $N_G(H) = H$. 

Proof. Let \( g \in N_G(H) \). Then \( P \) and \( gPg^{-1} \) are Sylow \( p \)-subgroups of \( H \). Since \( P \) is normal in \( H \), we have \( gPg^{-1} = P \), so \( g \in H \). \( \square \)

**Theorem 1.11.12.** A finite group \( G \) is nilpotent if and only if \( G \) is a product of \( p \)-groups.

*Proof. (\( \iff \)) Products of nilpotent groups, in particular \( p \)-groups, are nilpotent.*

(\( \Rightarrow \)) By Theorem 1.10.9, it suffices to show that every Sylow \( p \)-subgroup \( P \leq G \) is normal. Let \( H = N_G(P) \). Then \( N_G(H) = H \) by Lemma 1.11.11, so by Lemma 1.11.10, \( H \) cannot be a proper subgroup of \( G \), i.e. \( H = G \). Thus \( P \trianglelefteq G \). \( \square 

**Proposition 1.11.13.** Let \( N \trianglelefteq G \). Then \( G/N \) is abelian if and only if \([G,G] \leq N\).

*Proof. (\( \iff \)) Let \( g, h \in G \). Then since \( G/N \) is abelian, \([gN, hN] = [g, h]N = N\), so \([g, h] \in N\). Since \( N \) contains all commutators, it contains \([G,G]\).

(\( \Leftarrow \)) If \([G,G] \leq N\), then \( G/N \cong (G/[G,G])/[N/G,G]\), so it suffices to show that \( G/[G,G] \) is abelian. This is immediate from \([G,G]\) containing all commutators. \( \square \)

**Definition 1.11.14** (Derived subgroup / abelianization). The *derived subgroup* of \( G \) is \( G' = [G,G] \). The *abelianization* of \( G \) is \( G/G' \).

**Definition 1.11.15** (Derived series). The *derived series* of \( G \) is

\[ G = G^{(0)} \triangleright G^{(1)} \triangleright \cdots \]

with \( G^{(i+1)} = [G^{(i)}, G^{(i)}] \) for each \( i \).

**Definition 1.11.16** (Solvable group). We say that \( G \) is *solvable* if its derived series terminates in the trivial group. Equivalently, there is a sequence of subgroups

\[ G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1 \]

with \( G_i/G_{i+1} \) abelian for each \( i \).

**Example 1.11.17.** 1. Every nilpotent group, in particular every abelian group, is solvable.

2. A subgroup of a solvable group is solvable.

3. A quotient of a solvable group is solvable.

**Lemma 1.11.18.** If \( N \trianglelefteq G \) and \( G/N \) are solvable, then so is \( G \).

**Example 1.11.19.** Let \(|G| = pq\) for \( p < q \) primes. If \( H \) is the Sylow \( q \)-group, then \( G \) is solvable since \( H \) and \( G/H \) are cyclic, hence solvable.

For a group of this form, \( G \) is nilpotent if and only if \( G \) is abelian (in which case it is cyclic). Thus for example, \( S_3 \) is solvable but not nilpotent.
1.12 SYMMETRIC AND ALTERNATING GROUPS

Recall that $S_n$ is the symmetric group on the indices $\{1, 2, \ldots, n\}$.

**Definition 1.12.1** (Cycle / transposition). An element $\sigma \in S_n$ is a $k$-cycle if there exist $k$ distinct indices $a_1, \ldots, a_k$ with $\sigma(a_j) = a_{j+1}$ and every other element fixed by $\sigma$. (Here $a_{k+1} = a_1$.) A transposition is a 2-cycle.

**Notation.** A cycle is written $\sigma = (a_1, a_2, \ldots, a_k)$. This is the same as $(a_2, \ldots, a_k, a_1)$, etc.

**Example 1.12.2.** The elements of $S_3$ are $id$, $(1, 2)$, $(1, 3)$, $(2, 3)$, $(1, 2, 3)$, $(1, 3, 2)$.

**Proposition 1.12.3.** Every $\sigma \in S_n$ can be written as a product of disjoint cycles. Moreover, this is unique up to rearrangement and internal cycling of indices.

**Definition 1.12.4** (Cycle type). Let $\sigma \in S_n$ and write

$$\sigma = (a_{1,1}, \ldots, a_{1,k_1})(a_{2,1}, \ldots, a_{2,k_2}) \cdots (a_{r,1}, \ldots, a_{r,k_r}),$$

with $k_1 \geq k_2 \geq \cdots \geq k_r$ and $k_1 + \cdots + k_r = n$. The cycle type of $\sigma$ is the $r$-tuple $(k_1, \ldots, k_r)$.

**Notation.** It is convenient to drop 1’s from the cycle type if the degree $n$ of the symmetric group $S_n$ is understood. For example, $(12)(34)(5) \in S_5$ has cycle type $(2, 2, 1)$ or simply $(2, 2)$.

**Proposition 1.12.5.** Two permutations $\sigma, \tau \in S_n$ are conjugate if and only if they have the same cycle type.

**Proof.** See Homework 5 Problem 1.

**Definition 1.12.6** (Permutation representation). The (complex) permutation representation of $S_n$ is the homomorphism $\pi : S_n \to GL_n(\mathbb{C})$ given by

$$\pi(\sigma) = (\delta_{\sigma(i),j}).$$

**Definition 1.12.7** (Sign homomorphism / alternating group). The sign homomorphism of $S_n$ is $\sgn = \det \circ \pi : S_n \to \{\pm 1\}$. The alternating group is $A_n = \ker \sgn \leq S_n$.

**Proposition 1.12.8.** Every element in $S_n$ is a product of transpositions.

**Example 1.12.9.** The $k$-cycle $(a_1, \ldots, a_k)$ is a product of $k - 1$ transpositions

$$(a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2).$$

**Proposition 1.12.10.** If $\sigma$ can be written as a product of $k$ transpositions, then $\sgn(\sigma) = (-1)^k$.

**Lemma 1.12.11.** $A_n$ is generated by 3-cycles.
Proof. It suffices to write any product of two transpositions in terms of 3-cycles, as elements of \( A_n \leq S_n \) can be written as products of transpositions, and being in \( A_n \) requires these products to have an even number of factors. For this, we have

\[
\begin{align*}
(a, b)(a, b) &= \text{id}, \\
(a, b)(b, c) &= (a, b, c), \\
(a, b)(c, d) &= (a, b, c)(b, c, d).
\end{align*}
\]

Lemma 1.12.12. If \( n \geq 5 \), then any two 3-cycles in \( A_n \) are conjugate.

Proof. Let \( \sigma, \tau \in A_n \) be 3-cycles. Then there exists \( \rho \in S_n \) with \( \tau = \rho \sigma \rho^{-1} \). If \( \rho \in A_n \), we are done. Otherwise, suppose \( \sigma = (a, b, c) \). Since \( n \geq 5 \), there are indices \( d, e \) disjoint from \( \sigma \). Then \( \rho' = \rho(d, e) \in A_n \), and

\[
\rho' \sigma \rho'^{-1} = \rho(d, e)(a, b, c)(d, e)^{-1} = \rho(a, b, c) \rho^{-1} = \tau.
\]

Definition 1.12.13 (Simple group). A group \( G \neq 1 \) is simple if its only normal subgroups are 1 and \( G \).

Example 1.12.14. If \( G \) is abelian or solvable, then \( G \) is simple if and only if \( G \cong C_p \).

Theorem 1.12.15. If \( n \geq 5 \), then \( A_n \) is simple.

Proof. Let \( N \trianglelefteq A_n \) be non-trivial. It suffices to show that \( N \) contains a 3-cycle. Pick some \( \sigma \in N \). If \( \sigma \) is not a 3-cycle, then since (single) transpositions are not in \( A_n \), \( \sigma \) moves at least four indices. Suppose \( \sigma \) contains a \( k \)-cycle for some \( k \geq 4 \), say \( \sigma = (12 \cdots k)\tau \) by relabeling (conjugation). Then

\[
\sigma(123)\sigma^{-1}(123)^{-1} = (234)(132) = (142) \in N.
\]

Suppose \( \sigma = (123)(456)\tau \) for some \( \tau \) which is a product of 3-cycles and transpositions. Then

\[
\sigma(124)\sigma^{-1}(124)^{-1} = (235)(142) = (14352) \in N,
\]

so we are done by the previous case.

Suppose \( \sigma = (123)\tau \) for some \( \tau \) which is a product of transpositions. Then \( \sigma \sigma = (123) \in N \).

Finally, suppose \( \sigma = (12)(34)\tau \) for some \( \tau \) which is a product of transpositions. Then

\[
\pi = \sigma(123)\sigma^{-1}(123)^{-1} = (214)(132) = (13)(24) \in N
\]

and \( \pi(135)\pi^{-1}(135)^{-1} = (315)(153) = (135) \in N \).

Corollary 1.12.16. \( S_n \) is not solvable for \( n \geq 5 \).

Remark 1.12.17. The group \( A_3 \cong C_3 \) is also simple, while groups \( A_1 \) and \( A_2 \) are trivial.

By order, \( A_5 \) is the smallest non-abelian simple group.

Proposition 1.12.18. \( S_n \) is solvable for \( n \leq 4 \).
1.13 SEMIDIRECT PRODUCTS

**Definition 1.13.1** (Semidirect product). Let $N$ and $K$ be groups and $f : K \to \text{Aut} N$ be a homomorphism. The *(external) semidirect product* $N \rtimes_f K$ is the group on $N \times K$ with operation

$$(h_1, k_1)(h_2, k_2) = (h_1 f(k_1)(h_2), k_1 k_2).$$

**Example 1.13.2.**
1. If $f$ is the trivial homomorphism, then $N \rtimes_f K = N \times K$.
2. Let $N = C_n$ and $K = C_2$. There is a non-trivial homomorphism $f : C_2 \to C_n$ which sends the non-identity element of $C_2$ to the map $g \mapsto g^{-1}$. This gives us the group $C_n \rtimes_f C_2$ with

$$(r_1, s_1)(r_2, s_2) = (r_1 r_2^{-1}, s_1 s_2).$$

This is the dihedral group of degree $n$, denoted $D_n$. It has order $2n$.
3. If $p < q$ are primes and $q \equiv 1 \pmod{p}$, then there is a non-trivial $f : C_p \to \text{Aut} C_q$. Then $C_q \rtimes_f C_p$ is a non-abelian group of order $pq$.

**Proposition 1.13.3.** $N \triangleleft N \rtimes_f K$.

**Definition 1.13.4** (Internal semidirect product). Let $N \triangleleft G$ and $K \leq G$. If $N \cap K = 1$ and $G = NK$, then we say that $G$ is the *internal semidirect product* of $N$ and $K$.

**Remark 1.13.5.** If $G$ is finite, then the last condition is equivalent to $|G| = |N||K|$.

**Proposition 1.13.6.** If $G$ is the internal semidirect product of $N$ and $K$, then $G \cong N \rtimes_f K$ for some homomorphism $f : K \to \text{Aut} N$.

**Proposition 1.13.7 (†).** If $H$ is a group, then $\text{Aut} H \leq \text{Inn} G$ for some group $G$ containing $H$.

**Proof.** We can take $G = H \rtimes \text{Aut}_H$ with $f : \text{Aut} H \to \text{Aut} H$ the identity. \qed

1.14 GROUPS OF SMALL ORDER

In this section we classify groups of order $n = |G| \leq 15$ up to isomorphism. Throughout, write $C_n = \mathbb{Z}/n\mathbb{Z}$ and assume $p < q$ are primes.

**Proposition 1.14.1.** The only group of order 1 is 1.

**Proposition 1.14.2.** If $n = p$, then $G \cong C_p$.

**Proof.** See Homework 2 Problem 5b. \qed

**Proposition 1.14.3.** If $n = p^2$ for $p$ prime, then $G \cong C_{p^2}$ or $G \cong C_p \times C_p$.

**Proof.** If $G$ contains an element of order $p^2$, then $G \cong C_{p^2}$. Otherwise, every non-identity element of $G$ has order $p$. Let $h \in G$ be such an element and consider the subgroup $H = \langle h \rangle$ of order $p$. We can then pick $k \in G \setminus H$ and take $K = \langle k \rangle$, also of order $p$. Then $H$ and $K$ satisfy the conditions of the direct product theorem, so $G \cong H \times K \cong C_p \times C_p$. \qed
Proposition 1.14.4. If \( n = pq \) and \( q \not\equiv 1 \pmod{p} \), then \( G \cong C_{pq} \).

Proof. This is Proposition 1.10.10. \( \square \)

Proposition 1.14.5. If \( q \equiv 1 \pmod{p} \) instead, then \( G \cong C_{pq} \) or \( G \cong C_q \rtimes_f C_p \) for \( f \) non-trivial.

Proof. The Sylow \( q \)-subgroup \( Q \cong C_q \) is normal in \( G \), while the number of Sylow \( p \)-subgroups is either 1 or \( q \). If \( n_p = 1 \), then \( G \cong C_q \times C_p \cong C_{pq} \) by Proposition 1.10.10.

If \( n_p = q \), then fix some Sylow \( p \)-subgroup \( P \). The subgroups \( Q \) and \( P \) meet the conditions for \( G \) to be an internal semidirect product, i.e. \( G = Q \rtimes f P \) for some non-trivial \( f : P \rightarrow Aut Q \). \( \square \)

Corollary 1.14.6. If \( p \) is an odd prime and \( |G| = 2p \), then \( G \cong C_{2p} \) or \( G \cong D_p \).

Proof. By Proposition 1.14.5, either \( G \cong C_{2p} \) or \( G \cong C_p \rtimes f C_2 \) for some non-trivial \( f : C_2 \rightarrow Aut C_p \). The only such \( f \) is the one which sends the generator of \( C_2 \) to the inversion automorphism of \( C_p \), which gives the dihedral group \( D_p \). \( \square \)

Using these results, we can classify groups of order up to \( n = 15 \) except for \( n = 8 \) and \( n = 12 \).

1. \( 1 \)
2. \( C_2 \)
3. \( C_3 \)
4. \( C_4, C_2 \times C_2 \)
5. \( C_5 \)
6. \( C_6, D_3 \cong S_3 \)
7. \( C_7 \)
8. \( C_8, C_2 \times C_4, C_2 \times C_2 \times C_2 \times C_2, D_4, \) and \( D_8 \)
9. \( C_9, C_3 \times C_3 \)
10. \( C_{10}, D_5 \)
11. \( C_{11} \)
12. \( C_{13} \)
13. \( C_{14}, D_7 \)
14. \( C_{15} \)

Proposition 1.14.7. The groups of order 8 are \( C_8, C_4 \times C_2, C_2 \times C_2 \times C_2 \), \( D_4 \), and \( Q_8 \).

\[ Q_8 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}. \]

Proof. If \( G \) has an element of order 8, then \( G \cong C_8 \).

If \( G \) has no elements of order 4 or 8, so every non-identity element has order 2, then repeated use of the direct product theorem shows that \( G \cong C_2 \times C_2 \times C_2 \).

If \( h \in G \) has order 4 and no element of \( G \) has order 8, then let \( H = \langle h \rangle \leq G \) and pick \( k \in G \setminus H \).

If \( k \) has order 2, then \( K = \langle k \rangle \) intersects \( H \) trivially and \( |G| = |H||K| \), so \( G = H \rtimes_f K \) for some \( f : K \rightarrow Aut H \). There are two possibilities for \( f \), which correspond to \( C_4 \times C_2 \) if \( f \) is trivial and \( D_4 \) if \( f \) sends \( k \) to the inversion automorphism.

If no \( k \in G \setminus H \) has order 2, so then every \( k \in G \setminus H \) has order 4, we have \( k^2 = h^2 \) for all \( k \in G \setminus H \) since \( (kH)(kH) = H \) in \( G/H \) and \( k^2 \) has order 2. From this we can deduce that \( h^2 \in Z \) and \( hk = kh^3 \), which is enough to deduce the multiplication table of \( G \). One can check that \( Q_8 \) has the same multiplication table. \( \square \)
Proposition 1.14.8. The groups of order 12 are $C_{12}$, $C_6 \times C_2$, $D_6$, $A_4$, and $C_3 \rtimes_f C_4$ for
\[
C_3 = \{1, a, a^2\}; \quad C_4 = \{1, b, b^2, b^3\}; \quad f(b)(a) = a^{-1}.
\]

Proof. Let $P \leq G$ be a Sylow 3-subgroup.
If $P$ is not normal, then there are 4 Sylow 3-subgroups, each of which contains 2 elements of order 3. Then there are only four elements of $G$ not of order 3, so the unique Sylow 2-subgroup $Q$ of 4 elements must contain all of them, and thus $Q$ is normal. Hence $G \cong Q \rtimes_f P$ for some $f : P \rightarrow \text{Aut} Q$.
If $Q \cong C_4$, then we seek homomorphisms $f : C_3 \rightarrow \text{Aut} C_4$. There are two elements of $\text{Aut} C_4$, and only the identity satisfies $\sigma^3 = 1$, so the only possible choice of $f$ is the trivial map. This gives $G \cong C_4 \times C_3 \cong C_{12}$.
If $Q \cong C_2 \times C_2$, then $\text{Aut} Q \cong S_3$, which has three elements $\sigma$ satisfying $\sigma^3 = 1$. Thus we have three possible choices of $f : P \rightarrow \text{Aut} Q$. If $f$ is trivial, then $G \cong C_2 \times C_2 \times C_3 \cong C_6 \times C_2$.
Otherwise, if $P = \{1, a, a^2\}$ and $Q = \{1, b, c, bc\}$, then without loss of generality $f(a)(b) = c$ and $f(a)(c) = bc$ (otherwise, relabel elements). The multiplication table is then completely determined, and it matches that of $A_4$.
Now suppose $P$ is normal and let $Q$ be a Sylow 2-subgroup of order 4. In this case $G \cong P \rtimes g Q$ for some $g : Q \rightarrow \text{Aut} P$.
If $Q \cong C_4$, then $\text{Aut} P$ has two elements, both satisfying $\sigma^4 = 1$, so there are two choices for $g$. If $g$ is trivial, then we get $G \cong C_3 \times C_4 \cong C_{12}$ again. Otherwise, if $P = \{1, a, a^2\}$ and $Q = \{1, b, b^2, b^3\}$, then elements of $G$ have the form $a^i b^j$, and multiplication is determined by $ba = a^{-1} b$. This is the last group of the list.
If $Q \cong C_2 \times C_2$, then there are four homomorphisms $g : Q \rightarrow \text{Aut} P$, but three of them are the same up to an isomorphism of $Q$ (i.e. by relabeling generators). The trivial $g$ produces $G \cong C_6 \times C_2$, while the non-trivial choices of $g$ turn out to produce $D_6$.

Remark 1.14.9. There are 14 isomorphism classes of groups of order 16.

1.15 EXACT SEQUENCES

Definition 1.15.1 (Exact sequence). A sequence of group homomorphisms
\[
G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} G_n
\]
is exact if $\text{im } f_i = \ker f_{i+1}$ for all $i = 1, \ldots, n - 1$.

Proposition 1.15.2. 1. $f : G \rightarrow H$ is injective if and only if $1 \rightarrow G \xrightarrow{f} H$ is exact.
2. $f : G \rightarrow H$ is surjective if and only if $G \xrightarrow{f} H \rightarrow 1$ is exact.

Definition 1.15.3 (Short exact sequence). A short exact sequence is an exact sequence
\[
1 \rightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} F \rightarrow 1,
\]
i.e. $\alpha$ is injective, $\beta$ is surjective, and $\text{im } \alpha = \ker \beta$. Then $H$ identifies with $\text{im } \alpha \leq G$ and $F \cong G/H$. 24
Proposition 1.15.4. If $H \triangleleft G$, then the sequence
\[ 1 \to H \xrightarrow{i} G \xrightarrow{\pi} G/H \to 1 \]
is exact.

Definition 1.15.5 (Split exact sequence). A short exact sequence
\[ 1 \to H \xrightarrow{\alpha} G \xrightarrow{\beta} F \to 1 \]
is split (or right split) if there exists $\gamma : F \to G$ such that $\beta \circ \gamma = \text{id}_F$.

Theorem 1.15.6. The short exact sequence
\[ 1 \to H \xrightarrow{\alpha} G \xrightarrow{\beta, \gamma} F \to 1 \]
is split if and only if there is a subgroup $K \leq G$ such that $\beta|_K : K \to F$ is an isomorphism. In this case, $G \cong H \rtimes_{\varphi} F$ with $\varphi : F \to \text{Aut} H$ given by $\varphi(f)(h) = ghg^{-1}$, where $g = \gamma(f)$.

Proof. ($\implies$) Let $K = \text{im} \gamma$. If $f \in F$ and $k = \gamma(f) \in K$, then $\beta|_K(k) = \beta(\gamma(f)) = f$, so $\beta|_K : K \to F$ is surjective. If $k \in \ker \beta|_K$, then $k = \gamma(f)$ for some $f \in F$ since $K = \text{im} \gamma$, and then $f = \beta(\gamma(f)) = \beta(k) = 1$. This means $k = \gamma(1) = 1$, so $\ker \beta|_K$ must be trivial.

($\impliedby$) Suppose such a $K$ exists, so $\beta|_K : K \to F$ is an isomorphism. Take $\gamma = \beta|_K^{-1} \circ i$.

If these conditions are met, then regard $K \cong \gamma(K)$ as a subgroup of $G$. We have that $H = \ker \beta \leq G$, and $H \cap K = 1$ since $\beta(H) = 1$ and $\beta|_K : K \to F$ is an isomorphism. Finally, if $g \in G$ and $f = \beta(g) \in F$, then $k = \gamma(f) \in K$ and $h = gk^{-1} \in H$ satisfy $hk = g$, so $G = HK$. Hence $G$ is the internal semidirect product of $H$ and $K$, so $G \cong H \rtimes_{\varphi} F$ for some $\varphi : F \to \text{Aut} H$. To determine $\varphi$, let $g = \gamma(f) \in K$ and $h \in H$. Then $gh = \varphi(g)(h) \cdot g$, so $\varphi(g)(h) = ghg^{-1}$, as required.

Example 1.15.7. Let $G$ be a non-abelian group of order 8, and let $h \in G$ be an element of order 4. Then $H = \langle h \rangle \triangleleft G$, so we have a short exact sequence
\[ 1 \to H \xrightarrow{} G \xrightarrow{} G/H \to 1. \]

If there is an element of order 2 in $G \setminus H$, then the sequence splits and we obtain $G \cong D_4$ via the theorem. Otherwise, there is no splitting, and we obtain $Q_8$ as before.

1.16 FREE GROUPS

Definition 1.16.1 (Words). Let $X$ be a set, called the alphabet. The elements of $X$ are referred to as letters. Form an inverse alphabet $\overline{X}$ of formal symbols $\{ \overline{x} \mid x \in X \}$.

For $n \geq 0$, a word of length $n$ on $X$ is a sequence of $n$ letters (not necessarily distinct) from $X \cup \overline{X}$. 

25
Concatenation of words $w$ and $v$ to get a new word $wv$ defines an associative non-commutative binary operation on the set of words on a given alphabet. The empty word $\lambda$ is the identity for this operation, but no element (other than $\lambda$) has an inverse.

**Definition 1.16.2** (Truncation / irreducible word). Let $w$ be a word on $X$ of the form $ua\pi v$ or $u\pi av$, where $u, v$ are words on $X$ and $a \in X$ is a letter. The word $w' = uv$ is a truncation of $w$.

If $w$ is a word on $X$, then $w$ is irreducible if there is no word $u$ on $X$ which is a truncation of $w$.

For two words $u, v$ on $X$, write $u \sim w$ if there is a sequence of words

$$u = w_0, w_1, \ldots, w_n = v$$

such that for each $i$, one of the words $w_i, w_{i+1}$ is a truncation of the other. Then $\sim$ is an equivalence relation on the set of words on $X$.

**Proposition 1.16.3.** If $u_1 \sim v_1$ and $u_2 \sim v_2$, then $u_1u_2 \sim v_1v_2$.

**Theorem 1.16.4.** Each equivalence class of words on $X$ contains exactly one irreducible word.

**Proof.** For existence, let $w$ be a word of minimum length in a given equivalence class. Since truncation reduces the length of a word by 2, $w$ must be irreducible.

For uniqueness, let $u$ and $v$ be irreducible words in the same equivalence class, and write down a sequence $u = w_0, w_1, \ldots, w_n = v$ as above. To show that $u = v$, we induct on $n$ and then the total length of the words $w_0, \ldots, w_n$. When $n = 0$, we have $u = w_0 = v$. Now consider $n \geq 1$ and look at a longest word $w_k$ in the sequence. Then $w_{k-1}$ and $w_{k+1}$ are necessarily truncations of $w_k$.

If the truncations are

$$stb\bar{u} \leftrightarrow sa\pi tb\bar{u} \rightarrow sa\pi tu,$$

then we replace $w_k$ with $stu$ and have truncations $w_{k-1} \rightarrow w_k$ and $w_{k+1} \rightarrow w_k$ instead. This does not change the number of words $n$ in the sequence, but it does reduce the total length of all words in the sequence, so we can apply the inductive hypothesis.

If the truncations are

$$sat \leftrightarrow sa\pi at \rightarrow sat \quad \text{or} \quad st \leftrightarrow a\pi at \rightarrow st,$$

then we can reduce the number of words $n$ in the sequence by omitting $w_k$ and $w_{k+1}$.

We can obtain every other case by swapping the roles of letters and inverse letters.

**Definition 1.16.5** (Free group). Let $X$ be an alphabet. The free group on $X$, denoted $F(X)$ (or $\text{Free } X$), is the set of all equivalence classes of words on $X$ with the concatenation operation.

**Example 1.16.6.**

1. If $X = \emptyset$, then $F(X) = 1$.

2. If $X = \{a\}$, then $F(X) \cong \mathbb{Z}$ is the cyclic group generated by $[a]$.

3. If $|X| \geq 2$ with $a, b \in X$ distinct, then $ab$ and $ba$ are distinct irreducible words. Hence $[ab] \neq [ba]$, so $F(X)$ is non-abelian.

**Notation.** In $F(X)$, we write $a^{-1}$ for $\pi$ when $a \in X$.

For convenience, we will write $w$ for $[w]$ and work on words themselves whenever possible.
Theorem 1.16.7 (Universal property of free groups). Let $X$ be a set, $G$ be a group, and $f : X \to G$ be a set function. Then there is a unique group homomorphism $\overline{f} : F(X) \to G$ such that $\overline{f}(x) = f(x)$ for all $x \in X$.

Proof. Let $w \in F(X)$ and write $w = b_1 \cdots b_n$ where $b_i = x_i^{\varepsilon_i}$ for some $x_i \in X$ and $\varepsilon_i \in \{\pm 1\}$. Then

$$\overline{f}(w) = \overline{f}(b_1) \cdots \overline{f}(b_n) = f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n},$$

which shows that if $\overline{f}$ exists, then it is unique and must be given by this formula.

To show existence, we can define $\overline{f}$ using this formula, provided it is well-defined on $F(X)$. For this, note that $\overline{f}$ is unchanged by truncations, hence whenever two words are equivalent. \qed

Corollary 1.16.8. Let $X \subset G$ generate $G$. Then $G \cong F(X)/N$ for some $N \unlhd F(X)$.

Proof. The inclusion function $i : X \hookrightarrow G$ extends to a homomorphism $f : F(X) \to G$. That $X$ generates $G$ means that $f$ is surjective, so $F(X)/\ker f \cong G$. \qed

Notation. If $G$ is a group and $S \subset G$ is a subset, then

$$\langle \langle S \rangle \rangle = \left\langle \bigcup_{g \in G} gSg^{-1} \right\rangle$$

is the smallest normal subgroup of $G$ containing $S$.

Definition 1.16.9 (Presentation / finite presentation). Let $G$ be a group and $X \subset G$ generate $G$. Choose a subset $R \subset F(X)$ such that $G \cong F(X)/\langle\langle R \rangle\rangle$. Then we write

$$G \cong \langle X \mid R \rangle = F(X)/\langle\langle R \rangle\rangle.$$ 

This is a presentation for $G$. We say that the presentation is finite if $X$ and $R$ are finite.

Example 1.16.10. 1. $\langle \sigma \mid \sigma^n \rangle \cong \mathbb{Z}/n\mathbb{Z}$

2. $\langle \sigma, \tau \mid \sigma^n, \tau^2, \tau \sigma \tau \sigma \rangle \cong D_n$

Proposition 1.16.11 (†). Every group $G$ has a presentation.

Proof. An explicit presentation is $G \cong \langle G \mid \{g_1g_2g_3 \mid g_1, g_2, g_3 \in G \text{ with } g_1g_2g_3 = 1\}\rangle$. \qed

Definition 1.16.12 (Free product). Let $G$ and $H$ be groups. The free product of $G$ and $H$, denoted $G * H$, is the group $F(G \cup H)/\langle\langle R \rangle\rangle$, where

$$R = \{1_G, 1_H\} \cup \{g_1g_2g_3 \mid g_1, g_2, g_3 \in G \text{ with } g_1g_2g_3 = 1_G \text{ in } G\}$$

$$\cup \{h_1h_2h_3 \mid h_1, h_2, h_3 \in H \text{ with } h_1h_2h_3 = 1_H \text{ in } H\}.$$ 

Proposition 1.16.13. Let $G$ and $H$ be groups with presentations $\langle X \mid R \rangle$ and $\langle Y \mid S \rangle$. Then

$$G * H \cong \langle X \cup Y \mid R \cup S \rangle.$$ 

Proof. See Homework 7 Problem 2. \qed

27
Example 1.16.14.  
1. $G \ast 1 \cong G$ and $1 \ast H \cong H$.

2. If $G, H \neq 1$, then $G \ast H$ is infinite with trivial center (see Homework 6 Problem 7).

Theorem 1.16.15 (Universal property of free products). Let $i, j : G, H \to G \ast H$ be the natural maps and let $g, h : G, H \to K$ be homomorphisms to some group $K$. Then there is a unique homomorphism $k : G \ast H \to K$ such that the following diagram commutes.

\[ \begin{array}{ccc}
G & \xrightarrow{i} & G \ast H \\
\downarrow{g} & & \downarrow{k} \\
H & \xrightarrow{j} & K
\end{array} \]

This is closely related to the following result for direct products.

Theorem 1.16.16 (Universal property of direct products). Let $\pi_G, \pi_H : G \times H \to G, H$ be the projections and let $g, h : K \to G, H$ be homomorphisms from some group $K$. Then there is a unique homomorphism $k : K \to G \times H$ such that the following diagram commutes.

\[ \begin{array}{ccc}
G & \xleftarrow{\pi_G} & G \times H \\
\downarrow{g} & & \downarrow{k} \\
H & \xleftarrow{\pi_H} & K
\end{array} \]
2 CATEGORIES AND FUNCTORS

2.1 DEFINITIONS AND BASIC PROPERTIES

Definition 2.1.1 (Category). A category $C$ consists of a collection (more formally a class) $\text{Ob} C$ of objects, a collection $\text{Hom} C$ (or $\text{Mor} C$) of morphisms (arrows) between objects, and a composition operation, which forms from morphisms $X \xrightarrow{f} Y \xrightarrow{g} Z$ a morphism $g \circ f : X \to Z$, such that

(i) if $W \xrightarrow{f} X \xrightarrow{g} Y \xrightarrow{h} Z$ are morphisms, then $h \circ (g \circ f) = (h \circ g) \circ f$;

(ii) for any object $X \in \text{Ob} C$, there is a unique identity morphism $\text{id}_X : X \to X$ such that for any morphisms $f : X \to Y$ and $g : W \to X$, we have

$$f = f \circ \text{id}_X, \quad g = \text{id}_X \circ g.$$ 

The collection of morphisms $X \to Y$ is denoted $\text{Hom}_C(X,Y)$ (or $\text{Mor}_C(X,Y)$).

Notation. We write $X \in C$ to mean $X \in \text{Ob} C$.

Example 2.1.2. 1. In $\text{Set}$, the category of sets, the morphisms are functions.

2. In $\text{Grp}$, the category of groups, the morphisms are group homomorphisms.

3. Given a group $G$, we can form a category $C$ with $\text{Ob} C = \{\ast\}$ and $\text{Hom}(\ast, \ast) = G$.

4. Given a poset $X$, we can form a category $C$ with $\text{Ob} C = X$ and

$$\text{Hom}(x,x') = \begin{cases} \{(x,x')\} & x \geq x', \\ \emptyset & \text{otherwise}. \end{cases}$$

5. Given categories $C$ and $D$, the product category $C \times D$ has $\text{Ob}(C \times D) = \text{Ob} C \times \text{Ob} D$ and $\text{Hom}_{C \times D}((A,X);(B,Y)) = \text{Hom}_C(A,B) \times \text{Hom}_D(X,Y)$ in the natural way.

6. Given a category $C$, the dual category (opposite category), denoted $C^{\text{op}}$ (or $C^o$) is the category with $\text{Ob} C^{\text{op}} = \text{Ob} C$ and $\text{Hom}_C^{\text{op}}(X,Y) = \text{Hom}_C(Y,X)$. For disambiguation, we may write $X^{\text{op}}$ or $X^o$ to denote the copy of $X$ in $C^{\text{op}}$.

7. Given a category $C$, the arrow category $\text{Arr} C$ has $\text{Ob} C = \text{Hom} C$. A morphism between $f : X \to Y$ and $f' : X' \to Y'$ is given by morphisms $g : X \to X'$ and $h : Y \to Y'$ such that the following diagram commutes.

\[
\begin{array}{ccc}
X & \xrightarrow{f} & Y \\
\downarrow{g} & & \downarrow{h} \\
X' & \xrightarrow{f'} & Y'
\end{array}
\]

Definition 2.1.3 (Isomorphism). A morphism $f : X \to Y$ is an isomorphism if there exists a morphism $g : Y \to X$ such that $f \circ g = \text{id}_Y$ and $g \circ f = \text{id}_X$. 

29
Proposition 2.1.4. If \( f : X \to Y \) is an isomorphism with \( g : Y \to X \) as above, then \( g \) is unique and \( g \) is an isomorphism.

Notation. If \( f \) is an isomorphism, then write \( f^{-1} \) for the morphism \( g \) above.

Definition 2.1.5 (Subcategory / full subcategory). Let \( C \) be a category. A category \( C' \) is a subcategory of \( C \) if \( \text{Ob} C' \subset \text{Ob} C, \text{Hom}_{C'}(X,Y) \subset \text{Hom}_C(X,Y) \), and the composition law in \( C' \) is inherited from \( C \).

We say that \( C' \) is a full subcategory of \( C \) if \( \text{Hom}_{C'}(X,Y) = \text{Hom}_C(X,Y) \) for all \( X,Y \in C' \).

Example 2.1.6. 1. In \( \text{Grp} \), the subcategory \( \text{Ab} \) of abelian groups is a full subcategory.

2. For any subclass \( A \subset \text{Ob} C \), there is a unique full subcategory \( C' \) of \( C \) such that \( \text{Ob} C' = A \).

Definition 2.1.7 (Initial and terminal objects). Let \( X \in C \) be an object.

1. \( X \) is initial if for every \( Y \in C \), there is a unique morphism \( X \to Y \).

2. \( X \) is terminal (final) if for every \( W \in C \), there is a unique morphism \( W \to X \).

Proposition 2.1.8. If \( X \in C \) is an object, then \( X \) is initial (terminal) in \( C \) if and only if \( X \) is terminal (initial) in \( C^{\text{op}} \).

Example 2.1.9. 1. In \( \text{Set} \), the initial object is \( \emptyset \) and the terminal objects are singleton sets.

2. In \( \text{Grp} \), the trivial group is initial and terminal.

3. Let \( G \) be a group and form \( C \) on one object as before. Then \( C \) has no initial or terminal objects (unless \( G \) is trivial).

4. Let \( X \) be a poset and form \( C \) on \( X \) as before. The initial object of \( C \) is the maximum of \( X \) (if it exists), while the terminal object is the minimum of \( X \) (if it exists).

Theorem 2.1.10. If \( X \) and \( X' \) are initial (terminal), then there is a unique isomorphism \( X \to X' \), i.e. \( X \) and \( X' \) are canonically isomorphic.

Proof. Let \( X \) and \( X' \) be initial, and let \( f : X \to X' \) and \( g : X' \to X \) be the unique morphisms. Then \( g \circ f : X \to X \) is a morphism \( X \to X \), but since \( X \) is initial and \( \text{id}_X : X \to X \) is a morphism, \( g \circ f = \text{id}_X \). Similarly, \( f \circ g = \text{id}_{X'} \), so \( f \) and \( g \) are inverses and \( f \) is an isomorphism.

2.2 PRODUCTS AND COPRODUCTS

Universal properties are applications of Theorem 2.1.10. As an example, we consider products.

Definition 2.2.1 (Product of two objects). Let \( X,Y \in C \). An object \( X \times Y \) together with morphisms \( p,q : X \times Y \to X,Y \) is a product of \( X \) and \( Y \) if for any morphisms \( f : Z \to X \) and \( g : Z \to Y \), there is a unique morphism \( h : Z \to X \times Y \) such that the following diagram commutes.

\[
\begin{array}{ccc}
X & \xleftarrow{f} & Y \\
\downarrow{p} & & \downarrow{q} \\
X \times Y & \xleftarrow{h} & Z \\
\end{array}
\]
**Theorem 2.2.2.** Let $X \times Y$ and $\tilde{X} \times \tilde{Y}$ be two products of $X$ and $Y$, with projections $p, q$ and $\tilde{p}, \tilde{q}$, respectively. Then there is a unique isomorphism $h : X \times Y \to \tilde{X} \times \tilde{Y}$ such that the following diagram commutes.

\[
\begin{array}{ccc}
X \times Y & \xrightarrow{p} & X \\
\downarrow{q} & & \downarrow{\tilde{p}} \\
Y & \xleftarrow{\tilde{q}} & \tilde{X} \times \tilde{Y} \\
\end{array}
\]

**Proof.** Fix $X$ and $Y$, and consider a new category $\mathcal{D}$ whose objects are diagrams of the form

\[
\begin{array}{ccc}
Z & \to & X \\
\downarrow & & \downarrow \\
Y & & \\
\end{array}
\]

A morphism between diagrams for $Z$ and $Z'$ is given by a morphism $Z \to Z'$ in $\mathcal{C}$ such that the following diagram commutes.

\[
\begin{array}{ccc}
Z & \to & X \\
\downarrow & & \downarrow \\
Y & \hookrightarrow & Z' \\
\end{array}
\]

The diagram for $Z = X \times Y$ is a terminal object in $\mathcal{D}$, which is unique up to unique isomorphism. \(\square\)

**Proposition 2.2.3.** Let $p, q : X \times Y \to X, Y$ be the projections. The function

\[
\text{Hom}(Z, X \times Y) \to \text{Hom}(Z, X) \times \text{Hom}(Z, Y) \\
h \mapsto (p \circ h, q \circ h)
\]

is a bijection.

**Definition 2.2.4** (Arbitrary product). Let $\{X_i\}_{i \in I}$ be a family of objects. The product is the object $\prod_i X_i$ along with morphisms $p_j : \prod_i X_i \to X_j$ for which $\text{Hom}(Z, \prod_i X_i) \cong \prod_i \text{Hom}(Z, X_i)$ with bijection $h \mapsto \prod_i \{p_i \circ h\}$.

**Definition 2.2.5** (Product morphism). Let $f : X \to X'$ and $g : Y \to Y'$ be morphisms. The product morphism $f \times g : X \times Y \to X' \times Y'$ is given by the following commuting diagram.

\[
\begin{array}{ccc}
X \times Y & \xrightarrow{q} & Y \\
\downarrow{p} & & \downarrow{g} \\
X & \xrightarrow{f} & X' \\
\end{array}
\]

\[
\begin{array}{ccc}
X' & \xleftarrow{f'} & X' \times Y' \\
\end{array}
\]
2.2 Products and coproducts

Example 2.2.6. 1. In \textbf{Set}, the product is the ordinary Cartesian product.

2. In \textbf{Grp}, the product is the (external) direct product.

3. In \textbf{Ab}, the product is the (external) direct product. Within the context of abelian groups, it is also known as the \textit{direct sum}, written $G \oplus H$.

4. In the category $n \rightarrow n - 1 \rightarrow \cdots \rightarrow 2 \rightarrow 1$, we have $i \times j = \max(i, j)$.

Definition 2.2.7 (Coproduct). The \textit{coproduct} of $X, Y \in \mathcal{C}$ is $(X^{\text{op}} \times Y^{\text{op}})^{\text{op}}$, i.e. the product in $\mathcal{C}^{\text{op}}$. More explicitly, the coproduct is an object $X \ast Y$ together with morphisms $i, j : X, Y \rightarrow X \ast Y$ such that given morphisms $f : X \rightarrow Z$ and $g : Y \rightarrow Z$, there is a unique morphism $h : X \ast Y \rightarrow Z$ such that $h \circ i = f$ and $h \circ j = g$.

Proposition 2.2.8. The function

$$\text{Hom}(X \ast Y, Z) \rightarrow \text{Hom}(X, Z) \times \text{Hom}(Y, Z)$$

$h \mapsto (h \circ i, h \circ j)$

is a bijection.

Definition 2.2.9 (Arbitrary coproduct). Let $\{X_j\}_{j \in J}$ be a family of objects. The \textit{coproduct} is the object $\bigsqcup_j X_j$ along with morphisms $i_k : \bigsqcup_j X_j \rightarrow X_k$ for which $\text{Hom}(\bigsqcup_j X_j, Z) \cong \prod_j \text{Hom}(X_j, Z)$ with bijection $h \mapsto \prod_j \{h \circ i_j\}$.

Example 2.2.10. 1. In \textbf{Set}, the coproduct is the disjoint union $X \sqcup Y$.

2. In \textbf{Grp}, the coproduct is the free product $G \ast H$.

3. In \textbf{Ab}, the coproduct is the direct sum $G \oplus H$.

4. In $n \rightarrow n - 1 \rightarrow \cdots \rightarrow 2 \rightarrow 1$, we have $i \ast j = \min(i, j)$.

Definition 2.2.11 (Group object). Let $\mathcal{C}$ be a category. A \textit{group object} in $\mathcal{C}$ is a quadruple $(G, m, e, i)$ such that

(i) $G$ is an object;

(ii) $m : G \times G \rightarrow G$ is a morphism (corresponding to multiplication);

(iii) $e : F \rightarrow G$ is a morphism (corresponding to the identity element), where $F$ is terminal;

(iv) $i : G \rightarrow G$ is a morphism (corresponding to inverses);
(v) (associativity) the following diagram commutes:

\[ \begin{array}{c}
G \times G \times G \\
\downarrow m \times \text{id}_G \\
G \times G \\
\downarrow m
\end{array} \xrightarrow{\text{id}_G \times m} \begin{array}{c}
G \times G \\
\downarrow m
\end{array} \]

(vi) (identity) the following diagrams commute, where \( \pi_G \) is projection onto \( G \):

\[ \begin{array}{c}
G \times F \\
\downarrow m \circ \pi_G
\end{array} \xrightarrow{\text{id}_G \times e} \begin{array}{c}
G \times G \\
\downarrow m
\end{array} \]

\[ \begin{array}{c}
G \times F \\
\downarrow m \circ \pi_G
\end{array} \xrightarrow{e \times \text{id}_G} \begin{array}{c}
G \times G \\
\downarrow m
\end{array} \]

(vii) (inverse) the following diagrams commute.

\[ \begin{array}{c}
G \\
\downarrow e
\end{array} \xrightarrow{(\text{id}_G, i)} \begin{array}{c}
G \times G \\
\downarrow m
\end{array} \]

\[ \begin{array}{c}
G \\
\downarrow e
\end{array} \xrightarrow{(i, \text{id}_G)} \begin{array}{c}
G \times G \\
\downarrow m
\end{array} \]

Example 2.2.12. 1. The group objects in \( \textbf{Set} \) are the usual groups.

2. Group objects in \( \textbf{Top} \), the category of topological spaces, are topological groups.

3. Group objects in \( \textbf{Grp} \) are abelian groups.

2.3 FUNCTORS

Definition 2.3.1 (Functor). Let \( \mathcal{C} \) and \( \mathcal{D} \) be categories. A (covariant) functor \( F : \mathcal{C} \to \mathcal{D} \) is a collection of functions \( \text{Ob}\mathcal{C} \to \text{Ob}\mathcal{D} \) and \( \text{Hom}_\mathcal{C}(X,Y) \to \text{Hom}_\mathcal{D}(F(X),F(Y)) \) such that

(i) \( F(\text{id}_X) = \text{id}_{F(X)} \) for \( X \in \mathcal{C} \);

(ii) for morphisms \( X \xrightarrow{f} Y \xrightarrow{g} Z \) in \( \mathcal{C} \), we have \( F(g \circ f) = F(g) \circ F(f) \).

If instead \( F \) maps \( \text{Hom}_\mathcal{C}(X,Y) \) to \( \text{Hom}_\mathcal{D}(F(Y),F(X)) \) and \( F(g \circ f) = F(f) \circ F(g) \) for all \( f,g \), we say that \( F \) is a contravariant functor.

Remark 2.3.2. Contravariant functors are covariant functors \( \mathcal{C}^{\text{op}} \to \mathcal{D} \) or \( \mathcal{C} \to \mathcal{D}^{\text{op}} \), so it is only necessary to consider covariant functors.

Lemma 2.3.3. If \( f : X \to Y \) is an isomorphism in \( \mathcal{C} \), then \( F(f) : F(X) \to F(Y) \) is an isomorphism in \( \mathcal{D} \) and \( F(f)^{-1} = F(f^{-1}) \).

Corollary 2.3.4. If \( X \cong Y \) in \( \mathcal{C} \), then \( F(X) \cong F(Y) \) in \( \mathcal{D} \).
Example 2.3.5. 1. The identity functor \( \text{id} : \mathcal{C} \to \mathcal{C} \) is defined by \( \text{id}(X) = X \) and \( \text{id}(f) = f \).

2. Let \( Y \in \mathcal{D} \). The constant functor \( c_Y : \mathcal{C} \to \mathcal{D} \) is given by \( c_Y(X) = Y \) and \( c_Y(f) = \text{id}_Y \).

3. The forgetful functor \( \text{Forget} : \text{Grp} \to \text{Set} \) has \( \text{Forget}(G) = G \) and \( \text{Forget}(f) = f \).

4. If \( \mathcal{C}' \subset \mathcal{C} \) is a subcategory, there is an inclusion functor \( I : \mathcal{C}' \to \mathcal{C} \).

5. Let \( F : \text{Grp} \to \text{Ab} \) send a group \( G \) to its abelianization \( G/G' \). Given \( f : G \to H \), composing with the projection \( H \to H/H' \) gives a homomorphism \( \tilde{f} : G \to H/H' \). Then \( G/\ker \tilde{f} \) is abelian, so \( \tilde{f} \) descends to a homomorphism \( F(f) \). One can check that with this definition of \( F \) on morphisms, \( F \) is a functor.

Definition 2.3.6 (Small / locally small category). A small category is a category \( \mathcal{C} \) for which \( \text{Ob}\mathcal{C} \) and \( \text{Hom}\mathcal{C} \) are sets. A locally small category is one for which we can only say that \( \text{Hom}\mathcal{C}(X,Y) \) is a set for each pair of objects \( X,Y \in \mathcal{C} \).

Example 2.3.7. 1. Let \( \mathcal{I} \) be a small category. A functor \( \mathcal{I} \to \mathcal{C} \) is a commutative diagram in \( \mathcal{C} \) of shape \( \mathcal{I} \).

2. Let \( \mathcal{C} \) be a locally small category and fix \( X \in \mathcal{C} \). The hom-functor given by \( X \) is

\[
\begin{align*}
h^X(Y) & = \text{Hom}_\mathcal{C}(X,Y), \\
h^X(f)(g) & = f \circ g, \quad f : Y \to Z \text{ and } g \in \text{Hom}_\mathcal{C}(X,Y).
\end{align*}
\]

If we fix \( Y \) instead, then we obtain a contravariant functor \( h_Y \), i.e. a functor \( \mathcal{C}^{\text{op}} \to \text{Set} \).

Definition 2.3.8 (Category of small categories \( \dagger \)). In the category of small categories, denoted \( \text{Cat} \), the objects are small categories and the morphisms are functors.

Remark 2.3.9. For reasons related to Russell’s paradox, it is not possible to form the category of all categories.

Definition 2.3.10 (Faithful / full functor). Let \( F : \mathcal{C} \to \mathcal{D} \) be a functor. For each pair of objects \( X,Y \in \mathcal{C} \), there is a set map \( \varphi_{X,Y} : \text{Hom}_\mathcal{C}(X,Y) \to \text{Hom}_\mathcal{D}(F(X),F(Y)) \) given by \( \varphi_{X,Y}(f) = F(f) \).

1. \( F \) is faithful if \( \varphi_{X,Y} \) is injective for all \( X,Y \).

2. \( F \) is full if \( \varphi_{X,Y} \) is surjective for all \( X,Y \).

Example 2.3.11. If \( \mathcal{C}' \subset \mathcal{C} \) is a subcategory, the inclusion \( \mathcal{C}' \to \mathcal{C} \) is faithful. It is full if and only if \( \mathcal{C}' \) is a full subcategory.

Definition 2.3.12 (Equivalence of categories). A functor \( F : \mathcal{C} \to \mathcal{D} \) is an equivalence if

(i) \( F \) is full and faithful;

(ii) for any object \( Y \in \mathcal{D} \), there exists \( X \in \mathcal{C} \) such that \( F(X) \cong Y \).

Proposition 2.3.13. Let \( F : \mathcal{C} \to \mathcal{D} \) be a functor.

1. If \( X \cong Y \) in \( \mathcal{C} \), then \( F(X) \cong F(Y) \) in \( \mathcal{D} \).
2. If $F$ is full and faithful and $F(X) \cong F(Y)$ in $\mathcal{D}$, then $X \cong Y$ in $\mathcal{C}$.

3. If $F$ is an equivalence, then $F$ induces a bijection between isomorphism classes in $\mathcal{C}$ and $\mathcal{D}$.

**Example 2.3.14.** 1. Let $\mathcal{C}' \subset \mathcal{C}$ be a full subcategory. Then $\mathcal{C}' \hookrightarrow \mathcal{C}$ is an equivalence if and only if for every $Y \in \mathcal{C}$, there exists $X \in \mathcal{C}'$ such that $X \cong Y$.

2. Consider $\text{Vect}_K$, the category of vector spaces over $K$. The full subcategory of $K$-vector spaces of the form $K^n$, where $n$ is any cardinal number, is equivalent to $\text{Vect}_K$.

In particular, if we look at the full subcategory $\text{FdVect}_K$ of finite-dimensional vector spaces over $K$, it has as an equivalent full subcategory the vector spaces $K^n$ for $n \in \mathbb{N}$, which is a small category.

**Proposition 2.3.15.** If $F : \mathcal{C} \rightarrow \mathcal{D}$ is an equivalence, then there exists $G : \mathcal{D} \rightarrow \mathcal{C}$ such that $F \circ G : \mathcal{D} \rightarrow \mathcal{D}$ and $G \circ F : \mathcal{C} \rightarrow \mathcal{C}$ are equivalences.

### 2.4 NATURAL TRANSFORMATIONS

**Definition 2.4.1 (Natural transformation).** Let $F$ and $G$ be two functors $\mathcal{C} \rightarrow \mathcal{D}$. A natural transformation $\alpha : F \rightarrow G$ is a collection of morphisms $\alpha_X : F(X) \rightarrow G(X)$ in $\mathcal{D}$ such that for every morphism $f : X \rightarrow Y$ in $\mathcal{C}$, the following diagram commutes.

\[
\begin{array}{ccc}
F(X) & \xrightarrow{\alpha_X} & G(X) \\
\downarrow{F(f)} & & \downarrow{G(f)} \\
F(Y) & \xrightarrow{\alpha_Y} & G(Y)
\end{array}
\]

**Definition 2.4.2 (Category of functors).** Let $\mathcal{C}$ and $\mathcal{D}$ be two categories with $\mathcal{C}$ small. The category of functors from $\mathcal{C}$ to $\mathcal{D}$, denoted $\text{Fun}(\mathcal{C}, \mathcal{D})$, has objects the functors $\mathcal{C} \rightarrow \mathcal{D}$ and morphisms the natural transformations.

**Proposition 2.4.3.** If $F, G : \mathcal{C} \rightarrow \mathcal{D}$ and $\alpha : F \rightarrow G$ is a natural isomorphism, i.e. an isomorphism in $\text{Fun}(\mathcal{C}, \mathcal{D})$, then $\alpha_X : F(X) \rightarrow G(X)$ is an isomorphism in $\mathcal{D}$ for all $X \in \mathcal{C}$.

**Example 2.4.4.** 1. Let $F : \text{Grp} \rightarrow \text{Grp}$ be the abelianization functor (with target $\text{Grp}$). For each $G \in \text{Grp}$, set $\alpha_G = \pi : G \rightarrow G/G'$. Then $\alpha$ is a natural transformation $\text{id}_{\text{Grp}} \rightarrow F$.

2. Let $\mathcal{C}$ be a small category. Given $f : X \rightarrow X'$, we have a morphism $h^{X'}(Y) \rightarrow h^X(Y)$ for each $Y$ given by $g \mapsto g \circ f$, and one can check that this produces a natural transformation $h^f : h^{X'} \rightarrow h^X$. Hence there is a functor $\mathcal{C}^{\text{op}} \rightarrow \text{Fun}(\mathcal{C}, \text{Set})$ with $X^{\text{op}} \mapsto h^X$ and $f^{\text{op}} \mapsto h^f$.

Equivalently, we have a functor $\mathcal{C}^{\text{op}} \times \mathcal{C} \rightarrow \text{Set}$ with $(X^{\text{op}}, Y) \mapsto \text{Hom}_{\mathcal{C}}(X, Y)$, or a functor $\mathcal{C} \rightarrow \text{Fun}(\mathcal{C}^{\text{op}}, \text{Set})$ with $Y \mapsto h_Y$, where $h_Y(X^{\text{op}}) = \text{Hom}_{\mathcal{C}}(X, Y)$.

**Notation.** Let $\mathcal{C}, \mathcal{D}$ be categories and $F, G : \mathcal{C} \rightarrow \mathcal{D}$ be functors. Write $\text{Nat}(F, G)$ for the collection of natural transformations $F \Rightarrow G$. 

35
**Lemma 2.4.5** (Yoneda). Let \( C \) be a locally small category and fix \( X \in C \). Let \( F : C \to \text{Set} \) be a functor. Then there is a bijection \( \varphi : \text{Nat}(h^X, F) \to F(X) \) given by

\[
\varphi(\alpha) = \alpha_X(id_X).
\]

**Proof.** We construct an inverse map \( \psi : F(X) \to \text{Nat}(h^X, F) \). Let \( u \in F(X) \). To determine what \( \alpha = \psi(u) \) should be, let \( Y \in C \). Given \( f \in \text{Hom}_C(X, Y) \), there is a function \( F(f) : F(X) \to F(Y) \), so let

\[
\alpha_Y(f) = F(f)(u).
\]

This is a natural transformation \( h^X \to F \), as if \( g : Y \to Z \) is a morphism, we have

\[
(F(g) \circ \alpha_Y)(f) = F(g)(\alpha_Y(f)) = F(g)(F(f)(u)) = F(g \circ f)(u),
\]

\[
(\alpha_Z \circ h^X(g))(f) = \alpha_Z(h^X(g)(f)) = \alpha_Z(g \circ f) = F(g \circ f)(u).
\]

To see that \( \varphi \circ \psi = \text{id}_{F(X)} \), we have

\[
(\varphi \circ \psi)(u) = \varphi(\psi(u)) = \varphi(\alpha) = \alpha_X(id_X) = F(id_X)(u) = \text{id}_{F(X)}(u) = u.
\]

To see that \( \psi \circ \varphi = \text{id}_{\text{Nat}(h^X, F)} \), we must show that given \( \beta : R^X \to F \) with \( \varphi(\beta) = \beta_X(id_X) = u \), we have \( \alpha = \psi(u) = \beta \). For any \( Y \in C \) and \( f : X \to Y \), we compute

\[
\beta_Y(f) = \beta_Y(h^X(f)(id_X)) = F(f)(\beta_X(id_X)) = F(f)(u) = \alpha_Y(f).
\]

\[\square\]

**Corollary 2.4.6.** \( \text{Nat}(h^X, h^Y) \cong \text{Hom}_C(Y, X) \).

**Corollary 2.4.7.** Every natural transformation \( h^X \to h^Y \) is of the form \( h^f \) for a unique \( f : Y \to X \).

**Definition 2.4.8** (Presheaf of sets). A functor \( C^{\text{op}} \to \text{Set} \) is a presheaf of sets.

**Definition 2.4.9** (Representable functor). A functor \( F : C \to \text{Set} \) is represented by \( X \) if \( F \) is naturally isomorphic to \( h^X \).

**Proposition 2.4.10.** Let \( F \) be representable and suppose \( F \) is represented by \( X \) and \( Y \). Then there is a unique isomorphism \( f : X \to Y \) such that the following diagram commutes.

\[
h^Y \xleftarrow{\text{iso}} \quad F \xrightarrow{\text{iso}} h^X
\]

**Example 2.4.11.** 1. \( c_{\{+\}} : C \to \text{Set} \) is represented by any initial object of \( C \).

2. Let \( X \) be a set and define \( F : \text{Grp}^{\text{op}} \to \text{Set} \) by \( G^{\text{op}} \to \{ \text{left } G\text{-actions on } X \} \). Then the symmetric group \( S(X) \) represents \( F \).

3. Let \( C \) be a locally small category with products and fix \( X, Y \in C \). Let \( F : C^{\text{op}} \to \text{Set} \) be given by \( F(Z) = \text{Hom}(Z, X) \times \text{Hom}(Z, Y) \). This is represented by \( X \times Y \), i.e. \( R_{X \times Y} \cong R_X \times R_Y \). Similarly, \( R^X \times R^Y \cong R^{X \times Y} \) if \( C \) has coproducts.
4. Let \( \mathcal{C} \) be a small category and consider the functor \( \text{Fun}(\mathcal{C}, \text{Set}) \to \text{Set} \) given by \( F \mapsto F(X) \). This functor is represented by \( h^X \).

5. The forgetful functor \( \text{Grp} \to \text{Set} \) is represented by \( Z \).

**Definition 2.4.12 (Adjunction).** Let \( F : \mathcal{C} \to \mathcal{D} \) and \( G : \mathcal{D} \to \mathcal{C} \) be two functors. There are two functors \( \mathcal{C}^{\text{op}} \times \mathcal{D} \to \text{Set} \), given by

\[
(X^{\text{op}}, Y) \mapsto \text{Hom}_\mathcal{C}(X, G(Y)), \quad (X^{\text{op}}, Y) \mapsto \text{Hom}_\mathcal{D}(F(X), Y).
\]

We say that \( F,G \) form an *adjunction pair*, with \( F \) a left adjoint to \( G \) and \( G \) a right adjoint to \( F \), if these two functors are naturally isomorphic.

**Proposition 2.4.13.** Let \( F,G \) and \( F',G \) be adjunction pairs. Then \( F,F' \) are naturally isomorphic.

**Proof.** For any \( X \in \mathcal{C} \), the functor \( \mathcal{D} \to \text{Set} \) given by \( Y \mapsto \text{Hom}_\mathcal{C}(X, G(Y)) \approx \text{Hom}_\mathcal{D}(F(X), Y) = h^{F(X)}(Y) \) is represented by \( F(X) \). The same can be done for \( F' \), so \( F(X) \approx F'(X) \) for all \( X \in \mathcal{C} \). By following the natural transformations, we find that \( F \) and \( F' \) themselves are isomorphic. \( \square \)

**Example 2.4.14.**

1. The forgetful functor \( \text{Grp} \to \text{Set} \) has as a left adjoint \( X \mapsto \text{Free} X \).

2. The inclusion functor \( \text{Ab} \hookrightarrow \text{Grp} \) has as a left adjoint the abelianization functor.

**Definition 2.4.15 (Commuting with products).** Let \( F : \mathcal{C} \to \mathcal{D} \) be a functor between two categories with products. We say that \( F \) commutes with products if the unique natural transformation \( \alpha_{X,Y} : F(X \times Y) \to F(X) \times F(Y) \) is an isomorphism for all \( X,Y \in \mathcal{C} \).

**Proposition 2.4.16.** If \( F : \mathcal{C} \to \mathcal{D} \) has a left adjoint, then \( F \) commutes with products.

**Proof.** Let \( X,Y \in \mathcal{C} \) and \( Z \in \mathcal{D} \). Then

\[
\text{Hom}_\mathcal{D}(Z, F(X \times Y)) \cong \text{Hom}_\mathcal{C}(G(Z), X \times Y) \cong \text{Hom}_\mathcal{C}(G(Z), X) \times \text{Hom}_\mathcal{C}(G(Z), Y) \\
\cong \text{Hom}_\mathcal{D}(Z, F(X)) \times \text{Hom}_\mathcal{D}(Z, F(Y)) \cong \text{Hom}_\mathcal{D}(Z, F(X) \times F(Y)).
\]

**Example 2.4.17.** The forgetful functor \( \text{Grp} \to \text{Set} \) commutes with products.

### 2.5 LIMITS

**Definition 2.5.1 (Limits / colimits).** Let \( \mathcal{I} \) be a small category and \( X \in \mathcal{C} \). Let \( c_X : \mathcal{I} \to \mathcal{C} \) be the constant functor and \( F : \mathcal{I} \to \mathcal{C} \) be some other functor. A morphism \( X \to Y \) induces a natural transformation \( c_X \to c_Y \), so we have a functor \( \mathcal{C}^{\text{op}} \to \text{Set} \) given by \( X^{\text{op}} \mapsto \text{Nat}(c_X, F) \). The *limit* of \( F \) is an object \( \text{lim} F \) in \( \mathcal{C} \) representing this functor, if it exists.

The *colimit* of \( F \) is an object \( \text{colim} F \) representing the functor \( \mathcal{C} \to \text{Set} \) given by \( X \mapsto \text{Nat}(F, c_X) \).
Definition 2.5.2 (Cone). Let $\mathcal{I}$ be a small category with $\text{Ob}\mathcal{I} = \{X_j\}_{j \in J}$, let $\mathcal{C}$ be another category, and $F : \mathcal{I} \to \mathcal{C}$ be a functor. A cone of $F$ is an object $Y \in \mathcal{C}$ together with morphisms $f_j : Y \to F(X_j)$ such that for any morphism $g : X_j \to X_k$ in $\mathcal{I}$, we have $F(g) \circ f_j = f_k$ in $\mathcal{C}$.

Proposition 2.5.3 (Universal property of limits). The limit of a diagram $F : \mathcal{I} \to \mathcal{C}$ is specified by a terminal object in the category of cones to $F$.

Remark 2.5.4. One can similarly construct co-cones by reversing all of the morphisms in $\mathcal{C}$ in the definition of a cone, and then the colimit is an initial object in the category of co-cones of $F$.

Example 2.5.5. 1. If $\mathcal{I}$ has no non-identity morphisms, then

$$\lim F = \prod_{j \in J} F(X_j).$$

2. Let $\mathcal{I}$ be the following diagram and let $\mathcal{C} = \text{Set}$.

```
  ·  \\
  |  ↓  \\
  ·  →  ·
```

A functor $F : \mathcal{I} \to \mathcal{C}$ is then a diagram of the following form in $\mathcal{C}$.

```
    A  \\
   ↓    \\
B  →  C
```

The limit of $F$ is an object $X$, which has morphisms to $A, B, C$, such that for any other such object $Y$, there is a unique morphism $f : Y \to X$ such that the following diagram commutes.

```
    Y  \\
   ↓    \\
X  →  A  \\
   ↓    \\
B  →  C
```

The object $X$, if it exists, is called a pullback or fiber product, and is denoted $A \times_C B$. The colimit of the diagram is simply $C$. 
3 RINGS

3.1 DEFINITIONS AND BASIC PROPERTIES

**Definition 3.1.1** (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 3.1.2.**
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 3.1.3** (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 3.1.4.**
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 $R^\times = \{x \in R \mid x$ is a unit\} forms a group under multiplication.

**Definition 3.1.5** (Unit group). $R^\times$ is the unit group of $R$.

**Definition 3.1.6** (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 3.1.7.** If $R$ is a domain and $xy = xz$ with $x \neq 0$, then $y = z$.

**Example 3.1.8.**
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 $F^\times = F\setminus\{0\}$. 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 $\text{Mat}_n(R) = \{n \times n$ matrices over $R\}$ is a non-commutative ring for $n \geq 2$.
   Its unit group is $(\text{Mat}_n(R))^\times = \text{GL}_n(R)$, the general linear group of degree $n$ over $R$. If $R$ is commutative, then $A \in \text{GL}_n(R)$ if and only if $\det A \neq 0$.
5. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring. It is a domain if and only if $n$ is prime, in which case $\mathbb{Z}/n\mathbb{Z}$ is a field. Its unit group is $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \mid \gcd(a, n) = 1\}$, which has order $\varphi(n)$.  

39
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 $\text{End} A$, is a ring with pointwise addition and composition. It is generally not commutative. Its unit group is $(\text{End} A)^\times = \text{Aut} A$.

7. If $R$ is a ring, then $R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R\}$ 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 $R[\{x_i\}_{i \in I}]$ in infinitely many variables as sums of (finite) monomials.

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

8. Taking variables to be non-commuting, i.e. $x_i x_j \neq x_j x_i$ for $i \neq j$, we obtain non-commutative polynomial rings, which are denoted $R[\{x_i\}_{i \in I}]$.

**Definition 3.1.9** (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 3.1.10.** There is no ring homomorphism $\mathbb{Q} \to \mathbb{Z}$.

**Notation.** The category of rings is denoted $\text{Ring}$, while the category of commutative rings is denoted $\text{CRing}$.

**Proposition 3.1.11.** 1. In $\text{Ring}$, $\mathbb{Z}$ is an initial object.

2. $\text{CRing}$ is a full subcategory of $\text{Ring}$.

3. Forget : $\text{CRing} \to \text{Set}$ has left adjoint $I \mapsto \mathbb{Z}[\{X_i\}_{i \in I}]$.

4. Forget : $\text{Ring} \to \text{Set}$ has left adjoint $I \mapsto \mathbb{Z}[\{X_i\}_{i \in I}]$.

**Definition 3.1.12** (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 3.1.13.** If $S \subset R$ is a subring, then the inclusion $i : S \hookrightarrow R$ is a ring homomorphism.

**Example 3.1.14.** 1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ as subrings.

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

40
3.2 IDEALS

Definition 3.2.1 (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.

Example 3.2.2. 1. Every ring $R$ has the zero ideal $0 = \{0\}$ and the unit ideal $R$.

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

3. 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 $R = R \cdot 1$.

4. The intersection of left ideals is a left ideal.

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

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

Notation. If $R$ is a commutative ring and $x \in R$, then we may write $(x) = Rx = xR$ for the principal ideal generated by $x$. More generally, if $S \subset R$, then we may write $(S)$ for the ideal generated by $S$, i.e. the smallest ideal of $R$ containing $S$.

Proposition 3.2.3. 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 3.2.4 (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 3.2.5. 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 3.2.6 (Kernel / image). Let $f : R \to S$ be a homomorphism.

1. The kernel of $f$ is $f^{-1}(0) \subset R$.

2. The image of $f$ is $f(R) \subset S$.

Proposition 3.2.7. $\ker f \subset R$ is an ideal and $\im f \subset S$ is a subring.

Theorem 3.2.8 (First isomorphism theorem). Let $f : R \to S$ be a ring homomorphism. Then the map $\overline{f} : R/\ker f \to \im f$ given by $\overline{f}(x + \ker f) = f(x)$ is an isomorphism.

Proof. By the first isomorphism theorem for groups, $\overline{f}$ is a group isomorphism of $(R/\ker f, +)$ and $(\im f, +)$. 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 3.2.9 (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 3.2.10.  
1. $\mathbb{Z}/n\mathbb{Z}$ is the quotient of $\mathbb{Z}$ by the ideal $n\mathbb{Z}$.

2. Let $f : \mathbb{R}[x] \to \mathbb{C}$ be given by $f(g) = g(i)$. Then $\ker f = (x^2 + 1)$, 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 $x - y \in I$.

Definition 3.2.11 (Product ring). Let $R$ and $S$ be rings. The product ring $R \times S$ is the Cartesian product of $R$ and $S$ with component-wise operations. This extends to arbitrary products.

Definition 3.2.12 (Relatively prime ideals). Two ideals $I_1, I_2 \subset R$ are relative prime (or coprime) if $I_1 + I_2 = R$.

Theorem 3.2.13 (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 3.2.14. 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 $\ker f = I_1 \cap \cdots \cap I_n$, and by the Chinese remainder theorem, $f$ is surjective, so

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

is an isomorphism by the first isomorphism theorem.

Example 3.2.15. 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.
Definition 3.2.16 (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 3.2.17. An ideal $p \subset R$ is prime if and only if $R/p$ is a domain.

Proof. ($\implies$) 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.

($\impliedby$) 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 $y \in p$. \hfill $\square$

Definition 3.2.18 (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 3.2.19. A commutative ring $R$ has exactly two ideals if and only if $R$ is a field.

Theorem 3.2.20. 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. \hfill $\square$

Example 3.2.21.

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 3.2.22. 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. \hfill $\square$

Corollary 3.2.23. Every non-zero commutative ring has a prime ideal.

3.3 EUCLIDEAN RINGS

Definition 3.3.1 (Euclidean ring). A Euclidean ring is a commutative ring $R$ for which there is a function $\varphi : R \setminus \{0\} \to \mathbb{N}_0$ 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 3.3.2.

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

Definition 3.3.4 (Principal ideal ring). A principal ideal ring is a commutative ring $R$ for which every ideal of $R$ is principal.

Theorem 3.3.5. 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 $I \subset bR$. \qed

Remark 3.3.6. The converse does not hold. For example, $\mathbb{Z}[\frac{1 + \sqrt{-19}}{2}]$ is a principle ideal ring which is not a Euclidean ring.

3.4 FACTORIZATION IN DOMAINS

Throughout, let $R$ be a domain unless otherwise specified.

Definition 3.4.1 (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 3.4.2. 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 3.4.3 (Associates). Two elements $a, b$ in $R$ are associates if $(a) = (b)$.

Definition 3.4.4 (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 $y \in R^\times$.

Definition 3.4.5 (Prime element). A non-zero non-unit element $p \in R$ is prime if $(p)$ is a prime ideal, or equivalently, whenever $p \mid xy$, either $p \mid x$ or $p \mid y$.

Example 3.4.6. In $\mathbb{Z}[\sqrt{-5}]$, 2 is irreducible but not prime, since $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ but 2 does not divide either factor.

Proposition 3.4.7. 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. \qed

Definition 3.4.8 (Factorization). We say that $R$ admits factorization if for any non-zero non-unit $a \in R$, there exist irreducibles $b_1, \ldots, b_n$ such that $a = b_1 \cdots b_n$. 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 $i$. 44
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, and 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 \(i\).

**Definition 3.4.9 (Unique factorization domain).** We say that \( R \) is a unique factorization domain (UFD) if it admits factorization which is unique.

**Proposition 3.4.10.** In a UFD, every irreducible element is prime.

**Proof.** Let \( p \) be irreducible and suppose \( p \mid ab \), so \( ab = cp \) for some \( c \). Since we are in a UFD, we can write \( a, b, c \) as products of irreducibles

\[
a = q_1 \cdots q_l, \quad b = r_1 \cdots r_m, \quad c = s_1 \cdots s_n,
\]

so we have

\[
q_1 \cdots q r_1 \cdots r_m = p s_1 \cdots s_n.
\]

By unique factorization, we have \( l + m = n + 1 \) and that \( p \) is an associate of some \( q_i \) or some \( r_j \). If \( p \) is an associate of some \( q_i \), then \( p \mid q_i \mid a \). Otherwise, \( p \) is an associate of some \( r_j \), and then \( p \mid r_j \mid b \). Thus \( p \) is prime. \( \square \)

**Theorem 3.4.11.** A domain \( R \) is a UFD if and only if \( R \) admits factorization and every irreducible element is prime.

**Proof.** \((\Rightarrow)\) Immediate from proposition.

\((\Leftarrow)\) We must show that factorization in \( R \) is unique. To do this, we induct on the length of the minimal length factorization of a non-zero non-unit element into irreducibles.

For the base case, where this factorization has length 1, let \( a \) be irreducible and \( a = q_1 \cdots q_m \) be a factorization into irreducibles. Since \( a \) is also prime, without loss of generality \( a \mid q_m \).

Since \( q_m \) is irreducible, \( a \) and \( q_m \) are associates. Letting \( q_m = ua \) for some \( u \in R^\times \), we have

\[
a = q_1 \cdots q_{m-1} ua,
\]

so

\[
1 = q_1 \cdots q_{m-1} u.
\]

This shows that \( q_1, \ldots, q_{m-1} \) are units, which means that \( m = 1 \) and \( a = q_m = q_1 \).

Now suppose the minimal length factorization has length \( n \), with \( a = p_1 \cdots p_n \), and let \( a = q_1 \cdots q_m \) be another factorization into irreducibles. Since \( b_n \) is also prime, without loss of generality \( b_n \mid c_m \). Since \( c_m \) is irreducible, \( b_n \) and \( c_m \) are associates, with \( c_m = ub_n \) for some \( u \in R^\times \). This gives us

\[
b_1 \cdots b_{n-1} = c_1 \cdots c_{m-1} u = c_1 \cdots c'_{m-1},
\]

where \( c'_{m-1} = uc_{m-1} \) is an associate of \( c_{m-1} \). By induction, the result follows. \( \square \)

**Definition 3.4.12 (Noetherian ring).** Let \( R \) be a commutative ring. We say that \( R \) is noetherian if any 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 \( n \geq N \).
**Theorem 3.4.13.** Let $R$ be a commutative ring. The following are equivalent:

1. every ideal in $R$ is finitely generated;
2. $R$ is noetherian;
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 $a_i \in I_n$, 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 $I_1 \not\subset I_2$. This process must stop at some maximal $I_n$, as otherwise, we obtain a strictly ascending chain $I_1 \not\subset I_2 \not\subset \cdots$, 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 $x \in I \setminus I'$, 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.

**Corollary 3.4.14.** Every PID is noetherian.

**Theorem 3.4.15.** 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 $(a) \not\subset (b)$ and $(a) \not\subset (c)$. 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 3.4.16.** If $R$ is noetherian and every irreducible element is prime, then $R$ is a UFD.

**Corollary 3.4.17.** Every PID is a UFD.

**Proof.** It remains to show that in a PID $R$, irreducibles are prime. Let $p \in R$ be irreducible and suppose that $p \mid ab$, but $p \nmid a$. Pick $d \in R$ so that $pR + aR = dR$. Then $d \mid p$ and $d \mid a$, but $p \nmid a$, so since $p$ is irreducible, $d$ is a unit, wlog $d = 1$. There exist $r, s \in R$ so that $pr + as = 1$. Then $prb + abs = b$, and the left hand side is divisible by $p$, so $p \mid b$, as required.

### 3.5 FACTORIZATION IN POLYNOMIAL RINGS

Throughout, let $R$ be a UFD unless stated otherwise.

**Definition 3.5.1** (Greatest common divisor). Let $\{a_i\}$ be elements of $R$. A greatest common divisor (GCD) for $\{a_i\}$ is an element $d \in R$ such that $d \mid a_i$ for all $i$ and, if $c \mid a_i$ for all $i$, then $c \mid d$. 
Proposition 3.5.2. The GCD is unique up to multiplication by units.

Proof. If $d$ and $d'$ are greatest common divisors of elements $\{a_i\}$, then $d \mid d'$ and $d' \mid d$. \qed

Proposition 3.5.3. In a UFD, the GCD of a finite set of elements exists.

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

$$a_i = p_{i,1}^{e_{i,1}} \cdots p_{i,r}^{e_{i,r}}, \quad e_{ij} \geq 0.$$ 

The GCD is then

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

\qed

Definition 3.5.4 (Content). Let $f = a_0 + \cdots + a_n x^n \in R[x]$. The content of $f$, denoted $\text{cont } f$, is the ideal of $R$ generated by a GCD of $a_0, \ldots, a_n$.

Since the GCD is unique up to multiplication by units, the content is well-defined as an ideal. We may refer to any of the generators of this ideal as the content if we wish to work with elements rather than ideals.

Definition 3.5.5 (Primitive polynomial). A polynomial $f \in R[x]$ is primitive if $\text{cont } f = R$.

Proposition 3.5.6. If $a \in R$ and $f \in R[x]$, then $\text{cont}(af) = a \text{ cont } f$.

Lemma 3.5.7 (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 $\overline{fg} \neq 0$, showing that $p$ does not divide every coefficient of $fg$. Hence $fg$ is primitive. \qed

Corollary 3.5.8. If $f, g \in R[x]$, then $\text{cont}(fg) = (\text{cont } f)(\text{cont } g)$.

Definition 3.5.9 (Quotient field). Let $R$ be an integral domain. The quotient field (or field of fractions) $F$ of $R$ is the set

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

together with operations

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

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

Proposition 3.5.10. 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 unique 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 $g \circ i = f$. 

47
Lemma 3.5.11 (Gauss). Let \( R \) be a UFD and \( F \) be its quotient field. Then \( f \in R[x] \) is irreducible if and only if \( f \in F[x] \) is irreducible.

Proof. to be written

Theorem 3.5.12. If \( R \) is a UFD, then \( R[x] \) is a UFD.

Proof. to be written

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 \( \alpha_i \in F \) such that \( q_i = \alpha_i f_i \in R[x] \) is primitive. Then \( \beta = \alpha_1 \cdots \alpha_m \in R \) is the product of two primitive elements is primitive. Since \( q_1 \cdots q_m \mid f \) in \( F[x] \), it also holds in \( R[x] \), so \( \beta \in R \). Finally, factor \( \beta \) in \( R \).

Theorem 3.5.13 (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 \( f = \beta q_1 \cdots q_m \in F[x] \), so the constant terms of \( g \) and \( h \) are both divisible by \( p \) (factorization over \( K[x] \) is unique). Then \( p^2 \nmid a_0 \), a contradiction.

Example 3.5.14. 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.

3.6 Factorization in quadratic fields

Definition 3.6.1 (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 3.6.2 (Conjugate). The conjugate of \( x + y\sqrt{d} \in K \) is \( x - y\sqrt{d} \).
Proposition 3.6.3. Let $\alpha, \beta \in K$. Then
1. $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$;
2. $\overline{\alpha \beta} = \overline{\alpha} \overline{\beta}$;
3. $\overline{\alpha} = \alpha$; 
4. $\overline{\alpha} = \alpha$ if and only if $\alpha \in \mathbb{Q}$.

Definition 3.6.4 (Trace / norm). Let $\alpha = x + y\sqrt{d} \in K$.
1. The trace of $\alpha$ is $\text{tr}(\alpha) = \alpha + \overline{\alpha} = 2x$.
2. The norm of $\alpha$ is $\text{N}(\alpha) = \alpha \overline{\alpha} = x^2 - dy^2$.

Theorem 3.6.5. Let $\alpha, \beta \in K$. Then
\[ \text{tr}(\alpha + \beta) = \text{tr}(\alpha) + \text{tr}(\beta), \quad \text{N}(\alpha \beta) = \text{N}(\alpha) \text{N}(\beta). \]

For any $\alpha \in K$, we have
\((x - \alpha)(x - \overline{\alpha}) = x^2 - \text{tr}(\alpha)x + \text{N}(\alpha) \in \mathbb{Q}[x].\)

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

Definition 3.6.6 (Algebraic integer). We say that $\alpha \in K$ is an (algebraic) integer if $\text{tr}(\alpha), \text{N}(\alpha) \in \mathbb{Z}$.

Example 3.6.7. 1. If $\alpha \in \mathbb{Z}[\sqrt{d}]$, then $\text{tr}(\alpha)$ and $\text{N}(\alpha)$ are in $\mathbb{Z}$, so $\alpha$ 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 3.6.8. 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 $\text{tr}(\alpha) = 2x$ and $\text{N}(\alpha) = x^2 - dy^2$ 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 $c^2 - d(2y)^2 \equiv c^2 \neq 0 \pmod{4}$, a contradiction. If $y$ is half an odd integer, then we must have $d \equiv 1 \pmod{4}$. \qed

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

49
**Theorem 3.6.9.** 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.** ( \( \Rightarrow \) ) If \( \alpha \in \mathcal{O}_K \), then \( (x - \alpha)(x - \overline{\alpha}) \) will do.

( \( \Leftarrow \) ) 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 \( \alpha \not\in \mathbb{Q} \) and \( \alpha^2 + ma + n = 0 \), then since we also have \( \alpha^2 - \text{tr}(\alpha)\alpha + N(\alpha) = 0 \), we get

\[
(m + \text{tr}(\alpha))\alpha + (n - N(\alpha)) = 0.
\]

Since \( \alpha \not\in \mathbb{Q} \), this means \( m + \text{tr}(\alpha) = 0 \) and \( n - N(\alpha) = 0 \), from which it follows that \( \text{tr}(\alpha) \) and \( N(\alpha) \) are ordinary integers.

**Theorem 3.6.10.** 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 3.6.11.** \( \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z} \) and \( K = \{ \alpha/\beta \mid \alpha, \beta \in \mathcal{O}_K \} \).

**Theorem 3.6.12.** If \( \alpha \in \mathcal{O}_K \), then \( \overline{\alpha} \in \mathcal{O}_K \).

**Theorem 3.6.13.** Let \( K \) be a quadratic field. Then

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

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 \( \alpha \) is a unit with inverse \( \overline{\alpha} \).

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

### 3.7 THE SPECTRUM OF A COMMUTATIVE RING

Let \( R \) be a commutative ring.

**Definition 3.7.1** (Spectrum). The **spectrum** of \( R \), denoted \( \text{Spec} \ R \), is the set of prime ideals of \( R \).

**Notation.** For any subset \( S \subset R \), let

\[
V(S) = \{ \mathfrak{p} \in \text{Spec} \ R \mid S \subset \mathfrak{p} \}.
\]

**Definition 3.7.2** (Radical of an ideal). Let \( I \) be an ideal of \( R \). The **radical** of \( I \) is

\[
\sqrt{I} = \{ x \in R \mid x^n \in I \text{ for some } n \in \mathbb{N} \}.
\]
Lemma 3.7.3.  1. If \( I \) is the ideal generated by \( S \), then \( V(S) = V(I) = V(\sqrt{I}) \).

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

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

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 \( p \in \text{Spec} \ R \) 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 \( p \in \text{Spec} \ R \) 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 \( x \in I_1 \setminus p \). 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. \( \square \)

Definition 3.7.4 (Zariski topology). The Zariski topology is the topology on \( \text{Spec} \ R \) defined by taking the closed sets to be the sets \( V(I) \) for ideals \( I \subset R \).

Example 3.7.5.  1. If \( F \) is a field, then \( \text{Spec} \ F = \{0\} \) has one point.

2. \( \text{Spec} \ Z = \{ pZ \mid p \in Z \text{ a prime number or 0} \} \).

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

4. Since \( C[x] \) is a PID, prime ideals are in bijection with monic irreducible polynomials in \( C[x] \).

Since \( C \) is algebraically closed, the monic irreducible polynomials are precisely in monic irreducibles \( x - \alpha \) for \( \alpha \in C \). Thus \( \text{Spec} \ C[x] = \{ x - \alpha \mid \alpha \in C \} \cup \{0\} \). As in \( \text{Spec} \ Z \), every point except for 0 is closed, and 0 is generic in the sense that its closure is \( \text{Spec} \ C[x] \). There is a bijection \( \text{Spec} \ C[x] \to C \cup \{\ast\} \) where \( x - \alpha \to \alpha \) and \( 0 \to \ast \).

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

Proposition 3.7.6. If \( R \) is a commutative ring, then \( \text{Nil} R \) is the intersection of all prime ideals.

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

Lemma 3.7.7. \( \{D(f)\}_{f \in R} \) is a basis for the Zariski topology.
Proof. Let $U$ be an open subset of $\text{Spec } R$, i.e. $U = \text{Spec } R \setminus V(I)$ 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 $f \in I \setminus p$, so $p \in D(f)$, and hence $U \subset \bigcup_{f \in I} D(f)$.

Lemma 3.7.8. $\sqrt{I}$ is the intersection of all prime ideals containing $I$.

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

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

by the earlier bijection. \hfill \Box

Proposition 3.7.9. 1. $D(f) \cap D(g) = D(fg)$;

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

3. $D(f) = \text{Spec } R$ 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. $f \in \text{Nil } R$ 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 $f \not\in p$ for all $p \in \text{Spec } R$ if and only if $D(f) = \text{Spec } R$.

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 $(g)$. \hfill \Box
4 MODULES

4.1 DEFINITIONS AND BASIC EXAMPLES

Definition 4.1.1 (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

1. $r(m + n) = rm + rn$ for all $r \in R$ and $m, n \in M$;
2. $(r + s)m = rm + sm$ for all $r, s \in R$ and $m \in M$;
3. $1 \cdot m = m$ for all $m \in M$;
4. $r(sm) = (rs)m$ for all $r, s \in R$ and $m \in M$.

Right $R$-modules are defined analogously.

Remark 4.1.2. 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 4.1.3. 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 4.1.4. 1. If $F$ is a field, then $F$-modules are vector spaces over $F$.
2. $\mathbb{Z}$-modules are abelian groups.
3. Left (right) ideals are also left (right) $R$-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 $R$.
4. 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 $rm = f(r)m$.
5. Let $M$ be an abelian group. Then $M$ is a left $(\text{End} M)$-module by $f \cdot m = f(m)$.
6. Let $M$ be a left $R$-module. There is a ring homomorphism $R \to \text{End} M$ 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 $f : R \to \text{End} M$ is a ring homomorphism, then we can pull back the left $(\text{End} M)$-module structure on $M$ to make $M$ a left $R$-module.

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

Proposition 4.1.5 (Universal property of the endomorphism ring). Let $M$ be an abelian group. There is a contravariant functor $\text{Ring} \to \text{Set}$ sending $R$ to the set of all left $R$-module structures on $M$, and this functor is corepresented by $\text{End} M$. 

53
Definition 4.1.6 (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 $R$-$\text{Mod}$ and the category of right $R$-modules is denoted $\text{Mod}$-$R$.

For convenience, “$R$-module” will be taken to mean “left $R$-module” unless otherwise specified.

Definition 4.1.7 (Submodule). A subgroup $N \subset M$ is an $R$-submodule of $M$ if $RN \subset N$.

Definition 4.1.8 (Kernel / image). Let $M, N$ be $R$-modules and $f : M \to N$ be an $R$-module homomorphism. The kernel of $f$ is $\text{ker } f = f^{-1}(0)$ and the image of $f$ is $\text{im } f = f(M)$.

Proposition 4.1.9. $\text{ker } f \subset M$ and $\text{im } f \subset N$ are $R$-submodules.

Definition 4.1.10 (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 4.1.11 (Isomorphism theorems). 1. If $f : M \to N$ is an $R$-module homomorphism, then $\overline{f} : M/\text{ker } f \to \text{im } f$ 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 4.1.12 (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

$$
\{\text{R-submodules of } M/N\} \leftrightarrow \{\text{R-submodules of } M \text{ containing } N\},
$$

$$
\mathcal{P} \leftrightarrow q^{-1}(\mathcal{P}),
$$

$$
P/N \leftrightarrow P.
$$

4.2 EXACT SEQUENCES OF MODULES

Let $\{M_i \mid i \in I\}$ be a family of $R$-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 4.2.1 (Direct sum). Let $\{M_i \mid i \in I\}$ be a family of $R$-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 4.2.2. The direct sum of modules is the categorical coproduct of $R$-modules, i.e.

$$
\bigoplus_{i \in I} M_i = \prod_{i \in I} M_i.
$$
Proof. Let $M = \bigoplus_i M_i$ and for $i \in I$, define $f_i : M_i \to M$ by $f_i(m) = (m_i)$ 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

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

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

For given (left) $R$-modules $M, N$, the hom-set $\text{Hom}_R(M, N)$ forms an abelian group, so together with the existence of products and coproducts, $R$-$\text{Mod}$ is said to be an additive category.

As with groups, we can define 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 $\ker g = \text{im} f$. Then we can identify $N$ with $\text{im} f$, which gives

$$M/N = M/\ker g \cong \text{im} g = P.$$

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

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

is a short exact sequence.

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

The morphism $(u, v, w)$ is an isomorphism if and only if $u, v, w$ are isomorphisms. Every short exact sequence is isomorphic to a “standard” short exact sequence, i.e. the one for $N \subset M$ a submodule.

**Theorem 4.2.3.** 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 $g \circ g' = \text{id}_P$;
2. (left split) there exists $f' : M \to N$ such that $f' \circ f = \text{id}_N$;
3. this short exact sequence is isomorphic to $0 \to N \to N \oplus P \to P \to 0$.
4.2 Exact sequences of modules

Proof. (1) \implies (2) Let \( h : M \to M \) be given by \( h = \text{id}_M - g' \circ g \). Then \( g \circ h = g - g \circ g' \circ g = 0 \), so \( \text{im} \, h \subset \ker g = \text{im} \, f = N \), 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.

\[
\begin{array}{ccc}
0 & \to & N \\
\downarrow{1_N} & & \downarrow{(f',g)} \\
0 & \to & N \oplus P \\
\end{array}
\]

\[
\begin{array}{ccc}
P & \to & 0 \\
\downarrow{1_P} & & \\
0 & \to & P \\
\end{array}
\]

(3) \implies (1) Obvious.

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

**Example 4.2.4.** Consider the sequence

\[
0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0.
\]

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.

Let \( f : N \to M \). Then there is a group homomorphism \( f_* : \text{Hom}_R(X,N) \to \text{Hom}_R(X,M) \) given by \( g \mapsto f \circ g \), so for a fixed \( X \), we have a functor \( R\text{-Mod} \to \text{Ab} \) given by \( N \mapsto \text{Hom}_R(X,N) \) and \( f \mapsto f_* \). Similarly, there is a group homomorphism \( f^* : \text{Hom}_R(M,X) \to \text{Hom}_R(N,X) \) given by \( g \mapsto g \circ f \). This gives us a contravariant functor, i.e. a functor \( (R\text{-Mod})^{op} \to \text{Ab} \) with \( N^{op} \mapsto \text{Hom}_R(N,X) \) and \( f^{op} \mapsto f^* \).

Now consider a short exact sequence \( 0 \to N \to M \to P \to 0 \) and a fixed \( X \). Applying the first functor, we obtain a sequence in \( \text{Ab} \),

\[
0 \longrightarrow \text{Hom}_R(X,N) \xrightarrow{f_*} \text{Hom}_R(X,M) \xrightarrow{g_*} \text{Hom}_R(X,P) \longrightarrow 0.
\]

This is generally not exact, but if we remove the last 0, then it becomes exact. If \( f \) is injective, then \( f_*(g) = f \circ g = 0 \), so \( g = 0 \), which shows that \( \ker f_* = 0 \), i.e. \( f_* \) is injective. If \( h \in \text{Hom}_R(X,M) \), then \( g_*(h) = g \circ h = 0 \) if and only if \( \text{im} \, h \subset \ker g = \text{im} \, f \). Hence we can find \( k \in \text{Hom}_R(X,N) \) for which \( f \circ k = h \), so \( h \in \ker g_* \) if and only if \( h \in \text{im} \, f_* \).

Thus the functors \( \text{Hom}_R(X,-) \) and \( \text{Hom}_R(X,-) \) are said to be left exact.

There is a canonical isomorphism (of groups) \( \text{Hom}_R(M,N_1 \oplus N_2) \cong \text{Hom}_R(M,N_1) \oplus \text{Hom}_R(M,N_2) \). This generalizes to finite direct sums as

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

with the right being an (additive) group of matrices and the operation on elements being given by matrix multiplication.
4.3 FREE, PROJECTIVE, AND INJECTIVE MODULES

Definition 4.3.1 (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 4.3.2. 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 $\{e_x\}$.

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

Theorem 4.3.4 (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. to be written

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

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

Remark 4.3.5. 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 4.3.6. Every left $R$-module is isomorphic to a quotient of a free module.

Proof. to be written

Proposition 4.3.7. Let $P$ be a (left) $R$-module. The following are equivalent:

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

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

\begin{equation}
\begin{array}{c}
P \\
h \downarrow \\
B & \xrightarrow{f} & C \\
g \downarrow \\
\end{array}
\end{equation}

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

57
Proof. (1) $\iff$ (2) Let $0 \to A \to B \to C \to 0$ be a short exact sequence. Then

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

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

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

$$
\begin{array}{ccc}
0 & \to & N \\
\downarrow & & \downarrow f \\
M & \to & P \\
\downarrow & & \downarrow 1_P \\
P & \to & 0
\end{array}
$$

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.

$$
\begin{array}{ccc}
P & \to & C \\
\downarrow 1_P & & \downarrow 1_P \\
P & \to & P
\end{array}
$$

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 $k : M \to P$. Let $N = \ker k$. We then have the following diagram.

$$
\begin{array}{ccc}
0 & \to & N \\
\downarrow & & \downarrow i \\
M & \xrightarrow{k} & P \\
\downarrow & & \downarrow g \\
B & \xrightarrow{f} & C \\
\downarrow & & \downarrow 1_P \\
0 & \to & 0
\end{array}
$$

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

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

\[ \Box \]

**Definition 4.3.8** (Projective module). We say that $P$ is a projective (left) $R$-module if $P$ satisfies any of the conditions above.

**Example 4.3.9.** Free modules are projective.

**Definition 4.3.10** (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 $N \oplus N' = M$. 

58
Theorem 4.3.11. 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

$$0 \longrightarrow N \longrightarrow F \longrightarrow P \longrightarrow 0$$

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 $\text{Hom}_R(P \oplus P', -) = \text{Hom}_R(P, -) \oplus \text{Hom}_R(P', -)$ is exact. Thus both $\text{Hom}_R(P, -)$ and $\text{Hom}_R(P', -)$ are exact, so $P$ is projective.

Example 4.3.12. 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 $R^3 \rightarrow R$, 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 $R^3 \rightarrow R$, then we have a split short exact sequence

$$0 \longrightarrow PR^3 \longrightarrow R \longrightarrow 0$$

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 $\text{Hom}_R(-, X)$.

Proposition 4.3.13. Let $N$ be a (left) $R$-module. The following are equivalent:

1. the functor $\text{Hom}_R(-, N)$ is exact;
2. for a diagram of the below form, there exists $h : B \rightarrow N$ such that $h \circ f = g$;
3. every short exact sequence $0 \rightarrow N \rightarrow M \rightarrow P \rightarrow 0$ is split.

Definition 4.3.14 (Injective module). We say that $N$ is an injective (left) $R$-module if $N$ satisfies any of these conditions.

Example 4.3.15. 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 $\mathbb{Q}, \mathbb{Q}/\mathbb{Z}, \mathbb{R}/\mathbb{Z}$. 
Throughout, let \( R \) be a PID, \( F \) be its quotient field, and \( M \) be an \( R \)-module.

**Definition 4.4.1** (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 \( M_{\text{tors}} \).

We say that \( M \) is torsion free if \( M_{\text{tors}} = 0 \).

**Lemma 4.4.2.** \( M/M_{\text{tors}} \) is torsion free.

**Proof.** Let \( m + M_{\text{tors}} \in M/M_{\text{tors}} \) with \( m \not\in M_{\text{tors}} \) 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

\[
0 \longrightarrow M_{\text{tors}} \longrightarrow M \longrightarrow M/M_{\text{tors}} \longrightarrow 0
\]

(†)

**Definition 4.4.3** (Rank). The rank of \( M \) is the dimension of \( FM \) as an \( F \)-vector space.

If \( M \) is finitely generated, then \( \text{rank } M < \infty \).

**Example 4.4.4.** If \( M = R^n \), then \( \text{rank } M = n \).

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

**Proposition 4.4.5.** 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 (otherwise).

For the induction step, let \( \{m_1, \ldots, m_n\} \) 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 \( M'_{\text{tors}} \) free with basis \( \{m_1, \ldots, m_{n-1}\} \). 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

\[
0 \longrightarrow M'_{\text{tors}} \cap N \longrightarrow N \longrightarrow \frac{f}{I} \longrightarrow 0
\]

By induction, \( M'_{\text{tors}} \cap N \subset M' \) 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 \( N \cong (M'_{\text{tors}} \cap N) \oplus I \) is free of rank at most \( n \).

Free \( R \)-modules are torsion free.

**Remark 4.4.6.** The converse of this statement is false. For example, \( \mathbb{Q} \) is torsion free but not a free module over \( \mathbb{Z} \).
Theorem 4.4.7. Every finitely generated torsion-free \( R \)-module is free.

Proof. Let \( M \) be finitely generated and take its embedding \( M \to FM \), which is a vector space of dimension \( n = \text{rank} \, M \) over \( F \). Let \( \{x_1, \ldots, x_n\} \) be a basis for \( FM \), so then
\[
FM = \bigoplus_{i=1}^{n} Fx_i.
\]

Let
\[
P = \bigoplus_{i=1}^{n} Rx_i
\]
be the free \( R \)-module with basis \( \{x_1, \ldots, x_n\} \). Given any \( m \in M \), we can write \( m = \sum \alpha_i x_i \) with \( \alpha_i \in F \). Clearing denominators, \( am = \sum \alpha_i a \alpha_i x_i \) with \( a \alpha_i \in R \) for all \( i \), so then \( am \in P \).

Since \( M \) is finitely generated by some \( \{m_1, \ldots, m_s\} \), 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 \( M/M_{\text{tors}} \) is finitely generated and torsion-free, so it is free and \( M/M_{\text{tors}} \cong R^n \) with \( n = \text{rank} \, M \). Thus the short exact sequence is split and \( M \cong M_{\text{tors}} \oplus R^n \). From this decomposition, \( M_{\text{tors}} \) is finitely generated.

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

Definition 4.4.8 (p-primary). We say that \( m \in M \) is \( p \)-primary if \( p^n m = 0 \) for some \( n > 0 \).

\( M \) is a \( p \)-primary module if \( p^n M = 0 \) for some \( n > 0 \), or equivalently, if all \( m \in M \) are \( p \)-primary.

\( M \) is primary if \( M \) is \( p \)-primary for some \( p \).

Example 4.4.9. \( M = R/p^n \) is \( p \)-primary.

Notation. Let \( M(p) \) be the submodule of all \( p \)-primary elements of \( M \), called the \( p \)-primary part of \( M \).

Lemma 4.4.10. Let \( a_1, \ldots, a_n \in R \) be relatively prime (not necessarily pairwise) in the sense of having no non-unit common divisor. Then there exist \( b_1, \ldots, b_n \in R \) such that \( \sum a_i b_i = 1 \).

Proof. The ideal generated by \( (a_1, \ldots, a_n) \) 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 4.4.11. Let \( m \in M \) and suppose \( a_1 m = \cdots = a_n m = 0 \) for relatively prime \( a_1, \ldots, a_n \). Then \( m = 0 \).

Theorem 4.4.12. Let \( M \) be a finitely generated torsion \( R \)-module. Then \( M(p) = 0 \) for all but finitely many \( p \), and
\[
M = \bigoplus_p M(p).
\]
**Proof.** There exists a non-zero \( a \in R \) such that \( aM = 0 \). Suppose \( M(p) \neq 0 \) for \( p = (p) \) and let 
\( m \in M(p) \) be non-zero, so \( p^m m = 0 \). Since \( m \neq 0 \), it must be that \( p \mid a \). There are only finitely many prime divisors of \( a \), hence only finitely many \( p \) with \( M(p) \neq 0 \), and all such \( p \) contain \( a \). 

Factor \( a = up_1^{k_1} \cdots p_n^{k_n} \) with \( p_i, p_j \) not associates for \( i \neq j \). Then \( a_i = a/p_i^{k_i} \). Then \( a_1, \ldots, a_n \) are relatively prime, so \( \sum a_i b_i = 1 \) for some \( b_i \). Then \( m = \sum a_i b_i m \) and for each \( i \), we have \( a_i b_i m \in M(p) \), so \( M = \sum M(p) \). 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 \( b_i = \prod_{j \neq i} p_j^{k_j} \). We also have \( p_i^{k_i} m_i = 0 \), and so \( m_i = 0 \).

**Definition 4.4.13 (Cyclic module).** We say that \( M \) is cyclic if \( M \) is generated by one element.

**Example 4.4.14.** If \( I \subset R \) is an ideal, then \( R/I \) is cyclic.

If \( p = pR \neq 0 \) is a prime ideal, then \( R/p^n = R/p^n R \) is \( p \)-primary cyclic.

**Proposition 4.4.15.** Every cyclic \( R \)-module \( M \) is isomorphic to one of the form \( R/I \) for some ideal \( I \subset R \).

**Proposition 4.4.16.** If \( M \) is an \( R \)-module and \( I \subset R \) is an ideal such that \( IM = 0 \), then \( M \) has the structure of an \( R/I \)-module via \( (r + I)m = rm \).

If \( M, N \) are \( R \)-modules with \( IM = IN = 0 \) and \( f : M \to N \) is an \( R/I \)-module homomorphism, then \( f \) also gives an \( R \)-module homomorphism.

**Example 4.4.17.** Let \( p \subset R \) be non-zero prime. Then \( R/p = k \) is a field.

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

Let \( M \) be a finitely generated \( p \)-primary module with \( p^n M = 0 \). We have a descending chain

\[
M \supset pM \supset \cdots \supset p^n M = 0.
\]

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

**Definition 4.4.18 (Length).** The length of a finitely generated \( p \)-primary module with \( p^n M = 0 \) is

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

**Example 4.4.19.** We have \( l(R/p^n) = n \), as for \( i \leq n \),

\[
p^{i-1}(R/p^n)/p^i R = \bigoplus_{i=0}^{n-1} R/p^i R = k.
\]

**Proposition 4.4.20.**

1. \( l(M \oplus N) = l(M) + l(N) \).

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

**Proof.**

1. to be written
2. Let $\mathcal{M} = M/N$. For each $i$, projection gives a surjective map $\varphi_i: p^{i-1}M/p^iM \twoheadrightarrow p^{-1}\mathcal{M}/p\mathcal{M}$.

To show strict inequality, we must show that for some $i$, this map has non-trivial kernel. There is a unique $i$ such that $p^iM \not\subset N \subset p^{i-1}M$. Then the image of $N$ in $p^{i-1}M/p^iM$ is not zero, but is in the kernel of $\varphi_i$.

\[\square\]

**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 $p \cdot pM = 0$, so it is also a $k$-vector space.

**Lemma 4.4.21.** Let $M$ be an $R$-module and $p = pR$ be a prime ideal such that $p^nM = 0$ and $p^{n-1}M \neq 0$. If $\dim_k(pM) = 1$, then $M \cong R/p^nR$.

**Proof.** We induct on $n$. If $n = 1$, then $pM = 0$, so $M = pM \cong k = R/p$.

For the inductive step, there exists $x \in M$ for which $p^nx = 0$ but $p^{n-1}x \neq 0$. Suppose $rx = 0$ for $r = p^mq$ with $p \nmid q$. We claim that $m \geq n$. Suppose otherwise, so then $q(p^nx) = p^{n-m}(p^nx) = 0$. Since $q$ and $p^{n-m}$ are relatively prime, $p^nx = 0$, contradicting the choice of $n$.

Define a map $R \to M$ by $r \mapsto rx$. This induces a map $f: R/p^n \to M$, which we claim is an isomorphism. To see that $f$ is injective, if $rx = 0$, then $p^n | r$ from what we noted above, so $r + p^n = p^n$. 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 $p^my = 0$. 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, $y = sp^{n-1}$ for some $s \in R$. Inducting on $m$, if $p^my = 0$, then $p^{n-1}(py) = 0$, so $py$ is a multiple of $x$, say $py = sx$ for some $s \in R$. Then $p^{n-1}sx = 0$, so $p^n | p^{n-1}s$. This means that $p | s$ 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 $x$.

\[\square\]

**Proposition 4.4.22.** Let $M$ be a finitely generated $R$-module and $p \subset R$ be a non-zero prime ideal such that $p^nM = 0$ and $p^{n-1}M = 0$ for some $n > 0$. Then there exists a surjective $R$-module homomorphism $M \to R/p^n$.

**Proof.** There exists $x \in M$ for which $p^nx = 0$ and $p^{n-1}x \neq 0$, where $p = pR$. Then $p^{n-1}x \in pM$ is non-zero, so $\dim_k(pM) = 1$, then $M \cong R/p^n$. 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 $\mathcal{M} = M/N$. Since $N \neq 0$, we have $l(barM) < l(M)$ and $p^\mathcal{M} = 0$, while $p^{n-1}x \neq 0$ since $p^{n-1}x \not\in N$, so $p^n\mathcal{M} \neq 0$. By strong induction on $l(M)$, there is a surjective homomorphism $\mathcal{M} \to R/p^n$, so we can compose this with the quotient map.

\[\square\]

**Theorem 4.4.23.** Let $M$ be a finitely generated $R$-module. Then $M$ is a finite direct sum of cyclic modules of the form $R$ and $R/p^n$ for $p \subset R$ non-zero prime.

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

\[\square\]

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

\[l_n(p) = \dim_k(p^{n-1}M(p)/p^nM(p))\] is the number of cyclic summands $R/p^n$ in $M(p)$ with $m \geq n$.
Remark 4.4.24. The number of cyclic summands $R$ is equal to the rank of $M$, and the number of cyclic summands $R/p^n$ is $l_n(p) - l_{n+1}(p)$. Hence the decomposition is unique up to re-ordering.

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

$$M_{\text{tors}} \cong R/p_1^{\alpha_1} \oplus \cdots \oplus R/p_r^{\alpha_r}$$

$$R/p_1^{\alpha_1} \oplus \cdots \oplus R/p_s^{\alpha_s},$$

with $p_1, \ldots, p_s$ distinct non-zero prime ideals and $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_r$ for each $i$. The powers of prime ideals $\{P_1^{\alpha_i}\}$ are elementary divisors of $M$. Denote this family by ED($M$).

Theorem 4.4.25 (Elementary divisor form). Two finitely generated modules $M$ and $N$ over a PID $R$ are isomorphic if and only if $\text{rank } M = \text{rank } N$ and $\text{ED}(M) = \text{ED}(N)$.

By the Chinese remainder theorem, if $I_j = p_1^{\alpha_{1j}} \cdots p_s^{\alpha_{sj}}$, then

$$R/p_1^{\alpha_{1j}} \oplus \cdots \oplus R/p_s^{\alpha_{sj}} \cong R/I_j.$$ 

We may thus write

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

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

Theorem 4.4.26 (Invariant factor form). Two finitely generated modules $M$ and $N$ over a PID $R$ are isomorphic if and only if $\text{rank } M = \text{rank } N$ and IF($M$) = 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 $\{y_1, \ldots, y_m\}$ be generators for $N$. We can write

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

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

Suppose

$$A = \begin{pmatrix}
    r_1 & \cdots & r_m \\
    \vdots & \ddots & \vdots \\
    0 & \cdots & 0
\end{pmatrix} \quad (\dagger)$$

with $r_1 | \cdots | r_m \neq 0$. 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 \( \{ r_1 R, \ldots, r_n R \} \), but with \( r_i R \) 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 (I).

**Example 4.4.27.** Let \( R = \mathbb{Z} \) and \( M = \mathbb{Z}^2/(\langle (4, 2), (2, 4) \rangle) \). 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 \( \text{IF}(M) = \{ 2\mathbb{Z}, 6\mathbb{Z} \} \) and \( \text{ED}(M) = \{ 2\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z} \} \).

### 4.5 ABELIAN GROUPS

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

**Theorem 4.5.1** (ED form). Every finitely generated abelian group is isomorphic to a direct sum of cyclic groups \( \mathbb{Z} \) and \( \mathbb{Z}/p^k \mathbb{Z} \) for \( p \) prime. Two finitely generated abelian groups \( M \) and \( N \) are isomorphic if and only if \( \text{rank} M = \text{rank} N \) and \( \text{ED}(M) = \text{ED}(N) \).

**Theorem 4.5.2** (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 \( \text{rank} M = \text{rank} N \) and \( \text{IF}(M) = \text{IF}(N) \).

**Example 4.5.3.**

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 \( \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z} \).

### 4.6 MODULES OVER \( F[X] \)

Let \( F \) be a field and suppose \( V \) is an \( F[X] \)-module. Since \( F \subseteq F[X] \) is a subring, we can also regard \( V \) as an \( F \)-module, i.e., a vector space over \( F \). The map \( A : V \to V \) given by \( A(v) = X \cdot v \) is a linear operator on \( V \). Conversely, given a vector space \( V \) and a linear operator \( A : V \to V \), we can define an \( R \)-module structure on \( V \) by setting \( X \cdot v = Av \). Thus \( F[X] \)-modules correspond to vector spaces \( V \) over \( F \) together with a linear operator \( A : V \to V \). This corresponds to a conjugacy class of matrices \([A]\), depending on the choice of basis.

If \( V \cong W \) as \( F[X] \)-modules with \( W \) given by \( B(w) = X \cdot w \), then there is a linear isomorphism \( C : V \to W \) with \( CA = BC \), so then \([A]\) and \([B]\) are similar matrices (for any choice of bases). Conversely, two similar matrices define isomorphism \( F[X] \)-modules.
Given two $F[x]$-modules $V$ and $W$ specified by linear operators $A$ and $B$, the direct sum $V \oplus W$ is given by the operator $A \oplus B$ with matrix \[
abla A \\ B \nabla.\]

Suppose that $V$ is a cyclic $F[x]$-module, so then $V \cong F[x]/fF[x]$ for some $f = a_0 + \cdots + a_{n-1}x^{n-1} + x^n \in F[x]$. 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 $0 \leq i < n-1$ and $x \cdot v_{n-1} = -a_0v_0 - \cdots - a_{n-1}v_{n-1}$. The matrix of the corresponding $A$ is the companion matrix for $f$,

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

The characteristic polynomial and minimal polynomial for $C(f)$ are both $f$.

**Definition 4.6.1** (Rational canonical form). Let $A : V \to V$ be a linear operator. Then $A$ is similar to a unique matrix of the form

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

where $f_1 | \cdots | f_r$ are the invariant factors of $V$ as an $F[x]$-module. This matrix is the rational canonical form for $A$.

**Proposition 4.6.2.** Two matrices are similar if and only if they have the same rational canonical form.

The generator matrix for $V$ as an $F[x]$-module is precisely $x \cdot I - A$, so finding invariant factors reduces to computing the Smith normal form of $x \cdot I - A$.

**Example 4.6.3.** 1. Let $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. Then reducing $x \cdot I - A$ gives

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

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

66
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 \( \text{IF}(A) = \{f\} \), 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 \( \text{IF}(A) = \{f, g\} \), then \( f | g \) 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 \( 3 \times 3 \) 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 \( \text{IF}(A) = \{x, x^2\} \), and the RCF is \[
\begin{pmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 1 & 0 \\
\end{pmatrix}.
\]

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

5. We classify (up to similarity) all \( 4 \times 4 \) 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 \( \text{IF}(A) \) are

\[
\{x - 2, x - 2, x - 2, x - 2\}, \quad \{x - 2, x - 2, (x - 2)^2\}, \quad \{(x - 2)^2, (x - 2)^2\}.
\]

There are three similarity classes.

**Proposition 4.6.4.** Let \( A : V \to V \) be a linear operator. Then the following are equivalent:

1. \( V \) is cyclic as an \( F[x] \)-module;
2. the matrix of \( A \) in some basis is \( C(f) \) for some (monic) \( f \in F[x] \);
3. \( \text{IF}(A) = \{P_A\} \);
4. \( m_A = P_A \);
4.6 Modules over $F[x]$

(5) the elementary divisors of $A$ are pairwise coprime.

Proof. (1) $\implies$ (3) If $V$ is cyclic, then $V \cong F[x]/fF[x]$ for some $f \in F[x]$, so $\text{IF}(A) = \{f\}$, in which case $f = P_A$.

(3) $\implies$ (2) If $\text{IF}(A) = \{f\}$, then $V \cong F[x]/fF[x]$, so $[A] = C(f)$ in some basis.

(2) $\implies$ (1) If $[A] = C(f)$ in some basis, then $V \cong F[x]/fF[x]$ is cyclic.

(3) $\iff$ (4) Since $P_A$ is the product of all invariant factors and $m_A$ is always an invariant factor, $P_A = m_A$ if and only if $\text{IF}(A) = \{P_A\}$.

(5) $\implies$ (1) Let $\text{ED}(A) = \{p_i^{\alpha_i}\}$. Then by the Chinese remainder theorem, if $f = \prod p_i^{\alpha_i}$, then $V \cong F[x]/fF[x]$ is cyclic.

(3) $\implies$ (5) The elementary divisors are the primary divisors of $\text{IF} = \{P_A\}$.

Let $A : V \to V$ be linear and let $p$ be an elementary divisor with $p$ monic irreducible and $k > 0$. Suppose $p = x - \lambda$ for some $\lambda \in F$. In $M = F[x]/p^kF[x]$, consider the basis $\{1, x - \lambda, \ldots, (x - \lambda)^{k-1}\}$. Then

$$A((x - \lambda)^i) = \frac{x}{x - \lambda} = (x - \lambda)^{i+1} + \lambda(x - \lambda)^i.$$ 

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

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

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

**Definition 4.6.5** (Splitting). A monic polynomial $f$ is split over $F$ if $f = (x - \lambda_1) \cdots (x - \lambda_n)$ for some $\lambda_1, \ldots, \lambda_n \in F$.

If $P_A$ is split, then the elementary divisors are of the form $(x - \lambda)^k$, and applying this construction, there is a basis of $V$ such that

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

for some Jordan blocks $J_1, \ldots, J_t$. These are unique up to permutation, and this form of $A$ is the Jordan form, denoted $J(A)$. If $A \sim B$, then $J(A) = J(B)$ (up to rearrangement of blocks).

**Proposition 4.6.6.** Let $A : V \to V$ be a linear operator. The following are equivalent:

1. there exists a basis such that $[A]$ is diagonal;
(2) there exists a basis consisting of eigenvectors of $A$;

(3) $V$ is a direct sum of eigenspaces of $A$;

(4) all elementary divisors of $A$ are linear;

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

(6) $m_A$ is a product of distinct linear polynomials.

Proof. Linear algebra.
5 FIELDS

5.1 FIELD EXTENSIONS

Proposition 5.1.1. Every field homomorphism is injective.

Proof. If \( f : F \to K \) is a field homomorphism, then \( \ker f \subset F \) is an ideal which does not contain 1, so \( \ker f = 0 \). □

Given a homomorphism of fields \( f : F \to K \), we can identify \( F \) with \( \text{im} f \subset K \).

Definition 5.1.2 (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 \( \text{Field}/F \). 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 5.1.3 (Degree). The degree of a field extension \( K/F \) is \( [K:F] = \dim_F K \).

Example 5.1.4.
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 5.1.5 (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 \( (x_iy_j) \) is a basis for \( L/F \). For linear independence, suppose that \( \sum_{i,j} a_{ij}x_iy_j = 0 \) 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 \( (x_iy_j) \) 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 \( z = \sum_{i,j} a_{ij}x_iy_j \). □

Corollary 5.1.6. 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 5.1.7. 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 5.1.8. Let \( K/F \) be a field extension and \( \alpha_1, \ldots, \alpha_n \in K \). Then
\[
F(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f, g \in F[x_1, \ldots, x_n] \text{ and } g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.
\]

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

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

Example 5.1.9. 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 5.1.10 (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 \( \alpha \) is transcendental over \( F \). We say that \( K/F \) is an algebraic extension if every \( \alpha \in K \) is algebraic over \( F \).

Example 5.1.11. 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 \( \alpha \) 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 5.1.12. 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 \( \{1, \alpha, \ldots, \alpha^{n-1}\} \) 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 \( \alpha \) is algebraic, \( I \neq 0 \), so \( I = m_\alpha \cdot F[x] \) for a unique monic polynomial \( m_\alpha \). If \( m_\alpha \mid fg \) for some \( f, g \in F[x] \), then \( f(\alpha) = 0 \) or \( g(\alpha) = 0 \), so \( m_\alpha \) divides one of them. This shows that \( m_\alpha \) 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 \( \ker h = m_\alpha \cdot F[x] \), so \( F[x]/m_\alpha \cdot F[x] \cong F[\alpha] \). Since \( m_\alpha \) 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 \( \{1, \alpha, \ldots, \alpha^{n-1}\} \) is a basis for \( F[\alpha] \), it is enough to show linear independence. Suppose \( a_0, \ldots, a_{n-1} \) satisfy

\[
\alpha^n = a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} = 0, \quad f = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}.
\]

Then \( m_\alpha \mid f \) but \( \deg f \leq \deg m_\alpha \), so \( f = 0 \).

\[ \square \]

**Definition 5.1.13** (Minimal polynomial). \( m_\alpha \) is the minimal polynomial of \( \alpha \).

**Remark 5.1.14.** The proof of the theorem shows that \( F(\alpha) \cong F[x]/m_\alpha \cdot F[x] \). If we are not given \( \alpha \) 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 5.1.15.**

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 \( \xi_p \) is a root of \( x^p - 1 = (x - 1)(x^{p-1} + \cdots + 1) \) and \( \xi_p \neq 1 \), so \( \xi_p \) 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 5.1.16.** Let \( K/F \) be a field extension of \( F \). Then \( \alpha \) is algebraic over \( F \) if and only if \( [F(\alpha) : F] < \infty \).

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

\( \implies \) Since \( n = [F(\alpha) : F] < \infty \), the elements \( 1, \alpha, \ldots, \alpha^n \) are linearly dependent, so there exist \( a_0, \ldots, a_n \) 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 \( \alpha \) is algebraic.

\[ \square \]

**Corollary 5.1.17.** 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 \( \alpha \) is algebraic.

\[ \square \]

**Corollary 5.1.18.** Let \( K/F \) be a field extension and \( \alpha_1, \ldots, \alpha_n \in K \) be algebraic over \( F \). Then \( [F(\alpha_1, \ldots, \alpha_n) : F] < \infty \).

73
5.2 Splitting fields

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

\[
[F(\alpha_1, \ldots, \alpha_n):F] = [E(\alpha_n):E][E:F] < \infty.
\]

**Theorem 5.1.19.** 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 5.1.20.** If \( K/F \) and \( L/K \) are algebraic, then \( L/F \) is algebraic.

**Proof.** Let \( \alpha \in L \). Since \( \alpha \) 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 \( \beta_i \) is algebraic over \( F \) for each \( i \), and \( \alpha \) is algebraic over \( E \) by construction, so \( E(\alpha)/E \) is finite. Hence \( E(\alpha)/F \) is finite, so \( \alpha \) is algebraic over \( F \). □

### 5.2 SPLITTING FIELDS

**Theorem 5.2.1.** 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 \( K = F[x]/g \cdot F[x] \).

**Corollary 5.2.2.** 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 5.2.3** (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) \( f \) splits into linear factors in \( K[x] \) as \( f = a(x - \alpha_1) \cdots (x - \alpha_n) \);

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

**Theorem 5.2.4.** 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 \( K = F(\alpha_1, \ldots, \alpha_n) \), where \( \alpha_1, \ldots, \alpha_n \) are the roots of \( f \) (with multiplicity). □

**Example 5.2.5.** Let \( f = x^2 - 3 \in \mathbb{Q}[x] \). Then \( \mathbb{Q}(\sqrt{3}) \) is a splitting field of \( f \).
**Definition 5.2.6** (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 \( \psi \) is an extension of \( \varphi \) if \( \psi(x) = \varphi(x) \) for all \( x \in F \).

If \( \psi \) is an extension of \( \text{id}_F \), so that \( \psi(x) = x \) for all \( x \in F \), then \( \psi \) is an \( F \)-homomorphism, i.e. a morphism in the category of field extensions of \( F \).

\[
\begin{array}{ccc}
K' & \xrightarrow{\psi} & K \\
\downarrow & & \downarrow \\
F' & \xrightarrow{\varphi} & F
\end{array}
\]

**Proposition 5.2.7.** 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 \( \varphi \), 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 \( \varphi \) with \( \psi(\alpha) = \beta \).

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

2. Define a map \( \sigma : F[x] \to K' \) by \( g \mapsto \varphi(g)(\beta) \). Then \( \sigma \) 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 \( \psi \) extends \( \varphi \).

Uniqueness is clear since \( K \) is generated by \( \alpha \), so any extension is determined by the image of \( \alpha \).

\[\square\]

**Corollary 5.2.8.** For \( K = F(\alpha) \), the number of extensions \( \psi : K \to K' \) of \( \varphi : F \to F' \) is at most \( [K : F] \).

**Theorem 5.2.9.** 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 \( \varphi \).

**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 \( \beta \) be a root of \( \varphi(m_\alpha) \). There is a unique extension \( \rho : F(\alpha) \to F'(\beta) \) of \( \varphi \) such that \( \rho(\alpha) = \beta \), and since \( \rho \)
is surjective, it is an isomorphism.

\[
\begin{array}{cccc}
K & \xrightarrow{\psi} & K' \\
| & & |
\downarrow{\rho} & \downarrow{\psi}
F(\alpha) & \longrightarrow & F'(\beta) \\
| & & |
\downarrow{\varphi} & \downarrow{\varphi}
F & \longrightarrow & F'
\end{array}
\]

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

Let \(\mathcal{P}\) be some property of field extensions, e.g. finite or algebraic. 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.

### 5.3 Finite fields

**Definition 5.3.1 (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 \(\text{char } R\), is \(n\).

**Proposition 5.3.2.** 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 \(\ker f = n\mathbb{Z}\). Then \(\mathbb{Z}/n\mathbb{Z} \cong \text{im } f \subset F\), 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 5.3.3 (Prime subfield).** Let \(F\) be a field. The **prime subfield** of \(F\) is the smallest subfield of \(F\).

**Proposition 5.3.4.**
1. If \(\text{char } F = 0\), then the prime subfield of \(F\) is isomorphic to \(\mathbb{Q}\).
2. If \(\text{char } F = p\) for \(p > 0\) prime, then the prime subfield of \(F\) is isomorphic to \(\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}\).

**Corollary 5.3.5.** If \(\text{char } F = 0\), then \(F\) is infinite.

**Definition 5.3.6 (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 5.3.7 (Formal derivative).** If \(f = a_n x^n + \cdots + a_1 x + a_0\), the **(formal) derivative** of \(f\) is

\[f' = na_n x^{n-1} + \cdots + a_1.\]
Proposition 5.3.8. If \( f, g \in F[x] \) and \( a \in F \), then \((f + g)' = f' + g'\), \((af)' = af'\), and \((fg)' = f'g + fg'\).

Proposition 5.3.9. 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 5.3.10. If \( \gcd(f, f') = 1 \), then \( f \) has no multiple roots.

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

Theorem 5.3.11. 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 \( f' = q x^{q-1} - 1 = -1 \), the roots \( \alpha_i \) 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 \( \alpha \) 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 5.3.12. 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 \( n A = \{ a \in A \mid a^n = 1 \} \subset A \).

Proposition 5.3.13. Let \( A \) be a finite abelian group such that \( |n A| \leq n \) for all \( n \). Then \( A \) is cyclic.

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

Corollary 5.3.14. If \( F \) is a field, then every finite subgroup of \( F^\times \) is cyclic.

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

Example 5.3.15. \( (\mathbb{F}_q)^\times \) is cyclic of order \( q - 1 \), in particular \((\mathbb{Z}/p)^\times \) is cyclic of order \( p - 1 \).

Definition 5.3.16 (Simple extension). A field extension \( K/F \) is simple if \( K = F(\alpha) \) for some \( \alpha \in K \).

Corollary 5.3.17. 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 5.3.18. 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 \( m_\alpha \) is irreducible of degree \( n \).

5.4 NORMAL EXTENSIONS

Lemma 5.4.1. 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 \( \varphi \).

\[
\begin{array}{ccc}
E & \xrightarrow{\psi} & M \\
\downarrow & & \\
\varphi \downarrow & & \\
F & \to & L
\end{array}
\]

Proof. Since \( E/F \) is finite, we can write \( E = F(\alpha_1, \ldots, \alpha_n) \) 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 \( \varphi \) such that \( \varphi_1(\alpha_1) = \varphi(\alpha_1) \). Since \( E = F_1(\alpha_2, \ldots, \alpha_n) \), by induction, there is a finite field extension \( M/L_1 \) and homomorphism \( \psi : E \to M \) extending \( \varphi_1 \). Then \( \psi \) extends \( \varphi \) and \( M/L \) is finite.

Proposition 5.4.2. 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 \( E = F(\alpha_1, \ldots, \alpha_n) \). For all \( i \),

\[
0 = (\sigma f)(\sigma(\alpha_i)) = f(\sigma(\alpha_i)),
\]

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

\[
\begin{array}{c}
M \\
\downarrow \psi \\
L \\
\downarrow \\
E \\
\downarrow \varphi \\
F(\alpha) \\
\downarrow \\
F \\
\end{array}
\]

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) \( \implies \) (1) Let \( E = F(\alpha_1, \ldots, \alpha_n) \) 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 \( \alpha_1, \ldots, \alpha_n \), in fact \( E \) is generated by all roots of \( f \), so \( E \) is the splitting field of \( f \).

**Definition 5.4.3** (Normal extension). A finite extension \( E/F \) is normal if any of these conditions hold.

**Corollary 5.4.4** (Test for normality). If \( E = F(\alpha_1, \ldots, \alpha_n) \), then \( E/F \) is normal if and only if \( m_{\alpha_i} \) splits in \( E[x] \) for all \( i \).

**Example 5.4.5.**

1. \( F/F \) is normal.
2. If \( [E : F] = 2 \), then \( E = F(\alpha) \) for any \( \alpha \in E \setminus F \). 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, \( \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \) is not normal for \( n \geq 3 \).
4. The extensions \( \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2}) \) and \( \mathbb{Q}(\sqrt[2]{2})/\mathbb{Q} \) are normal, as both are quadratic, but \( \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \) is not normal.
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 \( \mathbb{Q}(\sqrt[2]{2}, \omega)/\mathbb{Q}(\sqrt[2]{2}) \) is quadratic, hence normal, the extension \( \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \) is not normal.

**Proposition 5.4.6.** 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 \( f \in E[x] \). \( \square \)

**Definition 5.4.7** (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 \( E \subseteq L' \subseteq L \), if \( L'/F \) is normal, then \( L' = L \).

**Example 5.4.8.**

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 5.4.9. 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, $E = F(α_1, \ldots, α_n)$, and $f = m_{α_1} \cdots m_{α_n} \in F[x]$. 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 $E$. □

5.5 SEPARABLE EXTENSIONS

Lemma 5.5.1. 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) 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) Take $K$ to be the splitting field of $f$.

(3) 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 5.5.2 (Separable polynomial). A non-constant $f \in F[x]$ is separable over $F$ if $f$ satisfies any of these conditions.

Corollary 5.5.3. 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 5.5.4. If char $F = p > 0$ and $a \in F \setminus F^p$, 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 $α ∈ K$ is a root, so $α^p = a$. Then $(x - α)^p = x^p - α^p = x^p - a$.

Definition 5.5.5 (Perfect field). A field $F$ is perfect if either char $F = 0$ or char $F > 0$ and $F^p = F$.

Proposition 5.5.6. If $F$ is perfect and $f \in F[x]$ is irreducible, then $f$ is separable.

Proof. If char $F = 0$, then this is clear. Otherwise, let char $F = p > 0$ and suppose $f = \sum a_kx^k$ with $f' = 0$. For each non-zero term $a_kx^k$ in $f$, the corresponding term in $f'$ is $ka_kx^{k-1}$, so $p \mid k$. Then $f(x) = g(x^p)$ for $g = \sum b_ix^i$, where $b_i = a_{pi}$. If $b_i = c_i^p$ for some $c_i \in F$, then $f(x) = g(x^p) = (\sum cx^i)^p$, contradicting irreducibility of $f$. □

Example 5.5.7. 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 5.5.8** (Separable element). Let $E/F$ be an extension and $\alpha \in E$ be algebraic. We say that $\alpha$ is separable over $F$ if $m_\alpha$ is separable.

**Example 5.5.9.** If $F$ is perfect, then every algebraic $\alpha \in E$ is separable.

**Lemma 5.5.10.** Let $L/K/F$ be a tower of extensions and suppose $\alpha \in L$ is separable over $F$. Then $\alpha$ is separable over $K$.

**Proof.** If $m_\alpha \in K[x]$ is the minimal polynomial of $\alpha$ over $K$, then $m_\alpha$ divides the minimal polynomial of $\alpha$ over $F$, which is separable, so $m_\alpha$ is separable.

**Lemma 5.5.11.** Let $E/F$ be a finite extension and $\varphi : F \to L$ be a homomorphism. Then $\varphi$ has at most $[E : F]$ extensions $\psi : E \to L$.

**Proof.** Let $E = F(\alpha_1, \ldots, \alpha_n)$ and induct on $n$. If $n = 1$, so $E = F(\alpha_1)$, there is a bijection between the set of extensions of $\varphi$ and the set of roots of $m_{\alpha_1}$ 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 $\rho$, the number of extensions $\psi$ of $\rho$ is at most $[E : F(\alpha_1)][F(\alpha_1) : F] = [E : F]$.

**Definition 5.5.12** (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 5.5.13.** Let $E = F(\alpha)/F$ be a finite extension. Then $E/F$ is separable if and only if $\alpha$ 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 $\alpha$ is separable.

($\Longleftarrow$) Let $L$ be the splitting field of $m_\alpha$ over $F$. Since $m_\alpha$ 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 5.5.14.** 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 $\text{char } F = p$ 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.
5.5 Separable extensions

**Lemma 5.5.15.** Let $F$ be an infinite field, $L/F$ be a field extension, and $g \in L[x_1, \ldots, x_n]$ be non-zero. Then there exist $a_1, \ldots, a_n \in F$ such that $g(a_1, \ldots, a_n) \neq 0$.

**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 $g = g_0 + g_1x_1 + \cdots + g_mx_n^m$ for $g_i \in L[x_1, \ldots, x_{m-1}]$ with $g_m \neq 0$. By induction, there exist $a_1, \ldots, a_{n-1} \in F$ with $g_m(a_1, \ldots, a_{m-1}) \neq 0$. Then $g(a_1, \ldots, a_{n-1}, x_n)$ is non-zero in $L[x_n]$, so by the $n = 1$ case, there exists $a_n \in F$ with $g(a_1, \ldots, a_n) \neq 0$. \hfill \qed

**Remark 5.5.16.** 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 5.5.17.** Let $f_1, \ldots, f_m \in L[x_1, \ldots, x_n]$ be distinct. Then there exist $a_1, \ldots, a_n \in F$ such that the values $f_i(a_1, \ldots, a_n)$ are distinct for $i = 1, \ldots, m$.

**Proof.** Apply the lemma to $g = \prod_{i<j}(f_i - f_j)$. \hfill \qed

**Theorem 5.5.18.** Every (finite) separable field extension is simple.

**Proof.** Let $E/F$ be separable with $E = F(\alpha_1, \ldots, \alpha_n)$. 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 $f = \alpha_1x_1 + \cdots + \alpha_nx_n \in E[x_1, \ldots, x_n]$ and $f_i = \psi_i(f) \in L[x_1, \ldots, x_n]$. These are distinct, so if $F$ is infinite, then there exist $a_1, \ldots, a_n \in F$ such that the values $\beta_i = f_i(a_1, \ldots, a_n) \in L$ are distinct. Let $\beta = \alpha_1a_1 + \cdots + \alpha_na_n$. By construction, $\psi_i(\beta) = \beta_i$ for each $i$, and these values are distinct, so there are at least $m$ extensions $\psi_i\vert_{F(\beta)} : F(\beta) \to L$ of $\varphi$. 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. \hfill \qed

**Theorem 5.5.19.** 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.** ($\implies$) 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 $\varphi$. There are at most $[K : F]$ extensions $\rho : K \to L$ of $\varphi$, and for any such $\rho$, there are at most $[E : K]$ extensions $\psi : E \to L$ of $\rho$, hence at most $[E : K][K : F] = [E : F]$ extensions $\psi : E \to L$ of $\varphi$. Since we know there are exactly this many, we must have equality, so there are exactly $[K : F]$ extensions $\rho : K \to L$ of $\varphi$, hence $K/F$ is separable.

($\impliedby$) 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 $f_1 \cdots f_m$.

$$E = K(\alpha)$$

The number of extensions $E \rightarrow M$ of $\psi_i$ 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 $\varphi$, so $E/F$ is separable.

\[\square\]

**Corollary 5.5.20.** 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. $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i$ separable over $F$;
4. $E = F(\alpha)$ for some $\alpha$ 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 $\alpha$ is separable over $F$.

2. $\implies$ 3. Since $E/F$ is finite, $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i$, which must all be separable.

3. $\implies$ 1. Each of the extensions $F(\alpha_1, \ldots, \alpha_k)/F(\alpha_1, \ldots, \alpha_{k-1})$ is separable, since $\alpha_k$ is separable over $F$, hence also over $F(\alpha_1, \ldots, \alpha_{k-1})$. 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.

\[\square\]

**Corollary 5.5.21.** 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 $m_\alpha$ is irreducible, hence separable, so $\alpha$ is separable. Thus $E/F$ is separable.

\[\square\]
5.6 GALOIS EXTENSIONS

Throughout, let $E/F$ be a finite extension.

**Notation.** Let $\text{Aut}_F E$ denote the group of all $F$-automorphisms of $E$.

**Proposition 5.6.1.**
1. $|\text{Aut}_F E| \leq [E : F]$.
2. $|\text{Aut}_F E| = [E : F]$ if and only if $E/F$ is normal and separable.

**Proof.**
1. Every $\sigma \in \text{Aut}_F E$ is an extension of the embedding $F \hookrightarrow E$, and there are at most $[E : F]$ such extensions.

2. ($\Rightarrow$) If $\text{Aut}_F E = [E : F]$, then there are exactly $[E : F]$ extensions of $F$ into $E$, so $E/F$ is separable. For normality, it suffices to show that for any extension $M/E$ and $F$-homomorphism $\varphi : E \rightarrow M$, we have $\varphi(E) = E$. For $\sigma \in \text{Aut}_F E$, if $\rho : E \rightarrow M$ is the inclusion, then $\{\rho \circ \sigma | \sigma \in \text{Aut}_F(E)\}$ is the set of all extensions of $\text{id}_F$ (by counting).

Hence $\varphi \in \text{Aut}_F E$ and $\varphi = \rho \circ \sigma$, so $\varphi(E) = \rho(\sigma(E)) = \rho(E) = E$.

($\Leftarrow$) By separability, there exists $\varphi : F \rightarrow L$ that has $[E : F]$ extensions $\psi_1, \ldots, \psi_n : E \rightarrow L$. Since $E/F$ is normal, $\psi_i(E) = E$, so $\psi_i \in \text{Aut}_F E$, so $\text{Aut}_F E = [E : F]$.

\[\square\]

**Definition 5.6.2** (Galois extension). We say that $E/F$ is Galois if $|\text{Aut}_F(E)| = [E : F]$, or equivalently if $E/F$ is normal and separable. The $F$-automorphism group of a Galois extension is its Galois group, denoted $\text{Gal}(E/F)$.

**Remark 5.6.3.** The notation $\text{Gal}(E/F)$ and term “Galois group” is sometimes used even if the extension is not Galois.

**Example 5.6.4.**
1. $\mathbb{C}/\mathbb{R}$ is Galois with $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}_\mathbb{C}, z \mapsto \overline{z}\}$

2. If $\text{char } F \neq 2$ and $a \in F \setminus F^2$, 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 $\text{Gal}(E/F) = \{\text{id}_E, \sigma\}$ for some $\sigma$. Since $\sigma(f) = f$, we have that $\sigma(\alpha)$ is a root of $f$, so $\sigma(\alpha) = \pm \alpha$. If $\sigma(\alpha) = \alpha$, then $\sigma = \text{id}_E$, so the non-identity element is determined by $\sigma(\alpha) = -\alpha$. A general element of $E$ is of the form $a + b\alpha$, and $\sigma(a + b\alpha) = a - b\alpha$.

If $\text{char } F = 2$ 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 $\alpha$ is a root of $f$, then the roots of $f$ are $\alpha$ and $1 + \alpha$, so $E = F(\alpha)$. We have $\text{Gal}(E/F) = \{\text{id}_E, \sigma\}$ with $\sigma(\alpha) = 1 + \alpha$.

3. Let $p$ be prime, $k \geq 1$, and $q = p^k$. The splitting field of $f = x^q - x$ over $\mathbb{F}_q$ is $\mathbb{F}_{q^n}$. This is normal and separable, hence Galois, so $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a group of order $n$. It is in fact cyclic, generated by $\sigma(x) = x^q$. In the case $q = p$, this $\sigma$ is the Frobenius automorphism.

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, $m_\alpha$ is split over $E$, so $m_\alpha$ has exactly $n$ distinct roots. Let $X = \{\alpha_1 = \alpha, \ldots, \alpha_n\}$ be the roots of $m_\alpha$. Then $G = \text{Gal}(E/F)$ acts on $X$, so there is a homomorphism $\rho : G \rightarrow S_n$. This is injective, as if $\sigma(\alpha_i) = \alpha_i$ for all $i$, then $\sigma = \text{id}_E$ 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 $\alpha_i$ is trivial by this uniqueness, so the action is simply transitive.
Example 5.6.5. 5. Consider \( \mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q} \) and let \( \alpha = \sqrt{2} + \sqrt{3} \). The minimal polynomial of \( \alpha \) 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 \( \sigma(\alpha) = \sqrt{2} - \sqrt{3} \). Then \( \sigma(\sqrt{2}) = \sigma(\alpha^2 - 2) = -\sqrt{2} \), and

\[
\sigma^2(\alpha) = \sigma(\sqrt{2} - \sqrt{3}) = \sigma\left(\frac{\sqrt{2}}{\alpha}\right) = \frac{-\sqrt{2}}{\sqrt{2} - \sqrt{3}} = -\alpha,
\]

so \( \sigma \) has order 4, hence generates \( G \) as a cyclic group.

6. Let \( E = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q} \). Then \( \sqrt{3} \not\in \mathbb{Q}(\sqrt{2}) \) 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 \( G = \text{Gal}(E/\mathbb{Q}) \) 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 \( E = \mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q} \), a Galois extension of degree 6. Let \( \sigma \in G = \text{Gal}(E/\mathbb{Q}) \) be given by \( \sigma(\sqrt{2}) = \sqrt{2}\omega \) and \( \sigma(\omega) = \omega \), and let \( \tau \in G \) be complex conjugation. Then \( \sigma(\sqrt{2}) = \sqrt{2}\omega \) while \( \tau \sigma(\sqrt{2}) = \sqrt{2}\omega^2 \), so \( G \) is not commutative. Therefore, \( G \cong S_3 \).

Definition 5.6.6 (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 \( \text{Gal}(f) = \text{Gal}(E/F) \). If \( \deg f = n \), then \( \text{Gal}(f) \hookrightarrow S_n \) by acting on the roots. Since splitting fields are unique up to \( F \)-isomorphism, the Galois group of \( f \) is well-defined.

Example 5.6.7. If \( f \) splits in \( F[x] \), then \( \text{Gal}(f) \) is trivial.

Theorem 5.6.8 (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 \( \text{Gal}(E/F) = G \).

Proof. That \( F \) is a subfield of \( E \) is clear. We claim that if \( \alpha \in E \), then \( \alpha \) 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 \( \alpha \) is a root of \( f \), so \( \alpha \) 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 \( \alpha_1, \ldots, \alpha_n \in E \) be linearly independent over \( F \) with \( n > |G| \). Then \( [F(\alpha_1, \ldots, \alpha_n) : F] \geq n > |G| \). Each \( \alpha_i \) is separable over \( F \), so \( F(\alpha_1, \ldots, \alpha_n)/F \) is separable. Hence there exists \( \beta \in E \) with \( F(\alpha_1, \ldots, \alpha_n) = F(\beta) \). However, \( [F(\beta) : F] \leq |G| \), a contradiction.

Finally, note that \( G \subset \text{Aut}_F E \), so

\[
|G| \leq |\text{Aut}_F E| \leq [E : F] \leq |G|.
\]

This gives equality everywhere, so \( E/F \) is Galois and \( G = \text{Aut}_F E = \text{Gal}(E/F) \). \( \square \)
Example 5.6.9. 1. Let $K$ be a field and $E = K(x_1, \ldots, x_n)$. 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 $\text{Gal}(E/F) = S_n$. In fact, $F = K(\phi_1, \ldots, \phi_n)$, 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 $E = K(x_1, \ldots, x_n)$ and $F = E^G$, we have that $E/F$ is Galois and $\text{Gal}(E/F) = G$. Since $E/F$ is normal, it is the splitting field of some polynomial $f \in F[x]$, and $\text{Gal}(f) = G$.

3. Let $\mathbb{Q} = F$. The inverse Galois problem asks whether there is a Galois extension $E/\mathbb{Q}$ with $\text{Gal}(E/\mathbb{Q}) \cong G$ 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 $G = \text{Gal}(E/F)$. Given a field $L$ with $F \subset L \subset E$, we obtain a subgroup of $G$ given by $\{ \sigma \in G \mid \sigma(x) = x \text{ for all } x \in L \} = \text{Gal}(E/L)$. Conversely, given $H \subset G$, we obtain a subfield $L$ with $F \subset L \subset E$ by setting $L = E^H$.

Theorem 5.6.10. The two maps are inverses to each other. (In particular, they are bijections.)

Proof. Let $L$ be an intermediate subfield of $E/F$. If $H = \text{Gal}(E/L)$, then clearly $L \subset E^H$. Since $E/E^H$ is Galois with $\text{Gal}(E/E^H) = H$, 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 $H \rightarrow E^H \rightarrow \text{Gal}(E/E^H)$, which is $H$.

Proposition 5.6.11. Let $E/F$ be a Galois extension and $G = \text{Gal}(E/F)$.

1. $E^1 = E$ and $E^G = F$.

2. If $H_1 \leq H_2 \leq G$ are subgroups, then $E^{H_2} \subset E^{H_1}$.


4. If $\sigma \in G$ and $L = E^H$, then $E^{\sigma H \sigma^{-1}} = \sigma(L)$.

5. $H \leq G$ if and only if $L = E^H/F$ is normal. In this case, $L/F$ is Galois and $\text{Gal}(L/F) \cong G/H$.

Example 5.6.12. 1. Let $E = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, so $G = \text{Gal}(E/\mathbb{Q}) = \langle \sigma \rangle$ is cyclic of order 4.

\[
\begin{array}{ccc}
E & 1 \\
\mathbb{Q}(\sqrt{2}) & \langle \sigma^2 \rangle \\
\mathbb{Q} & G
\end{array}
\]
2. Let \( E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \), so \( G = \text{Gal}(E/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \).

3. Let \( E = \mathbb{Q}(\sqrt[3]{2}, \omega) \), so \( G = S_3 = \langle r, s \mid r^3, s^2, rsr \rangle \). Suppose \( s(\omega) = \omega^2 \) and \( s(\sqrt[3]{2}) = \sqrt[3]{2} \).

**Definition 5.6.13** (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 5.6.14.** If \( K = F(\alpha_1, \ldots, \alpha_n) \), then \( KL = L(\alpha_1, \ldots, \alpha_n) \).

**Theorem 5.6.15.** If \( K/F \) is Galois, then \( KL/L \) is Galois. The restriction homomorphism \( r : \text{Gal}(KL/L) \to \text{Gal}(K/F) \) is injective with image \( \text{Gal}(K/K \cap L) \).
Proof. Write \( K = F(\alpha_1, \ldots, \alpha_n) \). Since \( K/F \) is separable, each \( \alpha_i \) 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 \( f \in K[x] \). Then \( KL/L \) is a splitting field of \( f \in L[x] \). Hence \( KL/L \) is Galois.

Since \( K/F \) is normal, for any \( \sigma \in \text{Gal}(KL/L) \), the restriction of \( \sigma \) to a map \( K \to KL \) must have \( \sigma(K) = K \), so restriction gives \( \sigma \in \text{Gal}(K/F) \). To see that restriction is injective, suppose \( \sigma \in \text{Gal}(KL/L) \) acts as the identity on \( K \). In particular \( \sigma(\alpha_i) = \alpha_i \) for each \( \alpha_i \) above, so \( \sigma \) acts as the identity on \( L \). Finally, let \( \tau \in H = \text{im} \), so \( \tau \) is the restriction of \( \sigma \) for some \( \sigma \in \text{Gal}(KL/L) \). Then \( \sigma \) fixes \( L \), so \( \tau \) fixes \( K \cap L \), so \( \tau \in \text{Gal}(KL/L) \) and \( H \subset \text{Gal}(K/K \cap L) \). 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 \( \sigma \in \text{Gal}(KL/L) \), so \( x \in (KL)^{\text{Gal}(KL/L)} = L \). By the Galois correspondence, \( H \supset \text{Gal}(K/K \cap L) \).

**Definition 5.6.16** (Linearly disjoint extensions). We say that \( K \) and \( L \) are linearly disjoint over \( F \) if \( K \cap L = F \).

**Corollary 5.6.17.** If \( K \) and \( L \) are linearly disjoint over \( F \), then \( r : \text{Gal}(KL/L) \to \text{Gal}(K/F) \) is an isomorphism.

**Theorem 5.6.18.** If \( K/F \) and \( L/F \) are Galois, then \( KL/F \) is Galois and the restriction map \( r : \text{Gal}(KL/F) \to \text{Gal}(K/F) \times \text{Gal}(L/F) \) is injective. If \( K \) and \( L \) are linearly disjoint over \( F \), then \( r \) is an isomorphism.

Proof. to be written

In fact, \( \text{Gal}(K/F) \cong \text{Gal}(KL/L) \) and \( \text{Gal}(L/F) \cong \text{Gal}(KL/K) \), both of which are subgroups of \( \text{Gal}(KL/F) \), satisfy

\[
\text{Gal}(KL/F) = \text{Gal}(KL/L) \times \text{Gal}(KL/K)
\]

as an internal direct product.

### 5.7 CYCLOTOMIC EXTENSIONS

Let \( n > 0 \) and \( F \) be a field with \( \text{char} \ F \nmid n \). 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 \( \mu_n \) 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 \( \mu_n \) 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 \( G_n = \text{Gal}(F_n/F) = \text{Gal}(f_n) \) are of the form \( \sigma(\zeta_n) = \zeta_n^k \) for \( k \in \mathbb{Z}/n \). Since \( \zeta_n^k \) must be a primitive \( n \)-th root of unity in order for \( \sigma \) to be an automorphism, we must have \( \gcd(k, n) = 1 \). Thus we get a group homomorphism \( \chi_n : G_n \to (\mathbb{Z}/n)^\times \).

**Proposition 5.7.1.** \( \chi_n \) is injective.

Proof. If \( \sigma \in \ker \chi_n \), then \( \chi_n(\sigma) = 1 + n\mathbb{Z} \), so \( \sigma(\zeta_n) = \zeta_n^1 = \zeta_n \), hence \( \sigma = \text{id}_{F_n} \).

**Remark 5.7.2.** By the proposition, \( G_n \) may be identified with a subgroup of \( (\mathbb{Z}/n)^\times \), hence \( G_n \) is abelian. It turns out that depending on the choice of \( F \), one can obtain any subgroup of \( (\mathbb{Z}/n)^\times \).
Now let $F = \mathbb{Q}$, and let $\Phi_n \in \mathbb{Q}[x]$ be the minimal polynomial of $\zeta_n$, 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 $\pm 1$, so $\alpha = \pm 1$ as $\Phi_n$ is monic. Hence $\Phi_n \in \mathbb{Z}[x]$. 

**Lemma 5.7.3.** Let $p$ be a prime integer, $p \nmid n$. Then $(\zeta_n)^p$ is a root of $\Phi_n$.

**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 $(\Psi_n)^p = \Delta_n$ and $\Phi_n \mid \Delta_n$. If $g$ is an irreducible divisor of $\Phi_n$ in $\mathbb{F}_p[x]$, then $g \mid \Phi_n$. 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 5.7.4.** Every primitive $n$-th root of unity is a root of $\Phi_n$.

**Proof.** Every primitive $n$-th root of unity has the form $\zeta_n^k$ with $\gcd(k, n) = 1$. The result follows by induction and writing $k$ as a product of primes, none of which divide $n$. □

**Theorem 5.7.5.** $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

**Proof.** Since every primitive $n$-th root of unity is a root of $\Phi_n$,

$$\varphi(n) \leq \deg \Phi_n = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| \leq |(\mathbb{Z}/n)^\times| = \varphi(n).$$

Every $\zeta \in \mu_n$ has $\text{ord} \zeta = d$ 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 $\Phi_n$,

$$\Phi_1 = x - 1 \quad \Phi_4 = x^2 + 1$$
$$\Phi_2 = x + 1 \quad \Phi_5 = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_3 = x^2 + x + 1 \quad \Phi_6 = x^2 - x + 1$$

**Remark 5.7.6.** The first several cyclotomic polynomials have coefficients $0$ and $\pm 1$. 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 $a, k, m \geq 0$. 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) 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) \( \Rightarrow \) (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) \( \Rightarrow \) (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) \( \Rightarrow \) (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) \( \Rightarrow \) (1) Let \( K/F \) be finite, \( \alpha \in K \), and \( m_\alpha \) be the minimal polynomial of \( \alpha \) over \( F \). Then \( m_\alpha \) splits into linear factors and is irreducible, so \( m_\alpha = x - \alpha \), so \( \alpha \in F \). \( \square \)

**Definition 5.8.2** (Algebraically closed field). A field \( F \) satisfying these properties is said to be algebraically closed.

**Theorem 5.8.3.** \( \mathbb{C} \) 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 \( m_\alpha \) has irreducible over \( \mathbb{R} \) and has odd degree, so \( m_\alpha \) 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 \( m_\alpha \) 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.

\[
\begin{array}{c}
E \\
\mathbb{C} \\
\mathbb{R}
\end{array}
\]

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 \( N = \text{Gal}(E/\mathbb{C}) \). 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 \( E = \mathbb{C} \). \( \square \)

**Definition 5.8.4** (Algebraic closure). An extension \( F_{\text{alg}}/F \) is an algebraic closure of \( F \) if \( F_{\text{alg}} \) is algebraically closed and \( F_{\text{alg}}/F \) is algebraic.

**Theorem 5.8.5.** Every field \( F \) admits an algebraic closure \( F_{\text{alg}}/F \).
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 \( (\alpha_f) \), the right hand side is 0, a contradiction.

Let \( m \subset A \) be a maximal ideal containing \( I \). Then \( F_1 = A/m \) 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 \( F_{\text{alg}} = \bigcup F_n \). \( \square \)

5.9 GALOIS GROUPS OF POLYNOMIALS

Let \( f \in F[x] \) be a non-constant separable polynomial, \( E/F \) be a splitting field of \( f \), and \( G = \text{Gal}(f) = \text{Gal}(E/F) \). 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 5.9.1. Let \( E/F \) be Galois, \( G = \text{Gal}(E/F) \), 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 \( H = \text{Gal}(E/F(\alpha)) \). Then \( \deg m_\alpha = |F(\alpha)/F| = [G:H] \). Since \( G \) acts transitively on \( T \), we have \( |T| = [G:\text{stab}(\alpha)] = [G:H] \).

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 \( g = m_\alpha \). \( \square \)

Example 5.9.2. Let \( \alpha = \sqrt{2} + \sqrt[5]{3} \). Then \( \alpha \) lies in the extension \( E = \mathbb{Q}(\sqrt{2}, \sqrt[5]{3}, \omega)/\mathbb{Q} \), the splitting field of \((x^2 - 2)(x^3 - 5)\). Since \( E = \mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(\sqrt[5]{3}, \omega) \) as the compositum and these are linearly disjoint, so \( \text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/2 \times S_3 \). One can check that the orbit of \( \alpha \) has size 6, so \( \mathbb{Q}(\alpha)/\mathbb{Q} \) is of degree 6. By direct computation,

\[
m_\alpha = (x^3 + 6x - 5)^2 - 2(3x^2 + 2)^2.
\]

5.10 RADICAL EXTENSIONS

Let \( \text{char } F = 0 \) and \( n > 0 \). A finite extension \( E/F \) is \( n \)-radical if \( E = F(\alpha) \) and \( \alpha^n \in F \).

Example 5.10.1. 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 \( \text{Gal}(E/F) \) cyclic.

Proposition 5.10.2. Suppose \( \zeta_n \in F \), so \( F \) contains every \( n \)-th root of unity. Then every \( n \)-radical extension is cyclic.

Proof. Since \( \mu_n \subset F \) and \( E = F(\alpha) \) for some \( \alpha \) with \( \alpha^n = a \in F \), the roots of \( x^n - a \) are \( \zeta_n^n \alpha \in E \). Thus \( E/F \) is normal, hence Galois. Define \( f : G = \text{Gal}(E/F) \to \mu_n \) 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 \( \mu_n \), hence cyclic. \( \square \)
Let $E/F$ be Galois with $G = \text{Gal}(E/F)$. The vector space $\text{End}_F(E)$ is also a vector space over $E$. Every element of $G$ is an endomorphism of $E$ over $F$, so $G$ is a subset of $\text{End}_F(E)$.

**Lemma 5.10.3.** $G \subset \text{End}_F(E)$ is linearly independent over $E$.

**Proof.** Let $G = \{\sigma_1, \ldots, \sigma_n\}$ and suppose $\sum x_i \sigma_i = 0$ 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 $\sum x_i \sigma_i(yz) = (\sum x_i \sigma_i(y) \sigma_i)(z) = 0$ 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 5.10.4** (Hilbert 90). Let $E/F$ be cyclic of degree $n$. If $\zeta_n \in F$, then $E/F$ is $n$-radical.

**Proof.** Let $G = \text{Gal}(E/F)$ be generated by $\sigma$ 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 $E = \sigma(\alpha)$. 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 5.10.5** (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 5.10.6.**  
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 $\alpha_i^n \in F$, then $L/F$ is radical.

**Lemma 5.10.7.** 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 $\alpha_i^n \in E_{i-1} = F(\alpha_1, \ldots, \alpha_{i-1})$ 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 $K_{m-1}/F$. 

\[
\begin{minipage}{0.5\textwidth}
\begin{tikzpicture}
  \node (E) at (0,0) {$E_m$};
  \node (K_m) at (2,2) {$K_m$};
  \node (K_m-1) at (2,-2) {$K_{m-1}$};
  \node (E_m-1) at (0,-4) {$E_{m-1}$};
  \node (F) at (0,-6) {$F$};
  \draw[->] (E) -- (K_m);
  \draw[->] (K_m) -- (K_m-1);
  \draw[->] (E) -- (E_m-1);
  \draw[->] (E_m-1) -- (F);
\end{tikzpicture}
\end{minipage}
\]
Let $K_{m-1}$ be the splitting field of $g \in F[x]$ over $F$, so $K_{m-1}/F$ is Galois with $G = \text{Gal}(K_{m-1}/F)$. Let $L = E_{m-1}(\alpha)$ with $\alpha^n = a \in E_{m-1}$ for some $n$ and $a$. Let $h = \prod_\sigma(m_\sigma) \in F$. 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 Galois, so it remains to find an embedding of $E_m$ into $K_m$. Since $f = m_\sigma \mid h$ 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 $K_m$ is Galois, we have that $K_m$ is generated over $K_{m-1}$ by the roots of $h$. If $\beta$ is a root of $h$, then $h(\beta) = 0$, so $(\psi_f)(\beta) = 0$, hence $f(\psi^{-1}_f(\beta)) = 0$. Since $f \mid x^n - a$, we have $\psi^{-1}_f(\beta)^n = a$, 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 5.10.8.** Let $f \in F[x]$ be a non-constant polynomial. Then $f$ is solvable by radicals if and only if $\text{Gal}(f)$ is solvable.

**Proof.** ($\Rightarrow$) 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 $E \subseteq L$ be the splitting field of $f$, so $\text{Gal}(E/F) = \text{Gal}(f)$. 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 $F' = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L'$, and set $G_i = \text{Gal}(L_i/L_0)$ for $i = 0, 1, \ldots, m$. Since $\zeta_n \in F'$, each $L_i/L_{i-1}$ is Galois cyclic, so $G_i \leq G_{i-1}$ with $\text{Gal}(L_i/L_{i-1}) = G_{i-1}/G_i$ cyclic. Hence $\text{Gal}(L'/F')$ is solvable. The extension $F'/F$ is cyclotomic, hence abelian, so $L'/F$ is solvable. Then $E/F$ is solvable.

($\Leftarrow$) If $G = \text{Gal}(f) = \text{Gal}(E/F)$ 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 $\text{Gal}(E/F)$ is solvable, $\text{Gal}(E'/F') \hookrightarrow \text{Gal}(E/F)$ is solvable. Take a descending sequence of subgroups $\text{Gal}(E'/F') = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = 1$ 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 5.10.9.** Let $E = K(x_1, \ldots, x_n)$. Then $S_n$ acts on $E$, and if $F = E^{S_n}$, then $\text{Gal}(E/F) = S_n$. 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 5.10.10.** 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 $\text{Gal}(f) = S_p$.

**Proof.** Let $E \subseteq \mathbb{C}$ 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 $G = \text{Gal}(E/\mathbb{Q})$. 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 5.10.11.** The polynomial $x^5 - 4x + 2$ is not solvable by radicals over $\mathbb{Q}$.

**Lemma 5.10.12.** For every finite abelian group $G$, there exists $n$ such that there is a surjective homomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow G$. 

93
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 5.10.13.** For every finite abelian group $G$, there is an extension $E/\mathbb{Q}$ with Galois group $G$. 
