Contents

1 Groups

1.1 Definitions and basic properties

Definition 1.1.1 (Group)**.** A *group* is a set G together with a binary operation $(a, b) \mapsto a \cdot b = ab$ such that

(i) (Associativity) $(ab)c = a(bc)$ 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 $b = 1 \cdot b = (b'a)b = b'(ab) = b' \cdot 1 = b'$.

□

Remark 1.1.3. The associativity axiom allows us to define the product of any finitely many elements $a_1 a_2 \ldots a_n$. For example, $abcd = ((ab)c)d = (ab)(cd) = a(b(cd))$.

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. *For $n, m \in \mathbb{Z}$, $a^n a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.*

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

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.

Definition 1.1.9 (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}.
4. the multiple na of a instead of n-th power a^n.

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. $(R, +)$ 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 operation $[a]_n + [b]_n = [a + b]_n$ is well-defined and makes $\mathbb{Z}/n\mathbb{Z}$ an abelian group of order n. For convenience, we may denote this additive group by $\mathbb{Z}/n$.

Example 1.2.4 (Fields)**.** If K is a field, then the set $K^\times = K\backslash\{0\}$ 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)**.** The operation $[a]_n \cdot [b]_n = [ab]_n$ is well-defined on $\mathbb{Z}/n\mathbb{Z}$, but it does not define a group structure (unless $n = 1$). However, it does define a group structure on the subset $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \gcd(a, n) = 1\}$. This group is abelian of order $\varphi(n)$, where φ is the Euler totient function.

Example 1.2.6 (Multiplication tables)**.** Given a finite set G, 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.

V_4	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Example 1.2.7 (Symmetric groups)**.** 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 S_n is not abelian for $n \geq 3$.

Example 1.2.8 (Matrix groups)**.** Let F be a field. The set of invertible $n \times n$ matrices with entries in F, together with matrix multiplication, form a group $GL_n(F)$ called the *general linear group* of degree n over F. This is not commutative for $n \geq 2$.

1.3 Homomorphisms

Definition 1.3.1 (Group homomorphism)**.** 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. $1 \cdot f(1) = f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$, so $f(1) = 1$.
2. $f(a)f(a^{-1}) = f(aa^{-1}) = f(1) = 1$.
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 injective, $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$. □

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 $g \circ f$.*

Proof. We have $(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b)$. If f, g are isomorphisms, then the inverse of $g \circ f$ is $f^{-1} \circ g^{-1}$. □

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 $x + iy \leftrightarrow (x, y)$.
4. The map $x \mapsto e^x$ is a homomorphism $\mathbb{R} \to \mathbb{R}^\times$.

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 ± 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). □

We write C_n for a cyclic group of order n. Infinite cyclic group is denoted by C_∞.

1.5 Subgroups

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

Proposition 1.5.2. *Let G be a group and $H \subset G$ a subset. Then H is a subgroup of 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 $H \subset G$ a subset. Then H is a subgroup of 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 the following subgroups $\{1\} \subset G$ and $G \subset G$.
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, $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
4. As multiplicative groups, $\mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times$.
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 $S \subset G$ be any subset. The *subgroup generated by S* is the smallest subgroup $\langle S \rangle$ 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
$$\operatorname{Ker} f = f^{-1}(1) = \{a \in G \mid f(a) = 1\} \subset G.$$
2. The *image of f* is
$$\operatorname{Im} f = f(G) = \{f(a) \mid a \in G\} \subset H.$$

Proposition 1.5.6. $\operatorname{Ker} f \subset G$ *and* $\operatorname{Im} f \subset H$ *are subgroups.*

Proof. For $\operatorname{Ker} f \subset G$, since $f(1) = 1$, we have $1 \in \operatorname{Ker} f$. If $a, b \in \operatorname{Ker} f$, then
$$f(ab^{-1}) = f(a)f(b)^{-1} = 1 \cdot 1^{-1} = 1,$$
so $ab^{-1} \in \operatorname{Ker} f$. Thus $\operatorname{Ker} f \subset G$.
For $\operatorname{Im} f \subset H$, it is clear that $\operatorname{Im} f$ is non-empty. If $x, y \in \operatorname{Im} f$ with $f(a) = x$ and $f(b) = y$ for some $a, b \in G$, then
$$xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in \operatorname{Im} f,$$
so $\operatorname{Im} f \subset H$. $\square$

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

Proof. **($\Longrightarrow$)** If $f(g) = 1 = f(1)$, then $g = 1$.

($\Longleftarrow$) Suppose $\operatorname{Ker} f = 1$ and $f(a) = f(b)$ for $a, b \in G$. Then $f(ab^{-1}) = 1$, so $ab^{-1} = 1$. $\square$

Theorem 1.5.8. *Let $f : G \to H$ be an injective homomorphism. Then $G \cong \operatorname{Im} f \subset H$.*

Proof. The homomorphism $f : G \to \operatorname{Im} f$ is injective and surjective. $\square$

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

$$f_a \circ f_b = f_{ab} \qquad \text{and} \qquad f_1 = 1_G.$$

In particular, $f_a \circ f_{a^{-1}} = f_1 = 1_G$, 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 $H \subset G$ 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 $H \subset G$, 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 $H \subset G$. Then $|G| = [G : H] \cdot |H|$.*

Proof. Each coset $X \in G/H$ has cardinality $|H|$ and $G = \bigsqcup_{X \in G/H} X$. $\square$

Corollary 1.5.14. *Let G be a finite group.*

1. *If $H \subset G$ is a subgroup, then $|H|$ divides $|G|$.*
2. *If $a \in G$, then $\operatorname{ord} a$ divides $|G|$.*

Proof.

1. Clear.
2. Apply the first statement to $H = \langle a \rangle$. $\square$

1.6 Normal subgroups

Definition 1.6.1 (Normal subgroup)**.** A subgroup $H \subset G$ is *normal* if $aH = Ha$ for every $a \in G$. In this case we write $H \lhd G$.

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. *$H \subset G$ is normal if and only if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.*

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

($\Longleftarrow$) 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 $N \lhd G$ and $H \subset G$ is a subgroup with $N \subset H$, then $N \lhd H$.*

Proposition 1.6.6. *Let $f : G \to H$ be a homomorphism. Then* $\operatorname{Ker} f \lhd G$.

Proof. Let $k \in \operatorname{Ker} f$ 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 $gkg^{-1} \in \operatorname{Ker} f$. □

Example 1.6.7. Let F be a field and fix $n \geq 1$. Then $\det : GL_n(F) \to F^{\times}$ is a homomorphism, so its kernel is a normal subgroup of $GL_n(F)$. The kernel of det is the *special linear group*

$$SL_n(F) = \{A \in GL_n(F) \mid \det A = 1\}.$$

Let S and T be two subsets of a group G. We define the product ST as the subset of all elements in G of the form st for $s \in S$ and $t \in T$.

Proposition 1.6.8. *If $H \lhd G$, then the product of two cosets in G/H is a coset. Precisely, $(aH)(bH) = abH$. The product of cosets makes G/H a group.*

Proof. This follows from the calculation

$$(aH)(bH) = aHbH = abHH = abH.$$ □

Definition 1.6.9 (Quotient group)**.** If $H \lhd G$, 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 $\operatorname{Ker} \pi = H$ and $\operatorname{Im} \pi = G/H$. 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 $n\mathbb{Z} \subset \mathbb{Z}$ 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 $H \lhd G$. There is a natural bijection*

$$\{\textit{subgroups of } G \textit{ containing } H\} \longleftrightarrow \{\textit{subgroups of } G/H\}$$
$$K \longmapsto \pi(K)$$
$$\pi^{-1}(L) \to L.$$

Furthermore, normal subgroups of G containing H are paired with normal subgroups of G/H. □

1.7 Isomorphism theorems

Definition 1.7.1 (Factoring through)**.** Let $f : G \to H$ be a homomorphism and $N \lhd G$ 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 $f = \overline{f} \circ \pi$.

Theorem 1.7.2. *Let $f : G \to H$ be a homomorphism and $N \lhd G$. Then f factors uniquely through G/N if and only if $N \subset \operatorname{Ker} f$.*

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 $N \subset \operatorname{Ker} f$.

($\Longleftarrow$) Suppose $N \subset \operatorname{Ker} f$. For f to factor as $\overline{f} \circ \pi$, 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 $a^{-1}b \in N \subset \operatorname{Ker} f$, 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. $\square$

Theorem 1.7.3 (First isomorphism theorem)**.** *Let $f : G \to H$ be a group homomorphism. Then $G/\operatorname{Ker} f \cong \operatorname{Im} f$, with isomorphism $\overline{f}$ given by factoring f through $G/\operatorname{Ker} f$. Precisely, $\overline{f}(a \operatorname{Ker} f) = f(a)$.*

Proof. Let $\pi : G \to G/\operatorname{Ker} f$ be the canonical homomorphism, so $f = \overline{f} \circ \pi$. Then $\operatorname{Im} f = \operatorname{Im} \overline{f}$, so $\overline{f} : G/\operatorname{Ker} f \to \operatorname{Im} f$ is surjective. To see that it is injective, suppose $a \operatorname{Ker} f \in \operatorname{Ker} \overline{f}$. Then

$$1 = \overline{f}(a \operatorname{Ker} f) = (\overline{f} \circ \pi)(a) = f(a),$$

so $a \in \operatorname{Ker} f$ and $a \operatorname{Ker} f = \operatorname{Ker} f$ is the identity in $G/\operatorname{Ker} f$. $\square$

Corollary 1.7.4. *If $f : G \to H$ is a surjective homomorphism, then $G/\operatorname{Ker} f \cong H$.*

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 $\mathbb{Z}/\operatorname{Ker} f \cong G$. Since $\operatorname{Ker} f \subset \mathbb{Z}$, 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 $K \subset G$ be a subgroup and $N \lhd G$. Then*

1. *$KN \subset G$;*
2. *$N \lhd KN$;*

3. *$K \cap N \lhd K$;*
4. *$KN/N \cong K/(K \cap N)$.*

Proof. Here KN is non-empty, and

$$(KN)(KN)^{-1} = KNNK = KNK = KKN = KN,$$

hence KN is a subgroup in G containing N. Since $N \lhd G$ we have $N \lhd KN$.
Define a homomorphism $f : K \to KN/N$ by $k \mapsto kN$. It is surjective since $knN = kN \operatorname{Im}(f)$ and $\operatorname{Ker}(f) = K \cap N$. It follows that $K \cap N \lhd K$ and $K/K \cap N \cong KN/N$ by the first isomorphism theorem. □

Theorem 1.7.7 (Third isomorphism theorem)**.** *Let $K, H \lhd G$ with $K \subset H$. Then*

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

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

1.8 Group actions

Definition 1.8.1 (Group action)**.** Let G be a group and X be a set. An *action of G on X* is a map

$$\begin{aligned} \theta : G \times X &\longrightarrow X \\ (g, x) &\to gx \end{aligned}$$

such that

(i) $1x = x$ for all $x \in X$;

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

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 θ is an action of H on X. The *pullback of θ by f* is the action of G on X given by $gx = f(g)x$.

There is a bijection

$$\{\text{actions of } G \text{ on } X\} \longleftrightarrow \{\text{homomorphisms } G \to S(X)\}.$$

Indeed, a G-action on X yields a group homomorphism $f : G \to S(X)$ by $f(g)(x) = gx$. Conversely, a homomorphism f defines a G-action on X via $gx = f(g)(x)$.
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 1.8.4 (Kernel / faithful action)**.** Let θ be an action of G on X. The *kernel of* θ is the kernel of the induced homomorphism $G \to S(X)$. We say that θ is *faithful* if $\operatorname{Ker}\theta = 1$.

Definition 1.8.5 (Orbit / stabilizer)**.** Let G act on X and let $x \in X$.

1. The *orbit of* x, written $\operatorname{orb} x$ or Gx, is
$$\operatorname{orb} x = \{gx \mid g \in G\} \subset X.$$

2. The *stabilizer of* x, written $\operatorname{stab} x$ or G_x, is
$$\operatorname{stab} x = \{g \in G \mid gx = x\} \subset G.$$

Proposition 1.8.6. *$\operatorname{Ker}\theta = \bigcap_x \operatorname{stab} x$.*

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

Definition 1.8.7 (Transitive action)**.** An action of G on X is *transitive* if the only orbit is X.

Example 1.8.8 (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 $\operatorname{orb} x = \{x\}$ and $\operatorname{stab} x = G$.

Example 1.8.9 (Regular action)**.** The *regular action* of G on $X = G$ is the action given by $(g, x) \mapsto gx$. This is faithful and transitive, as $\operatorname{stab} x = 1$ and $\operatorname{orb} x = G$ for all $x \in G$. The induced homomorphism $G \to S(G)$ is the embedding from Example 1.5.10.

Example 1.8.10 (Left coset action)**.** If $H \subset G$, 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 $\operatorname{orb}(gH) = G/H$ and $\operatorname{stab}(gH) = gHg^{-1}$. 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 1.8.11 (Automorphism)**.** An *automorphism* of G is an isomorphism $G \to G$. The group of automorphisms of G is denoted $\operatorname{Aut} G$.

Example 1.8.12.

1. $\operatorname{Aut}\mathbb{Z} = \{(n \mapsto n), (n \mapsto -n)\}$.
2. $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Example 1.8.13. Any automorphism of G is also a permutation of G, so $\operatorname{Aut}(G) \subset S(G)$. Then $\operatorname{Aut} G$ acts on G as the pullback of the universal action by the inclusion $\operatorname{Aut}(G) \hookrightarrow S(G)$.

Example 1.8.14 (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 1.8.15 (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 1.8.16 (Inner automorphism)**.** An *inner automorphism* of G is an automorphism of the form $x \mapsto gxg^{-1}$ for some $g \in G$. The group of inner automorphisms is denoted $\operatorname{Inn} G$, and is a subgroup of $\operatorname{Aut} G$.

Proposition 1.8.17. $\operatorname{Inn} G \cong G/Z$.

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

Example 1.8.18 (Conjugation action on subgroups)**.** Let G act on the set X of all subgroups of G by conjugation, i.e. $(g, H) \mapsto gHg^{-1}$. 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 1.8.19. *Let G be a finite group and $H \subset G$ such that $[G : H]$ is the smallest prime divisor of $|G|$. Then $H \lhd G$.*

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 $N = \operatorname{Ker} f \lhd G$. Then $N \subset H$ 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 $H = N \lhd G$. $\square$

Theorem 1.8.20 (Orbit-stabilizer)**.** *Let G be a group acting on a set X and let $x \in X$. Then $|\operatorname{orb} x| = [G : \operatorname{stab} x]$. In particular, if G is finite, then $|\operatorname{orb} x| = |G|/|\operatorname{stab} x|$.*

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

Example 1.8.21. If the group G is finite and $H \subset G$, then the number of subgroups conjugate to H is $|G|/|N_G(H)|$.

Definition 1.8.22 (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 $gx = x$ 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 1.8.23. *If $H = \langle S \rangle \subset G$, then $X^S = X^H$.*

Lemma 1.8.24 (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 $1/|\operatorname{orb} x|$, so we get by orbit-stabilizer

$$\begin{aligned}\sum_{x \in X} \frac{1}{|\operatorname{orb} x|} &= \sum_{x \in X} \frac{|\operatorname{stab} x|}{|G|} = \frac{1}{|G|} \sum_{x \in X} |\operatorname{stab} x| = \frac{1}{|G|} |\{(g, x) \in G \times X \mid gx = x\}| \\ &= \frac{1}{|G|} \sum_{g \in G} |\{x \in X \mid gx = x\}| = \frac{1}{|G|} \sum_{g \in G} |X^g|.\end{aligned}$$ $\square$

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 $H \subset G$, 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 $X^H = \{x_1, \dots, x_k\}$, then $\mathrm{orb}(x_i) = \{x_i\}$ 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 $X = \{(x_1, \dots, x_p) \in G^p \mid x_1 \cdots x_p = 1\}$. Then $|X| = |G|^{p-1}$, which is divisible by p. Consider the action of a cyclic group H of order p with a generator σ on X defined by $\sigma(x_1, \dots, x_p) = (x_p, x_1, \dots, x_{p-1})$. 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 $(x, \dots, x)$ with $x^p = 1$. Note that $(1, \dots, 1) \in X^H$, so $|X^H| \geq 1$ and is divisible by $p \geq 2$. Thus there exists $(x, \dots, x) \in X^H$ 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 $Z(G) \neq 1$.*

Proof. Let G act on $X = G$ by conjugation, so $X^G = Z(G)$. By Lemma 1.9.2, $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$, so $Z(G)$ 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 $n > 0$ and $p \nmid m$. A *Sylow p-subgroup* $H \subset G$ 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 $H \subset G$ 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 $H \triangleleft N$;*

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 $H \triangleleft N_G(H)$, we also have $H \triangleleft N$.

2. Apply the first statement repeatedly. □

Theorem 1.9.8 (Second Sylow theorem)**.** *Suppose $p \mid |G|$.*

1. *If $H \subset G$ is a p-subgroup and $P \subset G$ is a Sylow p-subgroup, then $gHg^{-1} \subset P$ 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 $|X^H| \equiv |X| = m \not\equiv 0 \pmod{p}$, so $|X^H| \geq 1$. Let $gP \in X^H$. Then $hgP = gP$ for all $h \in H$, so $g^{-1}Hg \subset P$.

2. Immediate from the first statement. □

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

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

Theorem 1.9.10 (Third Sylow theorem)**.** *Suppose $|G| = p^n m$ with $n > 0$ and $p \nmid m$. Then $n_p \mid m$ and $n_p \equiv 1 \pmod{p}$.*

Proof. By the second Sylow theorem, G acts transitively on $X = \mathrm{Syl}_p(G)$ by conjugation. Let $P \in X$ be some Sylow p-subgroup. Then $\operatorname{orb} P = X$ and $\operatorname{stab} P = N_G(P)$, 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, $|X^P| \equiv |X| = n_p \pmod{p}$ by Lemma 1.9.2. If $Q \in X^P$, then $gQg^{-1} = Q$ for all $g \in P$. Thus $P, Q \subset N_G(Q)$ are Sylow p-subgroups. Since $Q \triangleleft N_G(Q)$, this means that $Q = P$. Thus $X^P = \{P\}$ and $n_p \equiv 1 \pmod{p}$. □

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 $G_1, \ldots, G_n$.

Example 1.10.2. 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 1.10.3 (Internal direct product)**.** Let $H_1, \ldots, H_n \subset G$. We say that G is the *internal direct product* of $H_1, \ldots, H_n$ if the multiplication map

$$
\begin{aligned}
f : H_1 \times \cdots \times H_n &\longrightarrow G \\
(h_1, \ldots, h_n) &\longmapsto h_1 \cdots h_n
\end{aligned}
$$

is a group isomorphism.

Proposition 1.10.4. *If G is the internal direct product of $H_1, \ldots, H_n$, then $G \cong H_1 \times \cdots \times H_n$.*

Theorem 1.10.5 (Direct product theorem)**.** *Let G be a group and $H_1, \ldots, H_n \subset G$ be subgroups. Then G is the internal direct product of $H_1, \ldots, H_n$ if and only if*

1. *$H_i \triangleleft G$;*

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. ($\Longrightarrow$) 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.

($\Longleftarrow$) 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. □

Corollary 1.10.6. 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 1.10.7 (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

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

Theorem 1.10.8. *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* $H_i \subset G$ *be a Sylow* p_i*-subgroup. If* $H_i \triangleleft G$ *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 $H_1 \cdots H_{n-1}$ 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. □

Proposition 1.10.9. *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 $q \neq 1 \pmod{p}$). 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. □

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 $[g, h] = ghg^{-1}h^{-1}$.

If $H, K \subset G$, 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. $g[h, k]g^{-1} = [ghg^{-1}, gkg^{-1}]$;

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 $H, K \lhd G$, then $[H, K] \lhd G$.*

2. If $H \subset G$, then $[G, H] \lhd G$.

3. If $H, K \subset G$ and $[H, K] \subset H$, then $K \subset N_G(H)$.

Proof. 2) Let $x, g \in G$ and $h \in H$. Then

$$x[g, h]x^{-1} = xghg^{-1}h^{-1}x^{-1} = xghg^{-1}x^{-1}h^{-1}hxh^{-1}x^{-1} = [xg, h] \cdot [x, h]^{-1}$$ □

Definition 1.11.5 (Central series / lower central series)**.** A *central series* is a series of subgroups

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$$

such that $G_i \lhd G$ and $[G, G_i] \subset G_{i+1}$ 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

$$G = G_0 \rhd G_1 \rhd \cdots$$

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 nipotent.

2. Products of finitely many nilpotent groups are nilpotent.

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

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

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

Proof. Take a central series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$. There exists j such that $G_j \not\subset H$ but $G_{j+1} \subset H$. Then $[H, G_j] \subset [G, G_j] \subset G_{j+1} \subset H$, so $G_j \subset N_G(H)$, 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. ($\Longleftarrow$) Products of nilpotent groups, in particular p-groups, are nilpotent.

($\Longrightarrow$) By Theorem 1.10.8, it suffices to show that every Sylow p-subgroup $P \subset G$ 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 $P \lhd G$. $\square$

Proposition 1.11.13. *Let $N \lhd G$. Then G/N is abelian if and only if $[G, G] \subset N$.*

Proof. ($\Longrightarrow$) 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 $[G, G]$.

($\Longleftarrow$) If $[G, G] \subset N$, 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

$$G = G^{(0)} \rhd G^{(1)} \rhd \cdots$$

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

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$$

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 $N \lhd G$ 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 $\{1, 2, \ldots, n\}$. Elements of S_n are called *permutations*

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 σ. (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

$$\mathrm{id}, \qquad (1,2), \qquad (1,3), \qquad (2,3), \qquad (1,2,3), \qquad (1,3,2).$$

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.*

Proof. Let H be the cyclic subgroup generated by σ. The natural action of S_n on the set $X = \{1, \ldots, n\}$ restricts to an action of H on X. Let $X_1, \ldots, X_m$ be all H orbits in X. Then σ permutes cyclically the elements of every orbit X_i. Therefore, σ is the product of disjoint cycles $\sigma_1 \cdots \sigma_m$. □

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 σ 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, $(12)(34) = (12)(34)(5) \in S_5$ has cycle type $(2,2,1)$ or simply $(2,2)$.

Let $\sigma = (a_1, a_2, \ldots, a_k) \in S_n$ be a k-cycle and $\tau \in S_n$. Then $\tau\sigma\tau^{-1} = (b_1, b_2, \ldots, b_k)$ is a k-cycle, where $b_i = \tau(a_i)$ for all i.

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

Proof. If $\sigma = \sigma_1 \cdots \sigma_m$ is the product of disjoint cycles, where σ_i is a k_i-cycle, then $\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdots (\tau\sigma_m\tau^{-1})$ is the product of disjoint k_i-cycles $\tau\sigma_i\tau^{-1}$, i.e., σ and $\tau\sigma\tau^{-1}$ have the same cycle type.

Conversely, it is sufficient to prove that the two k-cycles $\sigma = (a_1, a_2, \ldots, a_k)$ and $\sigma' = (b_1, b_2, \ldots, b_k)$ are conjugate in S_k. If $\tau \in S_k$ is such that $\tau(a_i) = b_i$ for all i, then $\sigma' = \tau\sigma\tau^{-1}$. □

Example 1.12.6. 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 1.12.7. *Every element in S_n is a product of transpositions.*

Definition 1.12.8 (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 1.12.9 (Sign homomorphism / alternating group)**.** The *sign homomorphism* of S_n is $\operatorname{sgn} = \det \circ \pi : S_n \to \{\pm 1\}$. The *alternating group* is $A_n = \operatorname{Ker} \operatorname{sgn} \triangleleft S_n$. We say that σ from S_n is *even* if $\sigma \in A_n$ and *odd* otherwise.

If $n > 1$, we have $|A_n| = n!/2$, so there are $n!/2$ even and $n!/2$ odd permutations.

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

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

$$\begin{aligned} (a,b)(a,b) &= \mathrm{id}, \\ (a,b)(b,c) &= (a,b,c), \\ (a,b)(c,d) &= (a,b,c)(b,c,d). \end{aligned}$$

□

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 σ. Then $\rho' = \rho(d,e) \in A_n$, and

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

□

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 $N \triangleleft A_n$ be non-trivial. It suffices to show that N contains a 3-cycle. Pick some $\sigma \in N$. If σ is not a 3-cycle, then since (single) transpositions are not in A_n, σ moves at least four indices.

Suppose σ 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 τ 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 τ which is a product of transpositions. Then $\sigma\sigma = (132) \in N$.

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

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

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

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 $n \leq 4$.*

Proof. $\{1, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of S_4. $\square$

1.13 Semidirect products

Definition 1.13.1 (Semidirect product)**.** Let N and K be groups and $f : K \to \operatorname{Aut} N$ 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

$$(r_1, s_1)(r_2, s_2) = \begin{cases} (r_1 r_2, s_1 s_2), & \text{if } s_1 = e; \\ (r_1 r_2^{-1}, s_1 s_2), & \text{otherwise.} \end{cases}$$

   This is the *dihedral group*, denoted D_{2n}. The semidirect product $C_\infty \rtimes_f C_2$ is denoted D_∞. It has order $2n$.
3. If $p < q$ are primes and $q \equiv 1 \pmod p$, then there is a non-trivial $f : C_p \to \operatorname{Aut} C_q$. Then $C_q \rtimes_f C_p$ is a non-abelian group of order pq.

Proposition 1.13.3. *$N \lhd (N \rtimes_f K)$.*

Definition 1.13.4 (Internal semidirect product)**.** Let $N \lhd G$ and $K \subset G$ be subgroups. 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 $f : K \to \operatorname{Aut} N$.*

Proposition 1.13.7. *If H is a group, then $\operatorname{Aut} H \subset \operatorname{Inn} G$ for some group G containing H.*

Proof. We can take $G = H \rtimes_f \operatorname{Aut}_H$ with $f : \operatorname{Aut} H \to \operatorname{Aut} H$ the identity. $\square$

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 $G \cong C_p$.*

Let p be a prime integer. A finite group G is called *elementary abelian p-group* if G is an abelian p-group such that $a^p = 1$ for all $a \in G$. Such G can be viewed as a vector space over the field $\mathbb{Z}/p\mathbb{Z}$, hence it has a basis. It follows that $G \simeq C_p \times C_p \times \cdots \times C_p$.

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, i.e., G is an elementary abelian p-group. It follows that $G \cong C_p \times C_p$. $\square$

Proposition 1.14.4. *If $n = pq$ and $q \not\equiv 1 \pmod{p}$, then $G \cong C_{pq}$.*

Proof. This is Proposition 1.10.9. $\square$

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 1.10.9.

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 $f : P \to \operatorname{Aut} Q$. $\square$

Corollary 1.14.6. *If p is an odd prime and $|G| = 2p$, then $G \cong C_{2p}$ or $G \cong D_{2p}$.*

Proof. By Proposition 1.14.5, either $G \cong C_{2p}$ or $G \cong C_p \rtimes_f C_2$ for some non-trivial $f : C_2 \to \operatorname{Aut} C_p$. 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_{2p}. $\square$

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, $D_6 \cong S_3$
7. C_7
9. C_9, $C_3 \times C_3$
10. C_{10}, D_{10}
11. C_{11}
13. C_{13}
14. C_{14}, D_{14}
15. 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_8, and*

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

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 $H = \langle h \rangle \lhd G$ and pick $k \in G \backslash H$.

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 $f : K \to \operatorname{Aut} H$. There are two possibilities for f, which correspond to $C_4 \times C_2$ if f is trivial and D_8 if f sends k to the inversion automorphism.

If no $k \in G\backslash H$ has order 2, so then every $k \in G\backslash H$ has order 4, we have $k^2 = h^2$ for all $k \in G\backslash H$ 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. □

Proposition 1.14.8. *The groups of order 12 are C_{12}, $C_6 \times C_2$, D_{12}, A_4, and $C_3 \rtimes_f C_4$ for*

$$C_3 = \{1, a, a^2\}; \qquad C_4 = \{1, b, b^2, b^3\}; \qquad f(b)(a) = a^{-1}.$$

Proof. Let $P \subset G$ 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 $f : P \to \operatorname{Aut} Q$.

If $Q \cong C_4$, then we seek homomorphisms $f : C_3 \to \operatorname{Aut} C_4$. There are two elements of $\operatorname{Aut} C_4$, 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 $\operatorname{Aut} Q \cong S_3$, which has three elements σ satisfying $\sigma^3 = 1$. Thus we have three possible choices of $f : P \to \operatorname{Aut} Q$. 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 $g : Q \to \operatorname{Aut} P$.

If $Q \cong C_4$, then $\operatorname{Aut} P$ 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 $g : Q \to \operatorname{Aut} P$, 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_{12}. □

Remark 1.14.9. There are 14 isomorphism classes of groups of order 16. There are 2,328 isomorphism classes of groups of order $2^7 = 128$. There are 49,487,367,289 isomorphism classes of groups of order $2^{10} = 1024$.

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 $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$ for all $i = 1, \ldots, n-1$.

Proposition 1.15.2. *1. $f : G \to H$ is injective if and only if $1 \to G \xrightarrow{f} H$ is exact.*

2. $f : G \to H$ is surjective if and only if $G \xrightarrow{f} H \to 1$ is exact.

Definition 1.15.3 (Short exact sequence)**.** A *short exact sequence* is an exact sequence

$$1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} F \longrightarrow 1,$$

i.e. α is injective, β is surjective, and $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. Then H identifies with $\operatorname{Im}\alpha \triangleleft G$ and $F \cong G/H$.

Proposition 1.15.4. *If $H \triangleleft G$, then the sequence*

$$1 \longrightarrow H \xhookrightarrow{i} G \xrightarrow{\pi} G/H \longrightarrow 1$$

is exact.

Definition 1.15.5 (Split exact sequence)**.** A short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "\alpha"] & G \arrow[r, shift left, "\beta"] & F \arrow[l, shift left, dashed, "\gamma"] \arrow[r] & 1 \end{tikzcd}$$

is *split* (or *right split*) if there exists a homomorphism $\gamma : F \to G$ such that $\beta \circ \gamma = \mathrm{id}_F$.

Theorem 1.15.6. *The short exact sequence*

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "\alpha"] & G \arrow[r, shift left, "\beta"] & F \arrow[l, shift left, dashed, "\gamma"] \arrow[r] & 1 \\ & & K \arrow[u, hook, "i"] \arrow[ur, "\beta_K"'] & & \end{tikzcd}$$

is split if and only if there is a subgroup $K \subset G$ such that $\beta|_K : K \to F$ is an isomorphism. In this case, $G \cong H \rtimes_\varphi F$ with $\varphi : F \to \operatorname{Aut} H$ given by $\varphi(f)(h) = ghg^{-1}$, where $g = \gamma(f)$.

Proof. ($\Longrightarrow$) Let $K = \operatorname{Im}\gamma$. 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 $k \in \operatorname{Ker}\beta|_K$, then $k = \gamma(f)$ for some $f \in F$ since $K = \operatorname{Im}\gamma$, and then $f = \beta(\gamma(f)) = \beta(k) = 1$. This means $k = \gamma(1) = 1$, so $\operatorname{Ker}\beta|_K$ must be trivial.

($\Longleftarrow$) 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 $H = \operatorname{Ker}\beta \triangleleft G$, 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 $\varphi : F \to \operatorname{Aut} H$. To determine φ, 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. $\square$

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

$$1 \longrightarrow H \hookrightarrow G \twoheadrightarrow G/H \longrightarrow 1.$$

If there is an element of order 2 in $G \backslash H$, then the sequence splits and we obtain $G \cong D_8$ 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 $X \cup \overline{X}$.

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

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

If $\mathbf{w}$ is a word on X, then $\mathbf{w}$ is *irreducible* if there is no word $\mathbf{u}$ on X which is a truncation of $\mathbf{w}$.

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

$$\mathbf{u} = \mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_n = \mathbf{v}$$

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

Proposition 1.16.3. *If* $\mathbf{u}_1 \sim \mathbf{v}_1$ *and* $\mathbf{u}_2 \sim \mathbf{v}_2$*, then* $\mathbf{u}_1\mathbf{u}_2 \sim \mathbf{v}_1\mathbf{v}_2$*.*

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

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

For uniqueness, let $\mathbf{u}$ and $\mathbf{v}$ be irreducible words in the same equivalence class, and write down a sequence $\mathbf{u} = \mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_n = \mathbf{v}$ as above. To show that $\mathbf{u} = \mathbf{v}$, we induct on n and then the total length of the words $\mathbf{w}_0, \ldots, \mathbf{w}_n$. When $n = 0$, we have $\mathbf{u} = \mathbf{w}_0 = \mathbf{v}$. Now consider $n \geq 1$ and look at a longest word $\mathbf{w}_k$ in the sequence. Then $\mathbf{w}_{k-1}$ and $\mathbf{w}_{k+1}$ are necessarily truncations of $\mathbf{w}_k$.

If the truncations are

$$\mathbf{st}b\bar{b}\mathbf{u} \leftarrow \mathbf{s}a\bar{a}\mathbf{t}b\bar{b}\mathbf{u} \rightarrow \mathbf{s}a\bar{a}\mathbf{tu},$$

then we replace $\mathbf{w}_k$ with $\mathbf{stu}$ and have truncations $\mathbf{w}_{k-1} \to \mathbf{w}_k$ and $\mathbf{w}_{k+1} \to \mathbf{w}_k$ 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

$$\mathbf{s}a\mathbf{t} \leftarrow \mathbf{s}a\bar{a}a\mathbf{t} \to \mathbf{s}a\mathbf{t} \qquad \text{or} \qquad \mathbf{st} \leftarrow \mathbf{a}a\bar{a}\mathbf{t} \to \mathbf{st},$$

then we can reduce the number of words n in the sequence by omitting $\mathbf{w}_k$ and $\mathbf{w}_{k+1}$.

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 $\mathrm{Free}(X)$, is the set of all equivalence classes of words on X with the concatenation operation.

Example 1.16.6.

1. If $X = \emptyset$, then $\mathrm{Free}(X) = 1$.
2. If $X = \{a\}$, then $\mathrm{Free}(X) \cong \mathbb{Z}$ 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 $\mathrm{Free}(X)$ is non-abelian.

Notation. In $\mathrm{Free}(X)$, we write a^{-1} for $\bar{a}$ when $a \in X$.

For convenience, we will write $\mathbf{w}$ for $[\mathbf{w}]$ 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 $\overline{f} : \mathrm{Free}(X) \to G$ such that $\overline{f}(x) = f(x)$ for all $x \in X$.*

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

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

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 $\mathrm{Free}(X)$. For this, note that $\overline{f}$ is unchanged by truncations, hence whenever two words are equivalent. □

Corollary 1.16.8. *Let $X \subset G$ generate G. Then $G \cong \mathrm{Free}(X)/N$ for some $N \lhd \mathrm{Free}(X)$.*

Proof. The inclusion function $i : X \hookrightarrow G$ extends to a homomorphism $f : \mathrm{Free}(X) \to G$. That X generates G means that f is surjective, so $\mathrm{Free}(X)/\operatorname{Ker} f \cong G$. □

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 $R \subset \mathrm{Free}(X)$ such that $\langle\langle R \rangle\rangle = \mathrm{Ker}(\mathrm{Free}(X) \to G)$. Then we write

$$G \cong \langle X \mid R \rangle = \mathrm{Free}(X)/\langle\langle R \rangle\rangle.$$

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. $\langle \sigma, \tau \mid \sigma^n, \tau^2, \tau\sigma\tau\sigma \rangle \cong D_{2n}$

Let G and H be two groups. Fix presentations $G = \langle X \mid R \rangle$ and $H = \langle Y \mid S \rangle$ and set

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

Theorem 1.16.11 (Universal property of free products)**.** *Let $i, j : G, H \to G * H$ be the natural maps and let $g, h : G, H \to K$ be homomorphisms to some group K. Then there is a unique homomorphism $k : G * H \to K$ such that the following diagram commutes.*

$$\begin{tikzcd} & G \arrow[d, "i"'] \arrow[ddr, bend left, "g"] & \\ H \arrow[r, "j"] \arrow[drr, bend right, "h"'] & G * H \arrow[dr, dashed, "k"] & \\ & & K \end{tikzcd}$$

It follows that $G * H$ does not depend on the presentations. This group is called *free product (coproduct)* of G and H.

Example 1.16.12.

1. $G * 1 \cong G$ and $1 * H \cong H$.
2. $C_2 * C_2 \simeq D_\infty$.

The universal property of free products is closely related to the following result for direct products.

Theorem 1.16.13 (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.*

$$\begin{tikzcd} & G & \\ H & G \times H \arrow[u, "\pi_G"] \arrow[l, "\pi_H"'] & \\ & & K \arrow[uul, bend right, "g"'] \arrow[ull, bend left, "h"] \arrow[ul, dashed, "k"'] \end{tikzcd}$$

2 Categories and Functors

2.1 Definitions and basic properties

Definition 2.1.1 (Category). A *category* $\mathcal{C}$ consists of a collection (more formally a class) $\operatorname{Ob}\mathcal{C}$ of *objects*, a collection $\operatorname{Mor}\mathcal{C}$ of *morphisms* (*arrows*) between objects. Every morphism f has the *source* object $X = s(f)$ and the *target* object $Y = t(f)$. We write $f : X \to Y$. Moreover, there is a composition operation, which forms from morphisms $f : X \to Y$ and $g : Y \to Z$ 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 $X \in \operatorname{Ob}\mathcal{C}$, there is a (unique) identity morphism $1_X : X \to X$ such that for any morphisms $f : X \to Y$ and $g : W \to X$, we have

$$f = f \circ 1_X, \qquad g = 1_X \circ g.$$

The collection of morphisms $X \to Y$ is denoted $\operatorname{Mor}_{\mathcal{C}}(X, Y)$ or simply $\operatorname{Mor}(X, Y)$.

Definition 2.1.2 (Small / locally small category). A *small category* is a category $\mathcal{C}$ for which $\operatorname{Ob}\mathcal{C}$ and $\operatorname{Mor}\mathcal{C}$ are sets. A *locally small category* is one for which we can only say that $\operatorname{Mor}_{\mathcal{C}}(X, Y)$ is a set for each pair of objects $X, Y \in \mathcal{C}$.

In what follows we will only consider locally small categories.

Example 2.1.3.

1. In **Set**, the category of sets, the morphisms are maps (functions).
2. In **Grp**, the category of groups, the morphisms are group homomorphisms.
3. Given a group G, we can form a category $\underline{G}$ with $\operatorname{Ob}\underline{G} = \{*\}$ and $\operatorname{Mor}(*, *) = G$. The composition in $\mathcal{C}$ is the product in G.
4. Given a poset X, we can form a category $\mathcal{C}$ with $\operatorname{Ob}\mathcal{C} = X$ and
$$\operatorname{Mor}(x, x') = \begin{cases} \{(x, x')\} & x \geq x', \\ \emptyset & \text{otherwise.} \end{cases}$$
5. Given categories $\mathcal{C}$ and $\mathcal{D}$, the *product category* $\mathcal{C} \times \mathcal{D}$ has $\operatorname{Ob}(\mathcal{C} \times \mathcal{D}) = \operatorname{Ob}\mathcal{C} \times \operatorname{Ob}\mathcal{D}$ and $\operatorname{Mor}_{\mathcal{C}\times\mathcal{D}}((A, X); (B, Y)) = \operatorname{Mor}_{\mathcal{C}}(A, B) \times \operatorname{Mor}_{\mathcal{D}}(X, Y)$ in the natural way.
6. Given a category $\mathcal{C}$, the *dual category* (*opposite category*), denoted $\mathcal{C}^{\mathrm{op}}$ is the category with $\operatorname{Ob}\mathcal{C}^{\mathrm{op}} = \operatorname{Ob}\mathcal{C}$ and $\operatorname{Mor}_{\mathcal{C}^{\mathrm{op}}}(X, Y) = \operatorname{Mor}_{\mathcal{C}}(Y, X)$. For disambiguation, we may write X° to denote the copy of X in $\mathcal{C}^{\mathrm{op}}$.
7. Given a category $\mathcal{C}$, the *arrow category* $\operatorname{Arr}\mathcal{C}$ has $\operatorname{Ob}\mathcal{C} = \operatorname{Mor}\mathcal{C}$. 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:
$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "g"] & Y \arrow[d, "h"] \\ X' \arrow[r, "f'"] & Y' \end{tikzcd}$$

Definition 2.1.4 (Isomorphism)**.** A morphism $f : X \to Y$ is an *isomorphism* if there exists a morphism $g : Y \to X$ such that $f \circ g = 1_Y$ and $g \circ f = 1_X$.

Proposition 2.1.5. *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 2.1.6 (Subcategory / full subcategory)**.** Let $\mathcal{C}$ be a category. A category $\mathcal{C}'$ is a *subcategory* of $\mathcal{C}$ if $\mathrm{Ob}\,\mathcal{C}' \subset \mathrm{Ob}\,\mathcal{C}$, $\mathrm{Mor}_{\mathcal{C}'}(X,Y) \subset \mathrm{Mor}_{\mathcal{C}}(X,Y)$, and the composition law in $\mathcal{C}'$ is inherited from $\mathcal{C}$.

We say that $\mathcal{C}'$ is a *full subcategory* of $\mathcal{C}$ if $\mathrm{Mor}_{\mathcal{C}'}(X,Y) = \mathrm{Mor}_{\mathcal{C}}(X,Y)$ for all $X, Y \in \mathcal{C}'$.

Example 2.1.7.

1. In **Grp**, the subcategory **Ab** of abelian groups is a full subcategory.
2. For any subclass $A \subset \mathrm{Ob}\,\mathcal{C}$, there is a unique full subcategory $\mathcal{C}'$ of $\mathcal{C}$ such that $\mathrm{Ob}\,\mathcal{C}' = A$.

Definition 2.1.8 (Initial and terminal objects)**.** Let $X \in \mathcal{C}$ be an object.

1. X is *initial* if for every $Y \in \mathcal{C}$, there is a unique morphism $X \to Y$.
2. X is *terminal* (*final*) if for every $W \in \mathcal{C}$, there is a unique morphism $W \to X$.

Proposition 2.1.9. *If $X \in \mathcal{C}$ is an object, then X is initial (terminal) in $\mathcal{C}$ if and only if X is terminal (initial) in $\mathcal{C}^{\mathrm{op}}$.*

Example 2.1.10.

1. In **Set**, the initial object is $\emptyset$ and the terminal objects are singleton sets.
2. In **Grp**, the trivial group is initial and terminal.
3. Let G be a group. Then $\underline{G}$ has no initial or terminal objects (unless G is trivial).
4. Let X be a poset and form $\mathcal{C}$ on X as before. The initial object of $\mathcal{C}$ is the maximum of X (if it exists), while the terminal object is the minimum of X (if it exists).

Theorem 2.1.11. *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 $\mathrm{id}_X : X \to X$ is a morphism, $g \circ f = 1_X$. Similarly, $f \circ g = 1_{X'}$, so f and g are inverses and f is an isomorphism. □

2.2 Products and coproducts

Universal properties are applications of Theorem 2.1.11. As an example, we consider products.

Definition 2.2.1 (Product of two objects)**.** Let $X, Y \in \mathcal{C}$. An object $X \times Y$ together with morphisms (projections) $p : X \times Y \to X$ and $q : X \times Y \to Y$ 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.

$$\begin{tikzcd}
 & X & \\
Y & X \times Y \arrow[l, "q"'] \arrow[u, "p"] & \\
 & & Z, \arrow[ul, "h"'] \arrow[uul, bend right, "f"'] \arrow[ull, bend left, "g"]
\end{tikzcd}$$

i.e., $p \circ h = f$ and $q \circ h = g$.

Theorem 2.2.2. *Let $X \times Y$ and $\widetilde{X \times Y}$ be two products of X and Y, with projections p, q and $\tilde{p}, \tilde{q}$, respectively. Then there is a unique isomorphism $h : X \times Y \to \widetilde{X \times Y}$ such that the following diagram commutes.*

$$\begin{tikzcd}
X \times Y \arrow[r, "p"] \arrow[d, "q"'] \arrow[dr, "h"] & X \\
Y & \widetilde{X \times Y} \arrow[l, "\tilde{q}"] \arrow[u, "\tilde{p}"]
\end{tikzcd}$$

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

$$\begin{tikzcd}
Z \arrow[r] \arrow[d] & X \\
Y &
\end{tikzcd}$$

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.

$$\begin{tikzcd}
Z \arrow[r] \arrow[d] \arrow[dr] & X \\
Y & Z' \arrow[l] \arrow[u]
\end{tikzcd}$$

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

The definition of the product can be restated as follows.

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

$$\begin{aligned} \mathrm{Mor}(Z, X \times Y) &\longrightarrow \mathrm{Mor}(Z, X) \times \mathrm{Mor}(Z, Y) \\ h &\longmapsto (p \circ h, q \circ h) \end{aligned}$$

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 $\mathrm{Mor}\left(Z, \prod_i X_i\right) \cong \prod_i \mathrm{Mor}(Z, X_i)$ 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.

$$\begin{tikzcd}
X \times Y \arrow[r, "q"] \arrow[d, "p"'] \arrow[ddrr, dashed, "f\times g"] & Y \arrow[dr, "g"] & \\
X \arrow[dr, "f"'] & & Y' \\
& X' & X' \times Y' \arrow[l, "p'"] \arrow[u, "q'"']
\end{tikzcd}$$

Example 2.2.6. 1. In **Set**, the product is the ordinary Cartesian product.

2. In **Grp**, the product is the (external) direct product.
3. In **Ab**, the product is the (external) direct product. Within the context of abelian groups, it is also known as the *direct sum*, written $G \oplus H$.
4. In the category $n \to n-1 \to \cdots \to 2 \to 1$, we have $i \times j = \max(i, j)$.

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

$$\begin{tikzcd}
& X \arrow[d, "i"'] \arrow[ddr, bend left, "f"] & \\
Y \arrow[r, "j"] \arrow[drr, bend right, "g"'] & X * Y \arrow[dr, dashed, "h"] & \\
& & Z
\end{tikzcd}$$

Proposition 2.2.8. *The function*

$$\begin{aligned}
\operatorname{Mor}(X * Y, Z) &\longrightarrow \operatorname{Mor}(X, Z) \times \operatorname{Mor}(Y, Z) \\
h &\longmapsto (h \circ i, h \circ j)
\end{aligned}$$

is a bijection.

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

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

2. In **Grp**, the coproduct is the free product $G * H$.
3. In **Ab**, the coproduct is the direct sum $G \oplus H$.

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

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

(i) G is an object;

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

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

(iv) $i : G \to G$ is a morphism (corresponding to inverses);

(v) (associativity) the following diagram commutes;

$$\begin{tikzcd} G \times G \times G \arrow[r, "\mathrm{id}_G \times m"] \arrow[d, "m \times \mathrm{id}_G"] & G \times G \arrow[d, "m"] \\ G \times G \arrow[r, "m"] & G \end{tikzcd}$$

(vi) (identity) the following diagrams commute, where π_G is projection onto G;

$$\begin{tikzcd} G \times F \arrow[r, "\mathrm{id}_G \times e"] \arrow[dr, "\pi_G"'] & G \times G \arrow[d, "m"] \\ & G \end{tikzcd} \qquad \begin{tikzcd} F \times G \arrow[r, "e \times \mathrm{id}_G"] \arrow[dr, "\pi_G"'] & G \times G \arrow[d, "m"] \\ & G \end{tikzcd}$$

(vii) (inverse) the following diagrams commute.
$$\begin{tikzcd} G \arrow[r, "(\mathrm{id}_G, i)"] \arrow[d] & G \times G \arrow[d, "m"] \\ F \arrow[r, "e"] & G \end{tikzcd} \qquad \begin{tikzcd} G \arrow[r, "(i, \mathrm{id}_G)"] \arrow[d] & G \times G \arrow[d, "m"] \\ F \arrow[r, "e"] & G \end{tikzcd}$$

Example 2.2.12. 1. The group objects in **Set** are the usual groups.

2. Group objects in **Top**, the category of topological spaces, are *topological groups*.

3. Group objects in **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 $\operatorname{Ob} \mathcal{C} \to \operatorname{Ob} \mathcal{D}$ and $\operatorname{Mor}_{\mathcal{C}}(X, Y) \to \operatorname{Mor}_{\mathcal{D}}(F(X), F(Y))$ such that

(i) $F(1_X) = 1_{F(X)}$ 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 $\operatorname{Mor}_{\mathcal{C}}(X, Y)$ to $\operatorname{Mor}_{\mathcal{D}}(F(Y), F(X))$ 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 $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ or $\mathcal{C} \to \mathcal{D}^{\mathrm{op}}$, 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 $\mathrm{id} : \mathcal{C} \to \mathcal{C}$ is defined by $\mathrm{id}(X) = X$ and $\mathrm{id}(f) = f$.
2. Let $Y \in \mathcal{D}$. The constant functor $c_Y : \mathcal{C} \to \mathcal{D}$ is given by $c_Y(X) = Y$ and $c_Y(f) = \mathrm{id}_Y$.
3. The *forgetful functor* $\mathrm{Forget} : \mathbf{Grp} \to \mathbf{Set}$ has $\mathrm{Forget}(G) = G$ and $\mathrm{Forget}(f) = f$.
4. If $\mathcal{C}' \subset \mathcal{C}$ is a subcategory, there is an *inclusion functor* $I : \mathcal{C}' \hookrightarrow \mathcal{C}$.
5. Let $F : \mathbf{Grp} \to \mathbf{Ab}$ 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 $\tilde{f}$ descends to a homomorphism $G/G' \to H/H'$, which we call $F(f)$. One can check that with this definition of F on morphisms, F is a functor.
6. Let G be a group. Then to give a functor $\underline{G} \to \mathcal{C}$ is the same as to give an object X in $\mathcal{C}$ together with a "G-action" on X.
7. Let $\mathcal{I}$ be a small category. A functor $\mathcal{I} \to \mathcal{C}$ is a commutative diagram in $\mathcal{C}$ of shape $\mathcal{I}$. For example, $\mathrm{Arr}(\mathcal{C})$ is the category of diagrams of shape $\bullet \to \bullet$ in $\mathcal{C}$.

Definition 2.3.6 (Represented / corepresented functors)**.** Let $\mathcal{C}$ be a locally small category and fix $X \in \mathcal{C}$. The *functor $\mathcal{C} \to$ **Set** represented by X* is

$$\begin{aligned} R^X(Y) &= \mathrm{Mor}_{\mathcal{C}}(X, Y), \\ R^X(f)(g) &= f \circ g, \qquad\qquad f : Y \to Y' \text{ and } g \in \mathrm{Mor}_{\mathcal{C}}(X, Y). \end{aligned}$$

If we fix Y instead, then we obtain a contravariant *functor $R_Y : \mathcal{C}^{\mathrm{op}} \to$ **Set** corepresented by Y*:

$$\begin{aligned} R^Y(X^\circ) &= \mathrm{Mor}_{\mathcal{C}}(X, Y), \\ R^Y(f^\circ)(h) &= h \circ f, \qquad\qquad f : X' \to X \text{ and } h \in \mathrm{Mor}_{\mathcal{C}}(X, Y). \end{aligned}$$

Definition 2.3.7 (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 $\varphi_{X,Y} : \mathrm{Mor}_{\mathcal{C}}(X, Y) \to \mathrm{Mor}_{\mathcal{D}}(F(X), F(Y))$ 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 2.3.8. If $\mathcal{C}' \subset \mathcal{C}$ is a subcategory, the inclusion $\mathcal{C}' \hookrightarrow \mathcal{C}$ is faithful.
It is full if and only if $\mathcal{C}'$ is a full subcategory.

Definition 2.3.9 (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 2.3.10. *Let $F : \mathcal{C} \to \mathcal{D}$ be a functor.*

1. *If F is full and faithful, then $\mathcal{C}$ is equivalent to a full subcategory of $\mathcal{D}$.*
2. *If F is full and faithful, then $X \cong Y$ in $\mathcal{C}$ if and only if $F(X) \cong F(Y)$ in $\mathcal{D}$.*
3. *If F is an equivalence, then F induces a bijection between isomorphism classes in $\mathcal{C}$ and $\mathcal{D}$.*

Example 2.3.11.

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 $\mathbf{Vect}_K$, 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 $\mathbf{Vect}_K$.

   In particular, if we look at the full subcategory $\mathbf{FdVect}_K$ 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.

2.4 Morphisms of functors

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

$$\begin{tikzcd} F(X) \arrow[r, "\alpha_X"] \arrow[d, "F(f)"'] & G(X) \arrow[d, "G(f)"] \\ F(Y) \arrow[r, "\alpha_Y"] & G(Y) \end{tikzcd}$$

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

Notation. Let $\mathcal{C}, \mathcal{D}$ be categories and $F, G : \mathcal{C} \to \mathcal{D}$ be functors. Write $\mathrm{Mor}_{\mathbf{Fun}}(F, G)$ for the collection of morphisms of functors $F \to G$.

Proposition 2.4.3. *If $F, G : \mathcal{C} \to \mathcal{D}$ and $\alpha : F \to G$ is a morphism of functors, then α is an isomorphism in $\mathbf{Fun}(\mathcal{C}, \mathcal{D})$ if and only if $\alpha_X : F(X) \to G(X)$ is an isomorphism in $\mathcal{D}$ for all X in $\mathcal{C}$.*

Example 2.4.4.

1. If $\mathcal{I}$ is a small category, then the category $\mathbf{Fun}(\mathcal{I}, \mathcal{D})$ is the category $\mathrm{Diag}_{\mathcal{I}}(\mathcal{D})$ of diagrams of shape $\mathcal{I}$ in $\mathcal{D}$.
2. Let $F : \mathbf{Grp} \to \mathbf{Grp}$ be the abelianization functor (with target $\mathbf{Grp}$). For each $G \in \mathbf{Grp}$, set $\alpha_G = \pi : G \to G/G'$. Then α is a morphism $\mathrm{id}_{\mathbf{Grp}} \to F$.

3. Given $f : X \to X'$ in a category $\mathcal{C}$, we have a morphism $R^{X'}(Y) \to R^X(Y)$ for each Y given by $g \mapsto g \circ f$, and one can check that this produces a morphism of represented functors $R^f : R^{X'} \to R^X$. Hence there is a functor $\mathcal{C}^{\mathrm{op}} \to \mathbf{Fun}(\mathcal{C}, \mathbf{Set})$ with $X^{\mathrm{op}} \mapsto R^X$ and $f^{\mathrm{op}} \mapsto R^f$.

   Equivalently, we have a functor $\mathcal{C}^{\mathrm{op}} \times \mathcal{C} \to \mathbf{Set}$ with $(X^{\mathrm{op}}, Y) \mapsto \mathrm{Mor}_{\mathcal{C}}(X, Y)$, or a functor $\mathcal{C} \to \mathbf{Fun}(\mathcal{C}^{\mathrm{op}}, \mathbf{Set})$ with $Y \mapsto R_Y$, where $R_Y(X^{\mathrm{op}}) = \mathrm{Mor}_{\mathcal{C}}(X, Y)$.

Lemma 2.4.5 (Yoneda)**.** *Let $\mathcal{C}$ be a locally small category and fix X in $\mathcal{C}$. Let $F : \mathcal{C} \to \mathbf{Set}$ be a functor. Then there is a bijection $\varphi : \mathrm{Mor}_{\mathbf{Fun}}(R^X, F) \to F(X)$ given by*

$$\varphi(\alpha) = \alpha_X(1_X).$$

Proof. Let $\alpha : R^X \to F$ be a morphism of functors. By the very definition, for every morphism $f : X \to Y$ in $\mathcal{C}$ the diagram

$$\begin{tikzcd}
R^X(X) \arrow[r, equal] \arrow[d, "R^X(f)"'] & \mathrm{Mor}(X,X) \arrow[r, "\alpha_X"] \arrow[d, "f\circ-"] & F(X) \arrow[d, "F(f)"] \\
R^X(Y) \arrow[r, equal] & \mathrm{Mor}(X,Y) \arrow[r, "\alpha_Y"] & F(Y).
\end{tikzcd}$$

is commutative. It follows that

$$\alpha_Y(f) = F(f)(\alpha_X(1_X)) = F(f)(\varphi(\alpha)).$$

We prove the injectivity of φ. Suppose $\varphi(\alpha) = \varphi(\beta)$ for $\alpha, \beta \in \mathrm{Mor}_{\mathbf{Fun}}(R^X, F)$. Then for every morphism $f : X \to Y$ in $\mathcal{C}$ we have

$$\alpha_Y(f) = F(f)(\varphi(\alpha)) = F(f)(\varphi(\beta)) = \beta_Y(f),$$

hence $\alpha = \beta$.

Next we prove the surjectivity of φ. Let $u \in F(X)$. For every object Y define a map

$$\alpha_Y : R^X(Y) = \mathrm{Mor}(X, Y) \to F(Y)$$

by the formula

$$\alpha_Y(f) = F(f)(u).$$

Let $g : Y \to Y'$ be a morphism. The diagram

$$\begin{tikzcd}
R^X(Y) \arrow[r, equal] \arrow[d, "R^X(g)"'] & \mathrm{Mor}(X,Y) \arrow[r, "\alpha_Y"] \arrow[d, "g\circ-"] & F(Y) \arrow[d, "F(g)"] \\
R^X(Y') \arrow[r, equal] & \mathrm{Mor}(X,Y') \arrow[r, "\alpha_{Y'}"] & F(Y').
\end{tikzcd}$$

is commutative. Indeed, for every $f : X \to Y$,

$$(F(g) \circ \alpha_Y)(f) = F(g)(F(f)(u)) = F(g \circ f)(u) = \alpha_{Y'}(g \circ f)(u) = (\alpha_{Y'} \circ R^X(g))(f).$$

It follows that the collection (α_Y) is a morphism of functors $\alpha : R^X \to F$. Finally,

$$\varphi(\alpha) = \alpha_X(1_X) = F(1_X)(u) = 1_{F(X)}(u) = u,$$

i.e., φ is surjective. $\square$

Corollary 2.4.6. $\mathrm{Mor}_{\mathbf{Fun}}(R^X, R^Y) \cong \mathrm{Mor}_{\mathcal{C}}(Y, X)$.

Corollary 2.4.7. *Every natural transformation $R^X \to R^Y$ is of the form R^f for a unique morphism $f : Y \to X$.*

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

Definition 2.4.9 (Representable functor)**.** A functor $F : \mathcal{C} \to \mathbf{Set}$ is *representable* if F is isomorphic to R^X for some X. We say that F is *represented by 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.*

$$\begin{tikzcd} R^Y \arrow[dr, "R^f"'] & F \arrow[l, "iso"'] \arrow[d, "iso"] \\ & R^X \end{tikzcd}$$

In other words, the object X is uniquely determined up to canonical isomorphism.

Example 2.4.11.

1. $c_{\{*\}} : \mathcal{C} \to \mathbf{Set}$ is represented by any initial object of $\mathcal{C}$.
2. Let X be a set and define $F : \mathbf{Grp}^{\mathrm{op}} \to \mathbf{Set}$ by $G^{\mathrm{op}} \mapsto \{\text{left } G\text{-actions on } X\}$. Then the symmetric group $S(X)$ represents F.
3. Let $\mathcal{C}$ be a locally small category with products and fix $X, Y \in \mathcal{C}$. Let $F : \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ be given by $F(Z) = \mathrm{Mor}(Z, X) \times \mathrm{Mor}(Z, Y)$. This is corepresented by $X \times Y$, i.e. $R_{X\times Y} \cong R_X \times R_Y$. Similarly, $R^X \times R^Y \cong R^{X*Y}$ if $\mathcal{C}$ has coproducts.
4. Let X be an object of a category $\mathcal{C}$ and consider the functor $\mathbf{Fun}(\mathcal{C}, \mathbf{Set}) \to \mathbf{Set}$ given by $F \mapsto F(X)$. This functor is represented by R^X.
5. Let X be a set. The functor $\mathbf{Grp} \to \mathbf{Set}$ taking a group G to the set of all maps $X \to G$ is represented by the free group $\mathrm{Free}(X)$.
6. The forgetful functor $\mathbf{Grp} \to \mathbf{Set}$ is represented by $\mathbb{Z}$.

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 $\mathcal{C}^{\mathrm{op}} \times \mathcal{D} \to \mathbf{Set}$, given by

$$(X^\circ, Y) \longmapsto \mathrm{Mor}_{\mathcal{C}}(X, G(Y)), \qquad (X^\circ, Y) \longmapsto \mathrm{Mor}_{\mathcal{D}}(F(X), Y).$$

We say that F, G form an *adjunction pair* (or F and G are *adjoint*), 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 canonically isomorphic.*

Proof. For any X in $\mathcal{C}$, the functor $\mathcal{D} \to \mathbf{Set}$ given by

$$Y \longmapsto \mathrm{Mor}_{\mathcal{C}}(X, G(Y)) \cong \mathrm{Mor}_{\mathcal{D}}(F(X), Y) = R^{F(X)}(Y)$$

is represented by $F(X)$. The same can be done for F', so $F(X) \cong F'(X)$ for all X in $\mathcal{C}$. By following the isomorphisms, we find that F and F' themselves are isomorphic. $\square$

Example 2.4.14.

1. Let $F : \mathcal{C} \to \mathcal{D}$ be an equivalence of categories and let $G : \mathcal{D} \to \mathcal{C}$ be a *quasi-inverse* of F, i.e., $F \circ G$ is isomorphic to $\mathrm{id}_{\mathcal{D}}$ and $G \circ F$ is isomorphic to $\mathrm{id}_{\mathcal{C}}$. Then G is a left and right adjoint of F.
2. The product (resp., coproduct) functor $\mathcal{C} \times \mathcal{C} \to \mathcal{C}$ has a left (resp., right) adjoint functor $X \mapsto (X, X)$.
3. The forgetful functor $\mathbf{Grp} \to \mathbf{Set}$ has as a left adjoint $X \mapsto \mathrm{Free}(X)$.
4. The inclusion functor $\mathbf{Ab} \hookrightarrow \mathbf{Grp}$ has as a left adjoint the abelianization functor.
5. Fix an integer $n > 0$. The functor $F : \mathbf{Ab} \to \mathbf{Ab}$, $F(A) = A[n] := \{a \in A \ : \ na = 0\}$, has left adjoint $B \mapsto B/nB$.

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 morphism

$$F(\prod X_i) \to \prod F(X_i)$$

is an isomorphism for any family of objects X_i 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_i be a family of objects in $\mathcal{C}$ and Z in $\mathcal{D}$. Then

$$\begin{aligned}\mathrm{Mor}_{\mathcal{D}}(Z, F(\prod X_i)) &\cong \mathrm{Mor}_{\mathcal{C}}(G(Z), \prod X_i) \cong \prod \mathrm{Mor}_{\mathcal{C}}(G(Z), X_i) \\ &\cong \prod \mathrm{Mor}_{\mathcal{D}}(Z, F(X_i)) \cong \mathrm{Mor}_{\mathcal{D}}(Z, \prod F(X_i)).\end{aligned}$$

□

Example 2.4.17. The forgetful functor $\mathbf{Grp} \to \mathbf{Set}$ commutes with products.

2.5 Limits and colimits

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 $\mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ given by $X^{\mathrm{op}} \mapsto \mathrm{Mor}_{\mathbf{Fun}}(c_X, F)$. The *limit* of F is an object $\lim F$ in $\mathcal{C}$ corepresenting this functor. In other words, there are natural in X bijections

$$\mathrm{Mor}_{\mathbf{Fun}}(c_X, F) \simeq \mathrm{Mor}_{\mathcal{C}}(X, \lim F).$$

The *colimit* of F is an object $\mathrm{colim}\, F$ representing the functor $\mathcal{C} \to \mathbf{Set}$ given by $X \mapsto \mathrm{Mor}_{\mathbf{Fun}}(F, c_X)$. In other words, there are natural in X bijections

$$\mathrm{Mor}_{\mathbf{Fun}}(F, c_X) \simeq \mathrm{Mor}_{\mathcal{C}}(\mathrm{colim}\, F, X).$$

Definition 2.5.2 (Cone)**.** Let $\mathcal{I}$ be a small category with $\mathrm{Ob}\, \mathcal{I} = \{X_j\}_{j \in J}$, 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

$$\lim F = \prod_{i\in\mathcal{I}} F(i), \quad \operatorname{colim} F = \coprod_{i\in\mathcal{I}} F(i).$$

2. If $\mathcal{I}$ has a final (resp., initial) object i, then $\operatorname{colim} F = F(i)$ (resp., $\lim F = F(i)$).

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

$$\begin{tikzcd} & \cdot \arrow[d] \\ \cdot \arrow[r] & \cdot \end{tikzcd}$$

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

$$\begin{tikzcd} & A \arrow[d] \\ B \arrow[r] & C \end{tikzcd}$$

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.

$$\begin{tikzcd} Y \arrow[dr, "f"] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\ & X \arrow[r] \arrow[d] & A \arrow[d] \\ & B \arrow[r] & C \end{tikzcd}$$

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

4. Let $\mathcal{I}$ be a small category. The functor $\mathcal{C} \to \operatorname{Diag}_{\mathcal{I}}(\mathcal{C})$ taking an object X to the constant diagram c_X has right adjoint $F \mapsto \lim F$ and left adjoint $F \mapsto \operatorname{colim} F$.

5. Let G be a group and let $F : \underline{G} \to \mathcal{C}$ be given by a G-object X in $\mathcal{C}$. Then the object X^G of the "G-fixed part of X" can be defined as $\lim F$. The "orbit space" X/G is defined as $\operatorname{colim} F$.

6. The limit of the diagram

$$\begin{tikzcd} Y \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & X \end{tikzcd}$$

is called the *equalizer* of f and g. It is an object Z together with a morphism $i : Z \to Y$ such that $f \circ i = g \circ i$ satisfying the following universal property: for every morphism $j : U \to Y$

such that $f \circ j = g \circ j$ there is a unique morphism $k : U \to Z$ such that $j = i \circ k$. Equivalently, the sequence

$$\mathrm{Maps}(U, Z) \xhookrightarrow{i} \mathrm{Maps}(U, Y) \underset{g}{\overset{f}{\rightrightarrows}} \mathrm{Maps}(U, X)$$

is an equalizer sequence of maps of sets. Dually one defines the *co-equalizer* of f and g as the colimit of the diagram.

Let $\mathcal{I} \xrightarrow{F} \mathcal{C} \xrightarrow{G} \mathcal{D}$ be two functors. Applying G to the canonical morphism $c_{\lim F} \to F$, we get a morphism $c_{G(\lim F)} \to G \circ F$, that yields a morphism $\varphi : G(\lim F) \to \lim(G \circ F)$. We say that a functor $G : \mathcal{C} \to \mathcal{D}$ *commutes with limits* if for every functor $F : \mathcal{I} \to \mathcal{C}$ the morphism φ is an isomorphism.

Proposition 2.5.6. *If a functor $G : \mathcal{C} \to \mathcal{D}$ has a left (resp., right) adjoint, then G commutes with limits (resp., colimits).*

2.6 Additive and abelian categories

Definition 2.6.1 (Preadditive category)**.** A locally small category $\mathcal{A}$ is called *preadditive* if for every two objects X and Y in $\mathcal{A}$ the set $\mathrm{Mor}_{\mathcal{A}}(X, Y)$ is equipped with the structure of an abelian group (written additively) such that the composition is bilinear, i.e., $(f + f') \circ g = f \circ g + f' \circ g$ and $f \circ (g + g') = f \circ g + f \circ g'$.

If $\mathcal{A}$ is a preadditive category, then so is the opposite category $\mathcal{A}^{\mathrm{op}}$.

Definition 2.6.2 (Biproduct)**.** Let $\mathcal{A}$ be a preadditive category. Let X and Y be two objects in $\mathcal{A}$. A *biproduct* of X and Y is an object Z together with the four morphisms $i : X \to Z$, $p : Z \to X$, $j : Y \to Z$ and $q : Z \to Y$ such that $p \circ i = 1_X$, $q \circ i = 0$, $p \circ j = 0$, $q \circ j = 1_Y$ and $i \circ p + j \circ q = 1_Z$.

A biproduct of X and Y in $\mathcal{A}$ yields a biproduct of X^{op} and Y^{op} in $\mathcal{A}^{\mathrm{op}}$.

Let (Z, i, j, p, q) be a biproduct of X and Y. Then (Z, p, q) is a product of X and Y. Indeed, if $f : U \to X$ and $g : U \to Y$ be two morphisms, the setting $h = i \circ f + j \circ g : U \to Z$, we have $p \circ h = f$ and $q \circ h = g$. Moreover if $h' : U \to Z$ satisfies $p \circ h' = f$ and $q \circ h' = g$, then $h' = (i \circ p + j \circ q) \circ h' = i \circ f + j \circ g = h$.

Similarly, (Z, i, j) is a coproduct of X and Y. Thus, if X and Y admit a biproduct Z, then Z is also a product and coproduct of X and Y.

Let (Z, p, q) be a product of two objects X and Y. We claim that it extends to a biproduct of X and Y. Indeed, we let $i : X \to Z$ be the morphism determined by the pair of morphisms $1_X : X \to X$ and $0 : X \to Y$. Similarly, $j : Y \to Z$ is determined by the pair of morphisms $0 : Y \to X$ and $1_Y : Y \to Y$. This proves the claim.

Equivalently a coproduct (Z, i, j) of two objects X and Y extends naturally to a biproduct of X and Y. Thus, to give a biproduct of two objects in a preadditive category is equivalent to give their product (or coproduct).

Definition 2.6.3 (Additive category)**.** A preadditive category $\mathcal{A}$ is called *additive* if finite products exist in $\mathcal{A}$.

Note that the product, coproduct and biproduct of every two objects in an additive category coincide. In particular, initial and final objects coincide. They are called *zero objects*. A zero object X is characterized by the property $1_X = 0_X$.

Example 2.6.4. 1. The category **Ab** of abelian groups is additive.

2. The category of morphisms in **Ab** is additive.

3. The category of short exact sequences in **Ab** is additive.

4. A full subcategory of an additive category that is closed under finite products is additive. For example, the category of free groups $\mathbb{Z}^n$ is additive.

5. If $\mathcal{A}$ is an additive category, then the category of functors $\mathcal{A}^{\mathrm{op}} \to \mathbf{Ab}$ (the category of presheaves of abelian groups on $\mathcal{A}$) is additive.

A functor $F : \mathcal{A} \to \mathcal{B}$ between additive categories is called *additive* if $F(g+h) = F(g) + F(h)$ for every two morphisms $g, h : X \to Y$ in $\mathcal{A}$. If F is additive, then $F(0_X) = 0_{F(X)}$ for every object X in $\mathcal{A}$. It follows that for a zero object 0 in $\mathcal{A}$ we have $1_{F(0)} = F(1_0) = F(0_0) = 0_{F(0)}$, i.e., $F(0)$ is a zero object in $\mathcal{B}$. Thus, an additive functors take zero objects to zero objects.

Example 2.6.5. 1. Let $\mathcal{A}$ be an additive category and A an object in $\mathcal{A}$. The functor $R^A : \mathcal{A} \to \mathbf{Ab}$ taking an object X to the group $\mathrm{Mor}_{\mathcal{A}}(A, X)$ is additive. The functor R^A is called *represented by* A. An additive functor $F : \mathcal{A} \to \mathbf{Ab}$ is called *representable* if F is isomorphic to R^A for some A. By an additive analog of the Yoneda Lemma, the object A is uniquely determined up to canonical isomorphism. In a similar fashion one defines *corepresentable* functors $\mathcal{A}^{\mathrm{op}} \to \mathbf{Ab}$.

2. The constant functor $\mathcal{A} \to \mathbf{Ab}$ taking any object to a fixed abelian group A is not additive unless A is zero.

Let (Z, i, j, p, q) be a biproduct in $\mathcal{A}$. Then for an additive functor $F : \mathcal{A} \to \mathcal{B}$, the tuple $(F(Z), F(i), F(j), F(p), F(q))$ is a biproduct in $\mathcal{B}$. It follows that F takes direct products (coproducts) to direct products (coproducts).

Let $\mathcal{A}$ be an additive category and $f : A \to B$ a morphism in $\mathcal{A}$. The *kernel of* f, denoted $\mathrm{Ker}(f)$ is the equalizer of

$$A \underset{0}{\overset{f}{\rightrightarrows}} B.$$

By definition $\mathrm{Ker}(f)$ is equipped with a morphism $i : \mathrm{Ker}(f) \to A$ such that for every object X the sequence

$$0 \to \mathrm{Mor}(X, \mathrm{Ker}(f)) \xrightarrow{i_*} \mathrm{Mor}(X, A) \xrightarrow{f_*} \mathrm{Mor}(X, B) \tag{1}$$

is exact. In different words, the kernel of f corepresents the functor $\mathrm{Ker}(R_A \xrightarrow{f_*} R_B)$.

Similarly, the *cokernel of* f, denoted $\mathrm{Coker}(f)$ is the co-equalizer of the pair f and 0. By definition $\mathrm{Coker}(f)$ is equipped with a morphism $j : B \to \mathrm{Coker}(f)$ such that for every object Y the sequence

$$0 \to \mathrm{Mor}(\mathrm{Coker}(f), Y) \xrightarrow{j^*} \mathrm{Mor}(B, Y) \xrightarrow{f^*} \mathrm{Mor}(A, Y)$$

is exact. The cokernel of f represents the functor $\mathrm{Ker}(R^B \xrightarrow{f^*} R^A)$.
We also define the *image* $\mathrm{Im}(f)$ by the formula

$$\mathrm{Im}(f) = \mathrm{Ker}(B \xrightarrow{j} \mathrm{Coker}(f))$$

and the *coimage* $\mathrm{Coim}(f)$ by

$$\mathrm{Coim}(f) = \mathrm{Coker}(\mathrm{Ker}(f) \xrightarrow{i} A).$$

Definition 2.6.6 (Preabelian category)**.** An additive category $\mathcal{A}$ is called *pre-abelian* if every morphism in $\mathcal{A}$ has kernel and cokernel (and hence image and coimage).

Example 2.6.7.
1. The category **Ab** of abelian groups is pre-abelian, but the full subcategory of free groups is not preabelian.
2. The category of pairs (A, B) of abelian groups such that A is a subgroup of B and morphisms $(A', B') \to (A, B)$ being group homomorphisms $f : B' \to B$ such that $f(A') \subset A$ is pre-abelian.

Consider a commutative square in a pre-abelian category:

$$\begin{tikzcd} A' \arrow[r, "f'"] \arrow[d] & B' \arrow[d] \\ A \arrow[r, "f"] & B. \end{tikzcd}$$

The composition $\mathrm{Ker}(f') \to A' \to A \xrightarrow{j} B$ coincides with the composition $\mathrm{Ker}(f') \to A' \xrightarrow{j'} B' \to B$ and hence is zero. By the definition of the kernel (and similarly for the cokernel), there are unique morphisms $\mathrm{Ker}(f') \to \mathrm{Ker}(f)$ and $\mathrm{Coker}(f') \to \mathrm{Coker}(f)$ making the diagram

$$\begin{tikzcd} \mathrm{Ker}(f') \arrow[r] \arrow[d] & A' \arrow[r, "f'"] \arrow[d] & B' \arrow[r] \arrow[d] & \mathrm{Coker}(f') \arrow[d] \\ \mathrm{Ker}(f) \arrow[r] & A \arrow[r, "f"] & B \arrow[r] & \mathrm{Coker}(f) \end{tikzcd}$$

commutative. Moreover, we can view the kernels and cokernels as functors $\mathrm{Arr}(\mathcal{A}) \to \mathcal{A}$.
Let

$$A \xrightarrow{f} B \xrightarrow{g} C \tag{2}$$

two morphisms in a pre-abelian category such that $g \circ f = 0$. By the definition of the cokernel, there is a unique morphism $k : C \to C$ such that g is the composition $B \xrightarrow{j} \mathrm{Coker}(f) \xrightarrow{k} C$. The commutative square

$$\begin{tikzcd} B \arrow[r, "j"] \arrow[d, "1_B"] & \mathrm{Coker}(f) \arrow[d, "k"] \\ B \arrow[r, "g"] & C \end{tikzcd}$$

yields aa morphism

$$\mathrm{Im}(f) = \mathrm{Ker}(j) \to \mathrm{Ker}(g).$$

We say that the sequence (2) with $g \circ f = 0$ is *exact* if the morphism $\mathrm{Im}(f) \to \mathrm{Ker}(g)$ is an isomorphism.

Lemma 2.6.8. *Let $f : A \to B$ be a morphism in a pre-abelian category. TFAE:*

(1) The sequence $0 \to A \xrightarrow{f} B$ is exact;

(2) $\mathrm{Ker}(f) = 0$;

(3) f is a monomorphism, i.e., the map $f_* : \mathrm{Mor}(X, A) \to \mathrm{Mor}(X, B)$ is injective for any object X.

Proof. (1) $\Leftrightarrow$ (2): Clearly, the image of $0 \to A$ is 0. Thus the sequence is exact if and only if $\mathrm{Ker}(f) = 0$.

(2) $\Leftrightarrow$ (3): In view of (1), f_* is injective for all X if and only if $\mathrm{Mor}(X, \mathrm{Ker}(f)) = 0$ for all X. The latter is equivalent to $\mathrm{Ker}(f) = 0$. $\square$

Dually, the sequence $0A \xrightarrow{f} B \to 0$ is exact if and only if $\mathrm{Coker}(f) = 0$ if and only if f is an epimorphism.

Let $f : A \to B$ be a morphism in a pre-abelian category $\mathcal{A}$. Note that we have canonical morphisms $k : A \to \mathrm{Coim}(f)$ and $l : \mathrm{Im}(f) \to B$. Since the composition $A \xrightarrow{f} B \xrightarrow{j} \mathrm{Coker}(f)$ is zero, by the definition of the image of f, there is a unique morphism $m : A \to \mathrm{Im}(f)$ such that $l \circ m = f$. As the composition $\mathrm{Ker}(f) \xrightarrow{i} A \xrightarrow{f} B$ is zero and the map

$$l_* : \mathrm{Mor}(\mathrm{Ker}(f), \mathrm{Im}(f)) \to \mathrm{Mor}(\mathrm{Ker}(f), B)$$

is injective (since $\mathrm{Im}(f)$ is the kernel!), the composition $\mathrm{Ker}(f) \xrightarrow{i} A \xrightarrow{m} Im(f)$ is zero. By the definition of $\mathrm{Coim}(f)$, there is a unique morphism $g : \mathrm{Coim}(f) \to \mathrm{Im}(f)$ such that $g \circ k = m$. Since $l \circ g \circ k = l \circ m = f$, the morphism f factors into the composition

$$A \xrightarrow{k} \mathrm{Coim}(f) \xrightarrow{g} \mathrm{Im}(f) \xrightarrow{l} B.$$

Example 2.6.9. Let $f : A \to B$ be a morphism in **Ab**. Then $\mathrm{Coker}(f) = B/\mathrm{Im}(f)$ and $\mathrm{Coim}(f) = A/\mathrm{Ker}(f)$. The morphism $g : A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ is the isomorphism given by the First Isomorphism Theorem.

Definition 2.6.10 (Abelian category)**.** A pre-abelian category $\mathcal{A}$ is called *abelian* is for every morphism $f : A \to B$, the induced morphism $g : \mathrm{Coim}(f) \to \mathrm{Im}(f)$ is an isomorphism, i.e., the First Isomorphism Theorem holds in $\mathcal{A}$.

Example 2.6.11.

1. The category **Ab** of abelian groups is abelian.
2. The full subcategory of finite groups in **Ab** is abelian.
3. If $\mathcal{A}$ is a abelian, so is $\mathcal{A}^{\mathrm{op}}$.
4. For every category $\mathcal{C}$ and an abelian category $\mathcal{A}$, the category of functors $\mathcal{C} \to \mathcal{A}$ is abelian. In particular, the category of diagrams of a given shape in an abelian category is abelian.

5. The category of pairs of abelian groups as above is not abelian. Let $A' \subset A \subset B$ be subgroups and let $f : (A', B) \to (A, B)$ be the morphism given by the identity of B. We have $\mathrm{Ker}(f) = 0 = \mathrm{Coker}(f)$, $\mathrm{Coim}(f) = (A', B)$ and $\mathrm{Im}(f) = (A, B)$. The morphism $g = f : (A', B) \to (A, B)$ is not an isomorphism if $A' \neq A$.

Lemma 2.6.12. *If $f : A \to B$ be a monomorphism in an abelian category, then* $\mathrm{Im}(f) = A$*. Dually, if $g : B \to C$ be an epimorphism, then* $\mathrm{Coim}(g) = C$*.*

Proof. By Lemma 2.6.8, $\mathrm{Ker}(f) = 0$, hence

$$\mathrm{Coim}(f) = \mathrm{Coker}(\mathrm{Ker}(f) \to A) = \mathrm{Coker}(0 \to A) = A.$$

Since the category is abelian, $\mathrm{Im}(f) = \mathrm{Coim}(f) = A$. □

Corollary 2.6.13. *Let $f : A \to B$ be a morphism in an abelian category. TFAE:*

1. *f is an isomorphism;*
2. $\mathrm{Ker}(f) = 0 = \mathrm{Coker}(f)$*;*
3. *f is a monomorphism and epimorphism.*

Proof. (1) ⇒ (2) is clear and (2) ⇔ (3) is proved in Lemma 2.6.8.
(3) ⇒ (1): By Lemma 2.6.12, f is isomorphic to the isomorphism $\mathrm{Coim}(f) \xrightarrow{\sim} \mathrm{Im}(f)$. □

Proposition 2.6.14. *Let $\mathcal{A}$ be an abelian category. Then*
1) A sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ in $\mathcal{A}$ is exact if and only if $A = \mathrm{Ker}(g)$.
2) A sequence $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ in $\mathcal{A}$ is exact if and only if $C = \mathrm{Coker}(f)$.

Proof. We prove 1. If the sequence is exact, then f is a monomorphism by Lemma 2.6.8. Hence $A = \mathrm{Im}(f) = \mathrm{Ker}(g)$ by Lemma 2.6.12. Conversely, since $A = \mathrm{Ker}(g)$, the morphism f is a monomorphism in view of (1). By Lemma 2.6.12 again, $A = \mathrm{Im}(f)$, hence $\mathrm{Im}(f) = \mathrm{Ker}(g)$, i.e., the sequence is exact. □

Corollary 2.6.15. *Let $\mathcal{A}$ be an abelian category. Then*
1) A sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ in $\mathcal{A}$ is exact if and only if the sequence of abelian groups

$$0 \to \mathrm{Mor}(X, A) \xrightarrow{f_*} \mathrm{Mor}(X, B) \xrightarrow{g_*} \mathrm{Mor}(X, C)$$

is exact for every X.
2) A sequence $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ in $\mathcal{A}$ is exact if and only if the sequence of abelian groups

$$0 \to \mathrm{Mor}(C, Y) \xrightarrow{g^*} \mathrm{Mor}(B, Y) \xrightarrow{f^*} \mathrm{Mor}(A, Y)$$

is exact for every Y.

Example 2.6.16. For a morphism $f : A \to B$ in an abelian category the sequence

$$0 \to \operatorname{Ker}(f) \to A \xrightarrow{f} B \to \operatorname{Coker}(f) \to 0$$

is exact.

An additive functor $F : \mathcal{A} \to \mathcal{B}$ between two abelian categories is called *left exact* if for every exact sequence $0 \to A \to B \to C$ in $\mathcal{A}$ the sequence

$$0 \to F(A) \to F(B) \to F(C)$$

is exact in $\mathcal{B}$. Similarly, F is called *left exact* if for every exact sequence $A \to B \to C \to 0$ in $\mathcal{A}$ the sequence

$$F(A) \to F(B) \to F(C) \to 0$$

is exact in $\mathcal{B}$. The functor F is called *exact* if it is left and right exact.

Example 2.6.17. For an object A of an abelian category $\mathcal{A}$ the represented functor $R^A : \mathcal{A} \to \mathbf{Ab}$ is left exact. The corepresented functor $R_A : \mathcal{A}^{\mathrm{op}} \to \mathbf{Ab}$ is also left exact.

Theorem 2.6.18 (Mitchell)**.** *Let $\mathcal{A}$ be a small abelian category. Then there is a ring R and a full faithful exact functor from $\mathcal{A}$ to the abelian category of left R-modules.*

A commutative diagram

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

in an abelian category with exact rows yields a sequence

$$\operatorname{Ker}(f) \to \operatorname{Ker}(g) \to \operatorname{Ker}(h) \to \operatorname{Coker}(f) \to \operatorname{Coker}(g) \to \operatorname{Coker}(h)$$

Theorem 2.6.19 (Snake Lemma)**.** *This sequence is exact.*

Theorem 2.6.20. *Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence in an abelian category. Then the following are equivalent:*

(1) (right split) there exists $g' : C \to B$ such that $g \circ g' = \mathrm{id}_C$;

(2) (left split) there exists $f' : B \to A$ such that $f' \circ f = \mathrm{id}_A$;

(3) this short exact sequence is isomorphic to $0 \to A \to A \oplus C \to C \to 0$.

Proof. (2) $\implies$ (3) Given f' as in (2), we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "1_A"] & B \arrow[r, "g"] \arrow[d, "{(f',g)}"] & C \arrow[r] \arrow[d, "1_C"] & 0 \\
0 \arrow[r] & A \arrow[r] & A \oplus C \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

By the Snake Lemma, the middle morphism is an isomorphism.

(1) $\implies$ (3) is similar.

(3) $\implies$ (1) and (3) $\implies$ (2) are obvious. $\square$

Definition 2.6.21. A short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ in an abelian category is called *split* if all conditions in the theorem hold.

Proposition 2.6.22. *Let P be an object of an abelian category. The following are equivalent:*

(1) the functor $\mathrm{Mor}(P,-)$ *is exact;*

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

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

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

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

$$0 \longrightarrow \mathrm{Mor}(P,A) \xrightarrow{f_*} \mathrm{Mor}(P,B) \xrightarrow{g_*} \mathrm{Mor}(P,C) \longrightarrow 0$$

is exact if and only if g_* is surjective, or equivalently, for all $h \in \mathrm{Mor}(P,C)$, there exists $r \in \mathrm{Mor}(P,B)$ such that $g_*(r) = g \circ r = h$.

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

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

Then $s \circ r = 1_P$, so s gives the required splitting.

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

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

Let

$$A := \mathrm{Ker}(g), \qquad D := \mathrm{Ker}(B \oplus P) \xrightarrow{(g,h)} C.$$

We have a commutative diagram with the exact rows:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "k"] & B \arrow[r, "g"] \arrow[d, "{(1_B,0)}"] & C \arrow[r] \arrow[d, "1_C"] & 0 \\ 0 \arrow[r] & D \arrow[r, "{(i,j)}"] & B \oplus P \arrow[r, "{(g,h)}"] & C \arrow[r] & 0. \end{tikzcd}$$

By the Snake Lemma the top row of the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "k"] \arrow[d, "1_A"] & D \arrow[r, "-j"] \arrow[d, "i"] & P \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0.
\end{tikzcd}$$

is exact. The upper row is split, so there exists $l : P \to D$ with $(-j) \circ l = 1_P$. Take

$$r = i \circ l : P \to B.$$

Then

$$g \circ r = g \circ i \circ l = h \circ (-j) \circ l = h \circ 1_P = h. \qquad \square$$

Definition 2.6.23. An object P is called *projective* if P satisfies all equivalent conditions of the proposition.

Dually, we get the following statement.

Proposition 2.6.24. *Let Q be an object of an abelian category. The following are equivalent:*

(1) the functor $\mathrm{Mor}(-, Q)$ *is exact;*

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

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

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

Definition 2.6.25. An object Q is called *injective* if Q satisfies all equivalent conditions of the proposition.