Algebra I (Math 200)

UCSC, Fall 2021

Robert Boltje©

Contents

Chapter I: Groups

1 Semigroups and Monoids

1.1 Definition Let S be a set.

(a) A *binary operation* on S is a function $b : S \times S \to S$. Usually, $b(x, y)$ is abbreviated by xy, $x \cdot y$, $x * y$, $x \bullet y$, $x \circ y$, $x + y$, etc.

(b) Let $(x, y) \mapsto x * y$ be a binary operation on S.

(i) $*$ is called *associative*, if $(x * y) * z = x * (y * z)$ for all $x, y, z \in S$.

(ii) $*$ is called *commutative*, if $x * y = y * x$ for all $x, y \in S$.

(iii) An element $e \in S$ is called a *left* (resp. *right*) identity, if $e * x = x$ (resp. $x * e = x$) for all $x \in S$. It is called an *identity element* if it is a left and right identity.

(c) The set S together with a binary operation $*$ is called a *semigroup* if $*$ is associative. A semigroup $(S, *)$ is called a *monoid* if it has an identity element.

1.2 Examples (a) Addition (resp. multiplication) on $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ is a binary operation which is associative and commutative. The element 0 (resp. 1) is an identity element. Hence $(\mathbb{N}_0, +)$ and $(\mathbb{N}_0, \cdot)$ are commutative monoids. $\mathbb{N} := \{1, 2, \ldots\}$ together with addition is a commutative semigroup, but not a monoid. $(\mathbb{N}, \cdot)$ is a commutative monoid.

(b) Let X be a set and denote by $\mathcal{P}(X)$ the set of its subsets (its *power set*). Then, $(\mathcal{P}(X), \cup)$ and $(\mathcal{P}(X), \cap)$ are commutative monoids with respective identities $\emptyset$ and X.

(c) $x*y := (x+y)/2$ defines a binary operation on $\mathbb{Q}$ which is commutative but not associative. (Verify!)

(d) Let X be a set. Then, composition $(f, g) \mapsto f \circ g$ is a binary operation on the set $F(X, X)$ of all functions $X \to X$. $(F(X, X), \circ)$ is a monoid with the identity map $\mathrm{id}_X \colon X \to X$, $x \mapsto x$, as identity element. In general it is not commutative. (Verify!)

1.3 Remark Sometimes a binary operation $*$ is given by a table of the form

$$\begin{array}{c|ccc} * & \cdots & y & \cdots \\ \hline \vdots & & \vdots & \\ x & \cdots & x*y & \\ \vdots & & \vdots & \end{array}$$

For instance, the binary operation "and" on the set $\{\text{true}, \text{false}\}$ can be depicted as

$\wedge$	true	false
true	true	false
false	false	false

Thus, $(\{\text{true}, \text{false}\}, \wedge)$ is a commutative monoid with identity element true.

1.4 Remark Let $(S, *)$ be a semigroup and let $x_1, \ldots, x_n \in S$. One defines $x_1 * x_2 * \cdots * x_n := x_1 * (x_2 * (\cdots * x_n) \cdots)$. Using induction on $n \geqslant 3$, one can prove that this element equals the element that one obtains by any other choice of setting the parentheses. We omit the proof.

1.5 Proposition *Let S be a set with a binary operation $*$. If $e \in S$ is a left identity and $f \in S$ is a right identity, then $e = f$. In particular, there exists at most one identity element in S.*

Proof Since e is a left identity, we have $e * f = f$. And since f is a right identity, we also have $e * f = e$. Thus, $e = e * f = f$. $\square$

1.6 Remark Identity elements are usually denoted by 1 (resp. 0), if the binary operation is denoted by $*$, $\cdot$, $\bullet$, $\circ$ (resp. $+$).

1.7 Definition Let $(M, *)$ be a monoid and let $x \in M$. An element $y \in M$ is called a *left* (resp. *right*) *inverse* of x if $y * x = 1$ (resp. $x * y = 1$). If y is a left and right inverse of x, then y is called an *inverse* of x. If x has an inverse, we call x an *invertible* element of M.

1.8 Proposition *Let $(M, *)$ be a monoid and let $x \in M$. If $y \in M$ is a left inverse of x and $z \in M$ is a right inverse of x, then $y = z$. In particular, every element of M has at most one inverse.*

Proof We have $y = y * 1 = y * (x * z) = (y * x) * z = 1 * z = z$. $\square$

1.9 Remark If x is an invertible element in a monoid, then we denote its (unique) inverse by x^{-1} (resp. $-x$), if the binary operation is denoted by $*$, $\cdot$, $\bullet$, $\circ$ (resp. $+$).

1.10 Example Let

$$M := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\}.$$

M is a non-commutative monoid under matrix multiplication. The element $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ has an inverse if and only if $a, c \in \{\pm 1\}$. In this case, one has

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} a & -abc \\ 0 & c \end{pmatrix}.$$

(Verify!)

1.11 Proposition *Let $(M, *)$ be a monoid and let $x, y \in M$.*

(a) *If x is invertible, then also x^{-1} is invertible with $(x^{-1})^{-1} = x$.*

(b) *If x and y are invertible, then also $x * y$ is invertible with inverse $y^{-1} * x^{-1}$.*

(c) *The identity element 1 is invertible with $1^{-1} = 1$.*

Proof (a) Since $x * x^{-1} = 1 = x^{-1} * x$, the element x is a left and right inverse of x^{-1}.

(b) We have $(x*y)*(y^{-1}*x^{-1}) = ((x*y)*y^{-1})*x^{-1} = (x*(y*y^{-1}))*x^{-1} = (x * 1) * x^{-1} = x * x^{-1} = 1$, and similarly, we have $(y^{-1} * x^{-1}) * (x * y) = 1$. This implies that $y^{-1} * x^{-1}$ is a left and right inverse of $x * y$.

(c) This follows from the equation $1 * 1 = 1$. $\square$

1.12 Definition In a semigroup S we set $x^n := x * \cdots * x$ (n factors) for any $x \in S$ and $n \in \mathbb{N}$. If S is a monoid we also define $x^0 := 1$ for all $x \in S$. If additionally x is invertible, we define $x^{-n} := x^{-1} * \cdots * x^{-1}$ (n factors) for any $n \in \mathbb{N}$.

1.13 Remark For an element x in a semigroup (resp. monoid) one has

$$x^m * x^n = x^{m+n} \quad \text{and} \quad (x^m)^n = x^{mn},$$

for all $m, n \in \mathbb{N}$ (resp. all $m, n \in \mathbb{N}_0$). If x is an invertible element in a monoid, these rules hold for all $m, n \in \mathbb{Z}$. This can be proved by distinguishing the cases that m, n are positive, negative or equal to 0.

Moreover, if x and y are elements in a commutative semigroup (resp. monoid) then

$$(x * y)^n = x^n * y^n \quad \text{for all } n \in \mathbb{N} \text{ (resp. all } n \in \mathbb{N}_0).$$

If x and y are invertible elements in a commutative monoid, this holds for all $n \in \mathbb{Z}$.

Exercises for Section 1

1. Determine the invertible elements of the monoids among the examples in 1.2.

2. Prove the statement in Example 1.10.

3. Let S be the set of all matrices

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$$

with entries $a, b \in \mathbb{Z}$. Show that S is a semigroup under matrix multiplication and show that S has a right identity but no left identity. Determine all right identities. Give an example of a semigroup which has a left identity but no right identity.

4. Let G be a semigroup which has a left identity element e such that every element of G has a left inverse with respect to e, i.e., for every $x \in G$ there exists an element $y \in G$ with $yx = e$. Show that e is an identity element and that each element of G is invertible. (In other words, G is a *group*; see Section 2 for a definition.)

5. (a) Let S, T, U, and V be sets and let $X \subseteq S \times T$, $Y \subseteq T \times U$, and $Z \subseteq U \times V$ be subsets. Define

$$X * Y := \{(s, u) \in S \times U \mid \exists t \in T: \ (s, t) \in X \text{ and } (t, u) \in Y\} \subseteq S \times U.$$

Show that

$$(X * Y) * Z = X * (Y * Z).$$

(b) Let S be a set. Show that $(\mathcal{P}(S \times S), *)$ is a monoid. Is it commutative?

(c) What are the invertible elements in the monoid of Part (b)?

Digression into category theory

Definition A *category* $\mathcal{C}$ is a mathematical structure consisting of

- a class of *objects*, denoted by $\mathrm{Ob}(\mathcal{C})$,
- for any two objects $X, Y \in \mathrm{Ob}(\mathcal{C})$, a set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$, called the *morphisms* from X to Y,
- and for any three objects $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$, a function

  $$\mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)\,, \quad (g, f) \mapsto g \circ f\,,$$

  called *composition*,

satisfying the following axioms:

(i) Associativity of composition: For all $W, X, Y, Z \in \mathrm{Ob}(\mathcal{C})$ and all $f \in \mathrm{Hom}_{\mathcal{C}}(W, X)$, $g \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $h \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$, one has

$$(h \circ g) \circ f = h \circ (g \circ f)\,.$$

(ii) For every $X \in \mathrm{Ob}(\mathcal{C})$ there exists a morphism id_X (called the *identity morphism of* X), with the property that for all $W, Y \in \mathrm{Ob}(\mathcal{C})$ and all $f \in \mathrm{Hom}_{\mathcal{C}}(W, X)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, one has

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

(iii) If X, Y, X', Y' are objects of $\mathcal{C}$ and $(X, Y) \neq (X', Y')$ then $\mathrm{Hom}_{\mathcal{C}}(X, Y) \cap \mathrm{Hom}_{\mathcal{C}}(X', Y') = \emptyset$.

If $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ then X is called the *source* or *domain* of f and Y is called the *target* or *codomain* of f. By (iii), every morphism has a unique source object and a unique target object.

6. (a) Show that if $\mathcal{C}$ is a category and X is an object of $\mathcal{C}$ then $\mathrm{Hom}_{\mathcal{C}}(X, X)$ is a monoid under $\circ$.

(b) Show that the following examples form categories:

(i) The category Set of sets, whose objects are the sets, whose morphisms are the functions between two sets, and whose composition is the usual composition of functions.

(ii) The category Semigr of semigroups, whose objects are semigroups, whose morphisms are functions $f\colon X \to Y$ between semigroups X and Y which respect the binary operations of X and Y (i.e., $f(xx') = f(x)f(x')$ for all $x, x' \in X$), and the usual composition of functions.

(iii) The category Mon of monoids, whose objects are monoids, whose morphisms are functions $f\colon X \to Y$ between monoids X and Y that respect the binary operations (as in (ii)) and identity elements (i.e., $f(1_X) = 1_Y$), and the usual composition of functions.

(iv) The category $\widetilde{\mathsf{Set}}$, whose objects are sets, whose morphisms are given by $\mathrm{Hom}_{\widetilde{\mathsf{Set}}}(T, S) := \mathcal{P}(S \times T)$, and whose composition is the $*$-product from Exercise 5.

Notation A morphism $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ is often depicted as arrow $f\colon X \to Y$, although it does not need to be a function (as for instance in 6(b)(iv)). Often the composition symbol '$\circ$' is omitted and one writes gf instead of $g \circ f$ if the meaning is clear from the context.

2 Groups

From now on through the rest of this chapter we will usually write abstract binary operations in the multiplicative form $(x, y) \mapsto xy$ and denote identity elements by 1.

2.1 Definition A *group* is a monoid in which every element is invertible. A group is called *abelian* if it is commutative. The *order* of a group G is the number of its elements. It is denoted by $|G|$.

2.2 Remark If G is a semigroup with a left (resp. right) identity e and if every element of G has a left (resp. right) inverse with respect to e, then G is a group. (see Exercise 4 of Section 1.)

2.3 Examples (a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups, but $(\mathbb{N}_0, +)$ is not a group.

(b) $(\mathbb{Q} \smallsetminus \{0\}, \cdot)$, $(\mathbb{R} \smallsetminus \{0\}, \cdot)$, $(\mathbb{C} \smallsetminus \{0\}, \cdot)$ are abelian groups, but $(\mathbb{Z} \smallsetminus \{0\}, \cdot)$ and $(\mathbb{Q}, \cdot)$ are not groups.

(c) $(\{1\}, \cdot)$ and $(\{0\}, +)$ are groups of order 1. A group of order 1 is called a *trivial group*.

(d) For any set X, the set $\mathrm{Sym}(X) := \{f : X \to X \mid f \text{ is bijective}\}$ is a group under composition. It is called the *symmetric group on* X. Its elements are called *permutations* of X. If $|X| = n$, then $|\mathrm{Sym}(X)| = n!$. We write $\mathrm{Sym}(n)$ instead of $\mathrm{Sym}(\{1, 2, \ldots, n\})$ and call $\mathrm{Sym}(n)$ the *symmetric group of degree* n. We use the following notation for $\pi \in \mathrm{Sym}(n)$:

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}.$$

So if, for instance, π and ρ are elements of $\mathrm{Sym}(3)$ given by

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

then

$$\pi\rho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

(e) If $G_1, G_2, \ldots, G_n$ are groups, then also their *direct product*

$$G_1 \times G_2 \times \cdots \times G_n$$

is a group under the binary operation defined by

$$(x_1, \dots, x_n)(y_1, \dots, y_n) := (x_1 y_1, \dots, x_n y_n) .$$

(f) For every $n \in \mathbb{N}$, the sets $\mathrm{GL}_n(\mathbb{Q})$, $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$ of invertible matrices with entries in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, respectively, form groups under multiplication.

2.4 Definition Let G and H be groups. A function $f\colon G \to H$ is called a *homomorphism*, if $f(xy) = f(x)f(y)$ for all $x, y \in G$. The set of all homomorphisms from G to H is denoted by $\mathrm{Hom}(G, H)$. A homomorphism $f\colon G \to H$ is called

(a) a *monomorphism* if f is injective,
(b) an *epimorphism* if f is surjective,
(c) an *isomorphism* if f is bijective (often indicated by $f\colon G \xrightarrow{\sim} H$),
(d) an *endomorphism* if $G = H$,
(e) an *automorphism* if $G = H$ and f is bijective.

2.5 Remark Let $f\colon G \to H$ be a homomorphism between groups G and H. Then $f(1_G) = 1_H$ and $f(x^{-1}) = f(x)^{-1}$ for all $x \in G$. Moreover, if also $g\colon H \to K$ is a homomorphism between H and a group K, then $g \circ f\colon G \to K$ is a homomorphism. If $f\colon G \to H$ is an isomorphism, then also its inverse $f^{-1}\colon H \to G$ is an isomorphism. The automorphisms $f\colon G \to G$ form again a group under composition, called the *automorphism group* of G and denoted by $\mathrm{Aut}(G)$.

2.6 Examples (a) For each $n \in \mathbb{N}$, the function $(\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $k \mapsto nk$, is a monomorphism.

(b) $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, $x \mapsto e^x$, is an isomorphism.

(c) Let G be a group and let $g \in G$. Then $c_g\colon G \to G$, $x \mapsto gxg^{-1}$, is an automorphism of G with inverse $c_{g^{-1}}$. One calls c_g the *inner automorphism induced by* g (or *conjugation with* g). Note that $c_g \circ c_h = c_{gh}$ for $g, h \in G$. Thus, $G \to \mathrm{Aut}(G)$, $g \mapsto c_g$, is a group homomorphism.

(d) For each $n \in \mathbb{N}$, the sign map

$$\mathrm{sgn}\colon \mathrm{Sym}(n) \to (\{\pm 1\}, \cdot) , \quad \pi \mapsto \prod_{1 \leqslant i < j \leqslant n} \frac{\pi(j) - \pi(i)}{j - i} ,$$

is a homomorphism (see Exercise 2). To see that $\mathrm{sgn}(\pi) \in \{\pm 1\}$, let $\mathcal{P}_n^{(2)}$ denote the set of all subsets $\{i,j\}$ of $\{1,\ldots,n\}$ of cardinality 2 and note that

$$|\mathrm{sgn}(\pi)| = \prod_{\{i,j\}\in\mathcal{P}_n^{(2)}} \frac{|\pi(j)-\pi(i)|}{|j-i|} = \frac{\prod_{\{i,j\}\in\mathcal{P}_n^{(2)}} |\pi(j)-\pi(i)|}{\prod_{\{i,j\}\in\mathcal{P}_n^{(2)}} |j-i|} = 1\,,$$

since, for fixed $\pi \in \mathrm{Sym}(n)$, the function $\mathcal{P}_n^{(2)} \to \mathcal{P}_n^{(2)}$, $\{i,j\} \mapsto \{\pi(i),\pi(j)\}$, is a bijection. If $\mathrm{sgn}(\pi) = 1$ (resp. $\mathrm{sgn}(\pi) = -1$), then we call π an *even* (resp. *odd*) permutation.

(e) For every $n \in \mathbb{N}$, the determinant map $\det\colon \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \smallsetminus \{0\}, \cdot)$ is an epimorphism.

2.7 Definition Two groups G and H are called *isomorphic*, if there exists an isomorphism $f\colon G \xrightarrow{\sim} H$. In this case we write $G \cong H$.

2.8 Remark (a) The relation $\cong$ ('is isomorphic to') is an equivalence relation, i.e., for groups G, H, K we have:

(i) $G \cong G$.

(ii) If $G \cong H$ then $H \cong G$.

(iii) If $G \cong H$ and $H \cong K$ then $G \cong K$.

(b) Isomorphic groups G and H behave identically in all respects. In fact, if $f\colon G \xrightarrow{\sim} H$ is an isomorphism, every statement about G can be translated into a statement about H using f, and vice-versa. G and H are basically the same group: one arises from the other by renaming the elements using f, but keeping the multiplication.

2.9 Definition Let G be a group. A subset H of G is a called a *subgroup* of G if the following hold:

(i) If $x, y \in H$ then $xy \in H$.

(ii) $1_G \in H$.

(iii) If $x \in H$ then x^{-1} in H.

In this case, H together with the restricted binary operation $H \times H \to H$, $(x,y) \mapsto xy$, is again a group. We write $H \leqslant G$, if H is a subgroup of G. A subgroup H of G is called a *proper subgroup*, if $H \neq G$. In this case we write $H < G$.

2.10 Proposition *Let G be a group and let H be a subset of G. Then the following are equivalent:*

(i) *H is a subgroup of G.*

(ii) *H is non-empty and if $x, y \in H$ then also $xy^{-1} \in H$.*

Proof Exercise 3. $\square$

2.11 Examples (a) For each group G one has $\{1_G\} \leqslant G$ and $G \leqslant G$. The subgroup $\{1_G\}$ is called the *trivial subgroup* of G.

(b) If $H \leqslant G$ and $K \leqslant H$ then $K \leqslant G$. Also, if $K \subseteq H \leqslant G$ and $K \leqslant G$ then $K \leqslant H$.

(c) The intersection of any collection of subgroups of a group G is again a subgroup. (Warning: In general, the union of subgroups is not a subgroup.)

(d) $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are subgroups of $(\mathbb{C}, +)$.

(e) For any non-empty subsets $X_1, X_2, \ldots, X_n$ of a group G we define

$$X_1 X_2 \cdots X_n := \{x_1 x_2 \cdots x_n \mid x_1 \in X_1, \ldots, x_n \in X_n\}\,.$$

In general, this is not a subgroup, even if $X_1, \ldots, X_n$ are. For subgroups $H, K \leqslant G$ one has (see Exercise 4):

$$HK \leqslant G \iff KH = HK\,.$$

In any case, if H and K are finite subgroups one has (see Excercise 5):

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}\,.$$

(f) If X is a non-empty subset of a group G, its *normalizer* is defined as

$$N_G(X) := \{g \in G \mid gXg^{-1} = X\}\,.$$

Note that $gXg^{-1} = X \iff c_g(X) = X \iff gX = Xg$. One always has $N_G(X) \leqslant G$.

Moreover, the *centralizer* of X is defined as

$$C_G(X) := \{g \in G \mid gxg^{-1} = x \text{ for all } x \in X\}\,.$$

Note that $g \in C_G(X) \iff c_g$ is the identity on $X \iff gx = xg$ for all $x \in X$. It is easy to check that $C_G(X) \leqslant N_G(X)$ is again a subgroup. If $X = \{x\}$ consists only of one element we also write $C_G(x)$ instead of $C_G(\{x\})$.

(g) The subgroup $Z(G) := C_G(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$ is called the *center* of G. It is an abelian subgroup.

(h) If $f\colon G \to H$ is a group homomorphism and if $U \leqslant G$ and $V \leqslant H$, then $f(U) \leqslant H$ and $f^{-1}(V) := \{g \in G \mid f(g) \in V\} \leqslant G$. In particular, the *image of* f, $\mathrm{im}(f) := f(G)$, is a subgroup of H, and the *kernel of* f, $\ker(f) := f^{-1}(\{1_H\})$ is a subgroup of G. Note: f is injective if and only if $\ker(f) = 1$. (See Exercise 7.)

The kernel of $\mathrm{sgn}\colon \mathrm{Sym}(n) \to \{\pm 1\}$ is called the *alternating group of degree* n and is denoted by $\mathrm{Alt}(n)$.

The kernel of $\det\colon \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \smallsetminus \{0\}, \cdot)$ is called the *special linear group of degree* n over $\mathbb{R}$ and is denoted by $\mathrm{SL}_n(\mathbb{R})$.

2.12 Theorem *The subgroups of* $(\mathbb{Z}, +)$ *are the subsets of the form* $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ *for* $n \in \mathbb{N}_0$.

Proof For every $n \in \mathbb{Z}$, the function $\mathbb{Z} \to \mathbb{Z}$, $k \mapsto kn$, is a group homomorphism (cf. Example 2.6(a)) with image $n\mathbb{Z}$. By Example 2.11(h), it is a subgroup of $\mathbb{Z}$.

Conversely, assume that $H \leqslant \mathbb{Z}$. If $H = \{0\}$, then $H = 0\mathbb{Z}$ and we are done. So assume that $H \neq \{0\}$. Then H contains a non-zero integer and with it its inverse. So, H contains a positive integer. Let n be the smallest positive integer contained in H. We will show that $H = n\mathbb{Z}$. First, since $n \in H$ also $n+n, n+n+n, \ldots \in H$. Since H is a subgroup also the inverses of these elements, namely $-n, -n+(-n), \ldots$ are in H. Thus, $n\mathbb{Z} \leqslant H$. To show the other inclusion, take an arbitrary element h of H and write it as $h = qn+r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. Then we have $r = h - qn \in H$ which implies $r = 0$ (by the minimality of n). This shows that $h = qn \in n\mathbb{Z}$. So, $H \leqslant n\mathbb{Z}$. $\square$

2.13 Definition Let G be a group and let $X \subseteq G$ be a subset.

(a) The *subgroup generated by* X is defined as

$$\langle X \rangle := \{x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} \mid k \in \mathbb{N},\ x_1, \ldots, x_k \in X,\ \epsilon_1, \ldots, \epsilon_k \in \{\pm 1\}\}\,.$$

If $X = \emptyset$ one defines $\langle X \rangle := \{1_G\}$. Clearly, $\langle X \rangle$ is a subgroup of G. Moreover, if U is a subgroup of G which contains X then U also contains $\langle X \rangle$. Thus, $\langle X \rangle$ is characterized as the the smallest subgroup of G which contains X.

Moreover, one has

$$\langle X\rangle = \bigcap_{X\subseteq U\leqslant G} U\,,$$

i.e., $\langle X\rangle$ is the intersection of all subgroups of U that contain X.

(b) If $\langle X\rangle = G$, then we call X a *generating set* or a *set of generators* of G. If G is generated by a single element, then G is called *cyclic*.

2.14 Examples (a) Let G be a group and let $x, y \in G$. The element $[x, y] := xyx^{-1}y^{-1}$ is called the *commutator* of x and y. One has $xy = [x, y]yx$. Thus, $[x, y] = 1$ if and only if $xy = yx$, i.e., x and y commute. The subgroup of G generated by all the commutators $[x, y]$, $x, y \in G$, is called the *commutator subgroup* (or the *derived subgroup*) of G and it is denoted by G' or $[G, G]$. Note that $[x, y]^{-1} = [y, x]$. Therefore,

$$G' = \{[x_1, y_1]\cdots[x_k, y_k] \mid k \in \mathbb{N},\ x_1, \ldots, x_k, y_1, \ldots, y_k \in G\}\,.$$

Note that

$$G' = \{1\} \iff G \text{ is abelian} \iff Z(G) = G\,.$$

(b) The elements

$$x = \begin{pmatrix} 1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix} \qquad y = \begin{pmatrix} 1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix}$$

generate a subgroup V_4 of $\mathrm{Sym}(4)$, which is called the *Klein 4-group*. One checks easily that $x^2 = 1$, $y^2 = 1$ and

$$xy = yx = \begin{pmatrix} 1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix} =: z\,.$$

This shows that $V_4 = \{1, x, y, z\}$ and we obtain the following multiplication table:

	1	x	y	z
1	1	x	y	z
x	x	1	z	y
y	y	z	1	x
z	z	y	x	1

2.15 Definition Let G be a group and let $H \leqslant G$. For $x, y \in G$ we define $x \mathrel{{}_H{\sim}} y$ if $x^{-1}y \in H$. This defines an equivalence relation on G (verify). The equivalence class containing $x \in G$ is equal to xH (verify) and is called the *left coset* of H containing x. The set of equivalence classes is denoted by G/H. The number $|G/H|$ is called the *index* of H in G and is denoted by $[G : H]$.

2.16 Remark Let G be a group and let $H \leqslant G$. In a similar way one defines the relation $\underset{H}{\sim}$ on G by $x \underset{H}{\sim} y$ if $xy^{-1} \in H$. This is again an equivalence relation. The equivalence class of $x \in G$ is equal to Hx, the *right coset* of H containing x. The set of right cosets is denoted by $H\backslash G$. We will mostly work with left cosets. If G is abelian then $xH = Hx$ for all $x \in G$. However, in general this is not the case.

2.17 Example Fix $n \in \mathbb{N}_0$ and $k \in \mathbb{Z}$. Then the set $k + n\mathbb{Z}$ is a left and right coset of $n\mathbb{Z}$ in $(\mathbb{Z}, +)$. For example,

$$2 + 5\mathbb{Z} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}.$$

For this particular choice ($G = \mathbb{Z}$ and $H = n\mathbb{Z}$) we also write $x \equiv y \mod n$ instead of $x \,{}_{H}\!\sim y$ and say "x is *congruent* to y *modulo* n". The coset $k + n\mathbb{Z}$ is called the *congruence class* of k *modulo* n. One has

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

and $[\mathbb{Z} : n\mathbb{Z}] = n$.

2.18 Proposition *Let G be a group and let $H \leqslant G$.*

(a) *For each $g \in G$, the function $H \to gH$, $h \mapsto gh$, is a bijection. In particular, any two left cosets of H have the same cardinality, namely $|H|$.*

(b) *For each $g \in G$, the function $H \to Hg$, $h \mapsto hg$, is a bijection. In particular, any two right cosets of H have the same cardinality, namely $|H|$.*

(c) *The function $G/H \to H\backslash G$, $gH \mapsto Hg^{-1}$, is well-defined and bijective. In particular, $|G/H| = |H\backslash G|$.*

Proof (a) It is easy to verify that $gH \to H$, $x \mapsto g^{-1}x$, is an inverse.

(b) One verifies easily that $Hg \to H$, $x \mapsto xg^{-1}$, is an inverse.

(c) In order to show that the function is well-defined assume that $g_1, g_2 \in G$ such that $g_1H = g_2H$. We need to show that then $Hg_1^{-1} = Hg_2^{-1}$. But, we have: $g_1H = g_2H \iff g_1^{-1}g_2 \in H \iff Hg_1^{-1} = Hg_2^{-1}$. Finally, the function $H\backslash G \to G/H$, $Hg \mapsto g^{-1}H$, is an inverse. $\square$

2.19 Corollary (Lagrange 1736–1813) *Let H be a subgroup of a group G. Then*

$$|G| = [G : H] \cdot |H|$$

(with the usual rules for the quantity ∞). In particular, if G is a finite group then $|H|$ and $[G : H]$ are divisors of $|G|$.

Proof G is the disjoint union of the left cosets of H. There are $[G : H]$ such cosets, and each one has $|H|$ elements by Proposition 2.18(a). $\square$

2.20 Examples (a) The subgroups V_4 and $\mathrm{Alt}(4)$ of $\mathrm{Sym}(4)$ have order 4 and 12, which are divisors of 24 (in accordance with Lagrange's Theorem). By Lagrange, $\mathrm{Sym}(4)$ cannot have a subgroup of order 10. We will see later: $\mathrm{Alt}(4)$ does not have a subgroup of order 6, although 6 divides 12.

(b) Let G be a finite group whose order is a prime p. Then, by Lagrange, $\{1\}$ and G are the only subgroups of G. Moreover, G is cyclic, generated by any element $x \neq 1$. In fact, $H := \langle x \rangle$ is a subgroup of G with $1 < |H|$. Thus $H = G$.

Exercises for Section 2

1. Prove the statements in Remark 2.5.

2. Let $n \in \mathbb{N}$. For pairwise distinct elements $a_1, \ldots, a_k$ in $\{1, \ldots, n\}$ we denote by $(a_1, a_2, \ldots, a_k)$ the permutation $\sigma \in \mathrm{Sym}(n)$ given by $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$, and $\sigma(a) = a$ for all other $a \in \{1, \ldots, n\}$. Such an element is called a *k-cycle*. A 2-cycle is also called a *transposition*.

(a) Show that every element in $\mathrm{Sym}(n)$ is a product of disjoint cycles.

(b) Show that every cycle is a product of transpositions.

(c) Show that every transposition is a product of an odd number of *simple* transpositions, i.e., transpositions of the form $(i, i+1)$, $i = 1, \ldots, n-1$.

(d) Let $\sigma \in \mathrm{Sym}(n)$. A pair (i, j) of natural numbers i, j with $1 \leqslant i < j \leqslant n$ is called an *inversion* for σ if $\sigma(j) < \sigma(i)$. We denote by $l(\sigma)$ the number of inversions of σ. Show that for a transposition $\tau = (a, b)$ with $1 \leqslant a < b \leqslant n$ one has $l(\tau) = 2(b - a) - 1$.

(e) Show that for every $i = 1, \ldots, n-1$ one has

$$l((i, i+1)\sigma) - l(\sigma) = \begin{cases} 1 & \text{if } \sigma^{-1}(i) < \sigma^{-1}(i+1), \\ -1 & \text{if } \sigma^{-1}(i) > \sigma^{-1}(i+1). \end{cases}$$

(f) Show that if $\sigma \in \mathrm{Sym}(n)$ can be written as a product of r transpositions then $r \equiv l(\sigma) \mod 2$. Conclude that if σ can also be written as a product of s transpositions then $r \equiv s \mod 2$.

(g) Show that the function $\mathrm{Sym}(n) \to \{\pm 1\}$, $\sigma \mapsto (-1)^{l(\sigma)}$, is a group homomorphism which coincides with the homomorphism sgn from class and that $\mathrm{sgn}(\tau) = -1$ for every transposition τ.

3. Prove the statement in Proposition 2.10.

4. Let H and K be subgroups of a group G. Show that

$$HK \leqslant G \iff KH = HK\,.$$

5. Let H and K be finite subgroups of a group G. Show that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}\,.$$

Hint: Consider the function $f : H \times K \to HK$ given by $f(h, k) = hk$. Show that for every element $x \in HK$ there exist precisely $|H \cap K|$ elements $(h, k) \in H \times K$ with $hk = x$.

6. Show that for any non-empty subset X of a group G, the normalizer of X, $N_G(X)$, and the centralizer of X, $C_G(X)$, is again a subgroup of G. Show also that $C_G(X)$ is contained in $N_G(X)$.

7. Let $f\colon G \to H$ be a group homomorphism.

(a) If $U \leqslant G$ then $f(U) \leqslant H$.

(b) If $V \leqslant H$ then $f^{-1}(V) := \{g \in G \mid f(g) \in V\}$ is a subgroup of G. (The subgroup $f^{-1}(V)$ is also called the *preimage* of V under f. Note that the notation $f^{-1}(V)$ does not mean that f has an inverse.)

(c) Show that f is injective if and only if $\ker(f) = \{1\}$.

8. Let H be a subgroup of a group G.

(a) Show that the relation ${}_H\!\sim$ on G defined in Definition 2.15 is an equivalence relation.

(b) Show that the equivalence class of the element $g \in G$ with respect to ${}_H\!\sim$ is equal to gH.

9. Let G and A be groups and assume that A is abelian. Show that the set $\mathrm{Hom}(G, A)$ of group homomorphisms from G to A is again an abelian group under the multiplication defined by

$$(f_1 \cdot f_2)(g) := f_1(g) f_2(g) \quad \text{for } f_1, f_2 \in \mathrm{Hom}(G, A) \text{ and } g \in G.$$

10. Consider the elements $\sigma := (1, 2, 3)$ and $\tau := (1, 2)$ of Sym(3). Here we used the cycle notation from Exercise 2.

(a) Show that $\sigma^3 = 1$, $\tau^2 = 1$ and $\tau\sigma = \sigma^2\tau$.

(b) Show that $\{\sigma, \tau\}$ is a generating set of Sym(3).

(c) Show that every element of Sym(3) can be written in the form $\sigma^i\tau^j$ with $i \in \{0, 1, 2\}$ and $j \in \{0, 1\}$.

(d) Compute all subgroups of Sym(3) and their normalizers and centralizers.

(e) Compute the commutator subgroup of Sym(3) and the center of Sym(3).

11. Consider the elements $\sigma := (1, 2, 3, 4)$ and $\tau := (1, 4)(2, 3)$ of Sym(4).

(a) Show that $\sigma^4 = 1$, $\tau^2 = 1$, and $\tau\sigma = \sigma^3\tau$.

(b) Determine the subgroup $\langle\sigma, \tau\rangle$ of Sym(4). It is called the *dihedral group* of order 8 and is denoted by D_8.

(c) Determine $Z(D_8)$.

(d) Determine the derived subgroup D_8' of D_8.

12. Let G and H be groups and let $f\colon G \to H$ be an isomorphism.

(a) Show that G is abelian if and only if H is abelian.

(b) Let X be a subset of G and set $Y := f(X) \subseteq H$. Show that $f(\langle X\rangle) = \langle Y\rangle$, $f(N_G(X)) = N_H(Y)$, $f(C_G(X)) = C_H(Y)$.

(c) Show that G is cyclic if and only if H is cyclic.

(d) Show that $f(Z(G)) = Z(H)$.

(e) Show that $f(G') = H'$.

13. (Dedekind's Identity) Let U, V, W be subgroups of a group G with $U \leqslant W$. Show that

$$UV \cap W = U(V \cap W) \quad \text{and} \quad W \cap VU = (W \cap V)U\,.$$

14. (a) Let p be a prime, let $C_p = \langle x\rangle$ be a cyclic group of order p and set $G := C_p \times C_p$. Show that G has exactly $p + 1$ subgroups of order p.

(b) A group of 25 mathematicians meets for a 6 day conference. Between the morning and afternoon lectures they have their lunch in a room with 5 round tables and 5 chairs around each table. The organizer would like to assign every day new places at the tables in such a way that each participant has eaten with any other one at least once at the same table. Is this possible? (Hint: Use (a) and use convenient equivalence relations on G.)

More category theory

Definition Let $\mathcal{C}$ be a category and let $f\colon X \to Y$ be a morphism in $\mathcal{C}$.

(a) f is called a *monomorphism* if for all objects W of $\mathcal{C}$ and all $g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(W, X)$ one has

$$f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2 \,.$$

(b) f is called an *epimorphism* if for all objects Z of $\mathcal{C}$ and all $g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ one has

$$g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2 \,.$$

(c) f is called an *isomorphism* if there exists $g \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$ with $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.

Definition Let $\mathcal{C}$ be a category and X an object of $\mathcal{C}$.

(a) X is called an *initial object* in $\mathcal{C}$ if $|\mathrm{Hom}_{\mathcal{C}}(X, Y)| = 1$ for all objects Y of $\mathcal{C}$.

(b) X is called a *final object* in $\mathcal{C}$ if $|\mathrm{Hom}_{\mathcal{C}}(W, X)| = 1$ for all objects W of $\mathcal{C}$.

(c) X is called a *zero object* in $\mathcal{C}$ if it is an initial and final object in $\mathcal{C}$.

15. Prove the following statements for the category Set:

(a) A morphism $f\colon X \to Y$ is a monomorphism in Set if and only if f is injective.

(b) A morphism $f\colon X \to Y$ is an epimorphism in Set if and only if f is surjective.

(c) A morphism $f\colon X \to Y$ is an isomorphism in Set if and only if f is bijective.

(d) Does Set have an initial object? Does Set have a final object?

16. (a) Let $f\colon X \to S$ be a morphism of semigroups. Show that if X is a monoid (resp. group) then also $f(X)$ is a monoid (resp. group) with the binary operation restricted from S.

(b) Consider $\mathbb{N}_0$ and $\mathbb{Z}$ equipped with the binary operation $+$. Show that the inclusion $i\colon \mathbb{N}_0 \to \mathbb{Z}$ is an epimorphism in the category Semigr and also in the category Mon.

17. Prove the following statements for the category Gr, whose objects are the groups, whose morphisms are the group homomorphisms, and whose composition is the usual composition of functions.

(a) Gr has a zero object.

(b) A morphism $f\colon G \to H$ in Gr is a monomorphism if and only if it is injective.

Note: It is also true that a morphism $f\colon G \to H$ in Gr is an epimorphism if and only if f is surjective. But it is more difficult to prove. We will get back to that when we have more tools available.

Definition Two objects X and Y of a category $\mathcal{C}$ are called *isomorphic* if there exists an isomorphism $f\colon X \to Y$ in $\mathcal{C}$. Notation: $X \cong Y$.

18. Let $\mathcal{C}$ be a category.

(a) Show that if $f\colon X \to Y$ is an isomorphism in $\mathcal{C}$ then there exists precisely one morphism $g\colon Y \to X$ with the property $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. This morphism will be denoted by f^{-1} and called the *inverse* of f.

(b) Show that if $f\colon X \to Y$ and $g\colon Y \to Z$ are isomorphisms in $\mathcal{C}$ then also $g \circ f$ is an isomorphism in $\mathcal{C}$.

(c) Let X be an object of $\mathcal{C}$. An isomorphism $f\colon X \to X$ in $\mathcal{C}$ is called an *automorphism* of X. Show that the set $\mathrm{Aut}_{\mathcal{C}}(X)$ of automorphisms of X is a group under composition.

(d) Show that if X and Y are initial (resp. final) objects of $\mathcal{C}$ then $X \cong Y$.

3 Normal Subgroups and Factor Groups

3.1 Theorem *Let G be a group, let N be a subgroup of G, and let $\nu\colon G \to G/N$ denote the function defined by $\nu(g) := gN$. Then the following are equivalent:*

(i) *G/N is a group under $(g_1N, g_2N) \mapsto (g_1N)(g_2N)$, where $(g_1N)(g_2N)$ is defined as the product of the subsets g_1N and g_2N of G as in Example 2.11(e).*

(ii) *G/N has a group structure such that the function ν is a homomorphism.*

(iii) *There exists a group H and a group homomorphism $f\colon G \to H$ such that* $\ker(f) = N$.

(iv) *$gNg^{-1} \subseteq N$ for all $g \in G$.*

(v) *$gNg^{-1} = N$ for all $g \in G$.*

(vi) *$gN = Ng$ for all $g \in G$.*

Proof (i)$\Rightarrow$(ii): Use the group structure defined in (i). We need to show that ν is a homomorphism. For $g_1, g_2 \in G$ we have $\nu(g_1)\nu(g_2) = (g_1N)(g_2N)$ which must be again a left coset by (i). But $(g_1N)(g_2N)$ contains the element g_1g_2. This implies that $(g_1N)(g_2N) = (g_1g_2)N$. Thus, $\nu(g_1)\nu(g_2) = (g_1N)(g_2N) = (g_1g_2)N = \nu(g_1g_2)$, and ν is a homomorphism.

(ii)$\Rightarrow$(iii): Set $H := G/N$, which has a group structure, by (ii), such that $f := \nu$ is a homomorphism. Moreover, since ν is a homomorphism, $\nu(1) = N$ must be the identity element of G/N. Thus, $\ker(\nu) = \{g \in G \mid gN = N\} = N$.

(iii)$\Rightarrow$(iv): For each $g \in G$ and each $n \in N$ one has

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \cdot 1 \cdot f(g)^{-1} = 1$$

which shows that $gng^{-1} \in \ker(f) = N$. Thus $gNg^{-1} \subseteq N$ for all $g \in G$.

(iv)$\Rightarrow$(v): Let $g \in G$. Then, (iv) applied to the element g^{-1} yields $g^{-1}Ng \subseteq N$. Applying c_g then implies $N = gg^{-1}Ngg^{-1} \subseteq gNg^{-1}$. Together with (iv) for g we obtain (v) for g.

(v)$\Rightarrow$(vi): For each $g \in G$ we have $gN = gNg^{-1}g \overset{(v)}{=} Ng$.

(vi)$\Rightarrow$(i): For any $g_1, g_2 \in G$ we have

$$(g_1N)(g_2N) \overset{\text{(vi)}}{=} g_1g_2NN = g_1g_2N \tag{3.1.a}$$

so that $(g_1N, g_2N) \mapsto (g_1N)(g_2N)$ is a binary operation on G/N. Obviously, it is associative. Moreover, by (3.1.a), $N = 1 \cdot N$ is an identity element, and for any $g \in G$, $g^{-1}N$ is an inverse of gN. $\square$

3.2 Definition If the conditions (i)–(vi) in Theorem 3.1 are satisfied, we call N a *normal* subgroup of G and write $N \trianglelefteq G$. We write $N \triangleleft G$, if N is a proper normal subgroup of G. If $N \trianglelefteq G$ then (i) and (vi) in the previous theorem imply that the set G/N of left cosets is again a group under the binary operation

$$(g_1N, g_2N) \mapsto (g_1N)(g_2N) = g_1g_2NN = g_1g_2N\,.$$

It is called the *factor group* of G with respect to N, or shorter 'G modulo N'. Moreover, by the proof of (i)$\Rightarrow$(ii), the function $\nu\colon G \to G/N$, $g \mapsto gN$, is a homomorphism, called the *canonical epimorphism* or *natural epimorphism.*

3.3 Examples (a) We always have $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$. If G and $\{1\}$ are the only normal subgroups of G and if $G \neq \{1\}$, we call G a *simple* group. By Lagrange's Theorem, groups of prime order are always simple. If G is not simple, there exists $\{1\} < N \triangleleft G$ and we think of G as being built from the two groups N and G/N. This is often depicted as

$$\begin{array}{|c|}\hline G/N \\ \hline N \\ \hline \end{array} \qquad \text{or} \qquad \begin{array}{rccl} & & \bullet & G \\ G/N & \{ & | & \\ & & \bullet & N \\ N \cong N/\{1\} & \{ & | & \\ & & \bullet & \{1\} \end{array}$$

We may think of G/N as an approximation to G. An element of G/N determines an element of G up to an error term in N, and the multiplication in G/N determines the multiplication in G up to an error term in N.

(b) If G is a group and $H \leqslant Z(G)$, then $H \trianglelefteq G$. In particular, $Z(G) \trianglelefteq G$. In an abelian group G, every subgroup is normal (since $G = Z(G)$). The center of G is even more special. For every $f \in \mathrm{Aut}(G)$ one has $f(Z(G)) = Z(G)$ (verify!). A subgroup $N \leqslant G$ with $f(N) = N$ for all $f \in \mathrm{Aut}(G)$ is called *characteristic* in G. In this case we write $N \underset{\text{char}}{\trianglelefteq} G$. Note that $N \underset{\text{char}}{\trianglelefteq} G$ implies that $N \trianglelefteq G$ (since $c_g \in \mathrm{Aut}(G)$ for all $g \in G$).

(c) Let G be a group and let $G' \leqslant H \leqslant G$, where G' denotes the commutator subgroup of G, cf. Example 2.14(a). Then $H \trianglelefteq G$ and G/H is abelian. In fact, for any $g \in G$ and $h \in H$ one has

$$ghg^{-1} = ghg^{-1}h^{-1}h = [g,h]h \in G'H \leqslant H\,,$$

and for any $x, y \in G$ one has

$$(xH)(yH) = xyH = xy[y^{-1}, x^{-1}]H = yxH = (yH)(xH)\,.$$

Here, the second equality holds, since $[y^{-1}, x^{-1}] \in H$. In particular, with $H = G'$, we obtain that G' is normal in G and that G/G' is abelian.

Conversely, if N is a normal subgroup of G with abelian factor group G/N, then $G' \leqslant N \leqslant G$. In fact, let $x, y \in G$. Then one has

$$[x,y]N = xyx^{-1}y^{-1}N = (xN)(yN)(x^{-1}N)(y^{-1}N) = [xN, yN] = N\,,$$

which implies that $[x,y] \in N$. Thus, we have $G' \leqslant N$.

The above two considerations show that G' is the smallest (with respect to inclusion) normal subgroup of G with abelian factor group. This factor group G/G' is called the *commutator factor group* of G and it is denoted by G^{ab}.

(d) If $H \leqslant G$ with $[G:H] = 2$ then $H \triangleleft G$. In fact, for $g \in H$ we have $gH = H = Hg$, and for $g \in G \smallsetminus H$ we have $gH = G \smallsetminus H = Hg$, since there are only two left cosets and two right cosets and one of them is H.

(e) For every subgroup H of G one has $H \trianglelefteq N_G(H) \leqslant G$. Moreover, $N_G(H) = G$ if and only if $H \trianglelefteq G$.

(f) For each subset X of a group G one has $C_G(X) \trianglelefteq N_G(X)$ (see Exercises). In particular, setting $X = G$, we obtain again $Z(G) \trianglelefteq G$.

(g) For each $n \in \mathbb{N}$ one has $\mathrm{Alt}(n) = \ker(\mathrm{sgn}) \trianglelefteq \mathrm{Sym}(n)$.

(h) For each $n \in \mathbb{N}$ one has $\mathrm{SL}_n(\mathbb{R}) = \ker(\det) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$.

(i) Let $G := \mathrm{Sym}(3)$ and let

$$H := \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Then $H \ntrianglelefteq G$, since

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H\,.$$

3.4 Theorem (Fundamental Theorem of Homomorphisms, Universal Property of $\nu\colon G \to G/N$) *Let G be a group, $N \trianglelefteq G$, and let $\nu\colon G \to G/N$, $g \mapsto gN$, denote the natural epimorphism.*

For every homomorphism $f\colon G \to H$ with $N \leqslant \ker(f)$, there exists a unique homomorphism $\overline{f}\colon G/N \to H$ such that $\overline{f} \circ \nu = f$:

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\nu"'] & H \\ G/N \arrow[ur, dotted, "\overline{f}"'] & \end{tikzcd}$$

Moreover, $\ker(\overline{f}) = \{aN \mid a \in \ker(f)\} = \ker(f)/N$ *and* $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$.

Proof (a) Existence: Let $a, b \in G$ with $aN = bN$. Then $a^{-1}b \in N$ and $f(b) = f(aa^{-1}b) = f(a)f(a^{-1}b) = f(a)$, since $N \leqslant \ker(f)$. Therefore, the function $\overline{f}\colon G/N \to H$, $aN \mapsto f(a)$, is well-defined. It is a homomorphism, since

$$\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN)\,,$$

for all $a, b \in G$. Moreover, for all $a \in G$, we have $\overline{f}(\nu(a)) = \overline{f}(aN) = f(a)$. Thus, $\overline{f} \circ \nu = f$.

(b) Uniqueness: If also $\tilde{f}\colon G/N \to H$ satisfies $\tilde{f} \circ \nu = f$, then $\tilde{f}(aN) = (\tilde{f} \circ \nu)(a) = (\overline{f} \circ \nu)(a) = \overline{f}(aN)$, for all $a \in G$. Thus $\tilde{f} = \overline{f}$.

(c) For all $a \in G$ we have

$$aN \in \ker(\overline{f}) \iff \overline{f}(aN) = 1 \iff f(a) = 1 \iff a \in \ker(f)\,.$$

Therefore, $\ker(\overline{f}) = \{aN \in G/N \mid a \in \ker(f)\} = \ker(f)/N$.

Finally, $\mathrm{im}(\overline{f}) = \{\overline{f}(aN) \mid a \in G\} = \{f(a) \mid a \in G\} = \mathrm{im}(f)$. $\square$.

3.5 Remark (a) Assume the notation of Theorem 3.4. Note that $\nu\colon G \to G/N$ has the property that $N \leqslant \ker(f)$, or equivalently that $\nu(N) = \{1\}$. The homomorphism ν is *universal with this property* in the sense that every other homomorphism $f\colon G \to H$ with the property $f(N) = \{1\}$ can be factored in a unique way through ν.

(b) In the situation of Theorem 3.4 we also say that f *induces* the homomorphism $\overline{f}$.

3.6 Corollary *Let $f\colon G \to H$ be a homomorphism. Then f induces an isomorphism $\overline{f}\colon G/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$. If f is an epimorphism then $G/\ker(f) \cong H$.*

Proof This follows immediately from Theorem 3.4, choosing $N := \ker(f)$. Note that $\overline{f}$ is injective, since $\ker(\overline{f}) = \ker(f)/\ker(f) = \{\ker(f)\} = \{1_{G/\ker(f)}\}$ is the trivial subgroup of $G/\ker(f)$. $\square$

3.7 Example For $n \geqslant 2$, the sign homomorphism $\mathrm{sgn}\colon \mathrm{Sym}(n) \to \{\pm 1\}$ is surjective with kernel $\mathrm{Alt}(n)$. By the Fundamental Theorem of Homomorphisms, we obtain an isomorphism $\mathrm{Sym}(n)/\mathrm{Alt}(n) \cong \{\pm 1\}$. In particular, $[\mathrm{Sym}(n) : \mathrm{Alt}(n)] = 2$ and $|\mathrm{Alt}(n)| = n!/2$ by Lagrange's Theorem, Corollary 2.19.

Before we state the next theorem, note that the additive groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ (for $n \in \mathbb{N}$) are cyclic, generated by 1 and $1 + n\mathbb{Z}$, respectively. The next theorem shows that, up to isomorphism, there are no other cyclic groups.

3.8 Theorem (Classification of cyclic groups) *Let G be a cyclic group generated by the element $g \in G$.*

(a) *If G is infinite then $G \cong \mathbb{Z}$, $G = \{g^k \mid k \in \mathbb{Z}\}$ and, for all $i, j \in \mathbb{Z}$, one has $g^i = g^j$ if and only if $i = j$.*

(b) *If G is of finite order n then $G \cong \mathbb{Z}/n\mathbb{Z}$, $G = \{1, g, g^2, \ldots, g^{n-1}\}$ and, for all $i, j \in \mathbb{Z}$, one has $g^i = g^j$ if and only if $i \equiv j \mod n$.*

Proof We consider the function $f\colon \mathbb{Z} \to G$, $k \mapsto g^k$. It is a homomorphism, since $g^k g^l = g^{k+l}$ for all $k, l \in \mathbb{Z}$. We have $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ which implies that f is an epimorphism. By Theorem 2.12 we have $\ker(f) = n\mathbb{Z}$ for some $n \in \mathbb{N}_0$. By Theorem 3.4 we obtain an isomorphism $\overline{f}\colon \mathbb{Z}/n\mathbb{Z} \to G$, $k + n\mathbb{Z} \mapsto g^k$. This implies that G is infinite if and only if $n = 0$. Now all the assertions follow from considering the isomorphism $\overline{f}$. $\square$

3.9 Theorem (Fermat, 1601–1665) *Let G be a finite group, let $g \in G$ and let $k \in \mathbb{Z}$. Then $g^k = 1$ if and only if $|\langle g \rangle|$ divides k. In particular, $g^{|G|} = 1$.*

Proof Since G is finite, the order of $\langle g \rangle$ is finite. Applying Theorem 3.8(b) to the cyclic group $\langle g \rangle$, we obtain

$$g^k = 1 \iff g^k = g^0 \iff k \equiv 0 \mod |\langle g \rangle| \iff |\langle g \rangle| \text{ divides } k\,.$$

$\square$

3.10 Definition Let G be a group and let $g \in G$. One calls $|\langle g \rangle| \in \mathbb{N} \cup \{\infty\}$ the *order* of g and denotes it by $o(g)$. If $o(g)$ is finite then, by Theorem 3.9, we have $o(g) = \min\{n \in \mathbb{N} \mid g^n = 1\}$, and if also $|G|$ is finite then $o(g)$ divides $|G|$ (by Lagrange).

3.11 Theorem (1st Isomorphism Theorem) *Let G be a group and let $N, H \leqslant G$ be subgroups such that $H \leqslant N_G(N)$ (this is satisfied for instance if $N \trianglelefteq G$). Then*

$$HN = NH \leqslant G\,, \quad N \trianglelefteq HN\,, \quad H \cap N \trianglelefteq H$$

and

$$H/H \cap N \to HN/N\,, \quad h(H \cap N) \mapsto hN\,,$$

is an isomorphism.

Proof For all $h \in H$ and $n \in N$ we have $hn = (hnh^{-1})h \in NH$ and $nh = h(h^{-1}nh) \in HN$, since $H \leqslant N_G(N)$. Thus, $HN = NH$. By Examples 2.11(e), HN is a subgroup of G. Moreover, for $n \in N$ and $h \in H$ we have $nhN(nh)^{-1} = nhNh^{-1}n^{-1} = nNn^{-1} = N$, since $h \in N_G(N)$. Thus $N \trianglelefteq NH$. The composition of the inclusion $H \subseteq HN$ and the natural epimorphism $HN \to HN/N$ is a homomorphism $f\colon H \to HN/N$, $h \mapsto hN$. It is surjective, since $hnN = hN = f(h)$ for all $h \in H$ and $n \in N$. Its kernel is $H \cap N$. Thus, $H \cap N \trianglelefteq H$, and, by Corollary 3.6, f induces an isomorphism $\overline{f}\colon H/H \cap N \to HN/N$, $h(H \cap N) \mapsto hN$. $\square$

3.12 Theorem (Correspondence Theorem and 2nd Isomorphism Theorem) *Let G be a group, let $N \trianglelefteq G$ and let $\nu\colon G \to G/N$ denote the canonical epimorphism. The function*

$$\Phi\colon \{H \mid N \leqslant H \leqslant G\} \to \{X \mid X \leqslant G/N\}\,, \quad H \mapsto H/N = \nu(H)\,,$$

is a bijection with inverse $\Psi\colon X \mapsto \nu^{-1}(X)$. For subgroups H, H_1 and H_2 of G which contain N one has:

$$H_1 \leqslant H_2 \iff H_1/N \leqslant H_2/N \quad \text{and} \quad H \trianglelefteq G \iff H/N \trianglelefteq G/N\,.$$

Moreover, if $N \leqslant H \trianglelefteq G$ then $(G/N)/(H/N) \cong G/H$.

Proof Since images and preimages of subgroups are again subgroups (see Examples 2.11(g) applied to ν), the functions Φ and Ψ have values in the indicated sets and obviously respect inclusions. In fact, in regards to the function Ψ, note that $N = \ker(\nu) = \nu^{-1}(\{1\})$ is contained in $\nu^{-1}(X)$ for every subgroup X of G/N. For every $N \leqslant H \leqslant G$ we have $\nu^{-1}(\nu(H)) = H$, since $N \leqslant H$ (see also Exercise 6). And for every $X \leqslant G/N$ we have $\nu(\nu^{-1}(X)) = X$, since ν is surjective (see also Exercise 6). Thus, Φ and Ψ are inverse bijections.

The statement concerning H_1 and H_2 now follows immediately, since $H_1 \leqslant H_2 \leqslant G$ implies $\nu(H_1) \leqslant \nu(H_2)$ and $X_1 \leqslant X_2 \leqslant G/N$ implies $\nu^{-1}(X_1) \leqslant \nu^{-1}(X_2)$. Moreover, for $N \leqslant H \leqslant G$, $h \in H$ and $g \in G$ we have

$$ghg^{-1} \in H \iff ghg^{-1}N \in H/N \iff (gN)(hN)(g^{-1}N) \in H/N\,.$$

This shows that $N_G(H)/N = N_{G/N}(H/N)$. In particular, H is normal in G if and only if H/N is normal in G/N. Finally, for $N \leqslant H \trianglelefteq G$, the composition $f\colon G \to (G/N)/(H/N)$ of the two canonical epimorphisms $G \to G/N$ and $G/N \to (G/N)/(H/N)$ is an epimorphism with kernel H. Now, Corollary 3.6 induces an isomorphism $\overline{f}\colon G/H \to (G/N)/(H/N)$. □

3.13 Proposition *Every subgroup and factor group of a cyclic group is cylic.*

Proof Let G be a cyclic group generated by $g \in G$. If $N \trianglelefteq G$ then G/N is generated by gN. To prove that subgroups of G are again cyclic, we may assume that $G = \mathbb{Z}$ or $G = \mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$, using Theorem 3.8 and Exercise 5. In the first case ($G = \mathbb{Z}$), by Theorem 2.12, subgroups of $\mathbb{Z}$ are of the form $k\mathbb{Z}$, $k \in \mathbb{Z}$, and $k\mathbb{Z}$ is cyclic, generated by k. Now consider the second case $G = \mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{N}$. By the Correspondence Theorem, subgroups of $\mathbb{Z}/n\mathbb{Z}$ are of the form $k\mathbb{Z}/n\mathbb{Z}$ with $n\mathbb{Z} \leqslant k\mathbb{Z} \leqslant \mathbb{Z}$. But $k\mathbb{Z}$ is cyclic and, by the initial argument of the proof, with $k\mathbb{Z}$ also every factor group of $k\mathbb{Z}$ is cyclic. □

Exercises for Section 3

1. Let M and N be normal subgroups of a group G. Show that also $M \cap N$ and MN are normal subgroups of G.

2. Let G be a group and let X be a subset of G. Show that $C_G(X) \trianglelefteq N_G(X)$.

3. Let G be a group. Show that $Z(G)$ and G' are characteristic subgroups of G.

4. (a) Let G be a group, let N be a normal subgroup of G, and let $\nu\colon G \to G/N$, $g \mapsto gN$, denote the natural epimorphism. Show that, for every group H, the function

$$\mathrm{Hom}(G/N, H) \mapsto \{f \in \mathrm{Hom}(G,H) \mid N \leqslant \ker(f)\}\,, \quad \alpha \mapsto \alpha \circ \nu\,,$$

is bijective.

(b) Let G be a group and let A be an abelian group. Let $\nu\colon G \to G^{\mathrm{ab}} := G/G'$ denote the canonical epimorphism. Show that, with the group structure from Exercise 2.9 on the homomorphism sets, the function

$$\mathrm{Hom}(G^{\mathrm{ab}}, A) \to \mathrm{Hom}(G, A)\,, \quad \alpha \mapsto \alpha \circ \nu\,,$$

is a group isomorphism.

5. Let G and H be groups and let $f\colon G \to H$ be an isomorphism. Moreover, let $N \trianglelefteq G$ and set $M := f(N)$. Show that M is normal in H and that $G/N \cong H/M$.

6. (a) Let $f\colon G \to H$ be a group homomorphism and let $U \leqslant G$ and $V \leqslant H$ be subgroups. Show that

$$f^{-1}(f(U)) = U\ker(f) \quad \text{and} \quad f(f^{-1}(V)) = V \cap \mathrm{im}(f)\,.$$

(b) Let G be a group, let $N \trianglelefteq G$ and let $\nu\colon G \to G/N$ denote the canonical epimorphism. Show that for every subgroup U of G one has $\nu(U) = UN/N$.

7. Let G be a group. Show that:

(a) $H \underset{\text{char}}{\trianglelefteq} G \Rightarrow H \trianglelefteq G$.

(b) $M \underset{\text{char}}{\trianglelefteq} N \underset{\text{char}}{\trianglelefteq} G \Rightarrow M \underset{\text{char}}{\trianglelefteq} G$.

(c) $M \underset{\text{char}}{\trianglelefteq} N \trianglelefteq G \Rightarrow M \trianglelefteq G$.

(d) $M \trianglelefteq N \trianglelefteq G \not\Rightarrow M \trianglelefteq G$. (Give a counterexample.)

8. Let G be a cyclic group of order n and let $m \in \mathbb{N}$ be a divisor of n. Show that G has precisely one subgroup of order m.

9. (Butterfly Lemma or Zassenhaus Lemma or 3$^{\text{rd}}$ Isomorphism Theorem) Let U and V be subgroups of a group G and let $U_0 \trianglelefteq U$ and $V_0 \trianglelefteq V$. Show that

$$U_0(U \cap V_0) \trianglelefteq U_0(U \cap V)\,, \quad (U_0 \cap V)V_0 \trianglelefteq (U \cap V)V_0\,, \quad (U_0 \cap V)(U \cap V_0) \trianglelefteq U \cap V$$

and

$$U_0(U \cap V)/U_0(U \cap V_0) \cong (U \cap V)/(U_0 \cap V)(U \cap V_0) \cong (U \cap V)V_0/(U_0 \cap V)V_0 \,.$$

To see the 'butterfly', draw a diagram of the involved subgroups.

10. Let G be a finite group and let π be a set of primes. An element x of G is called a π-*element* if its order involves only primes from π. It is called a π'-*element* if its order involves only primes outside π.

(a) Let $g \in G$. Assume that we can write $g = xy$ with a π-element $x \in G$ and a π'-element $y \in G$ satisfying $xy = yx$. Show that x and y are powers of g.

(b) Show that for given $g \in G$ there exist unique elements $x, y \in G$ satisfying:

$$x \text{ is a } \pi\text{-element, } y \text{ is a } \pi'\text{-element, } g = xy \text{ and } xy = yx.$$

(The element x is called the π-*part* of g and the element y is called the π'-*part* of g. Notation: $x = g_\pi$, $y = g_{\pi'}$.)

11. Let G and H be groups and let $p_1 \colon G \times H \to G$, $(g,h) \mapsto g$, and $p_2 \colon G \times H \to H$, $(g,h) \mapsto h$, denote the projection maps. Note that they are epimorphisms. This exercise gives a description of all subgroups of $G \times H$.

(a) Let $X \leqslant G \times H$. Set

$$k_1(X) := \{g \in G \mid (g,1) \in X\} \quad \text{and} \quad k_2(X) := \{h \in H \mid (1,h) \in X\} \,.$$

Let $i \in \{1,2\}$. Show that $k_i(X) \trianglelefteq p_i(X)$. Moreover, show that the composition $\pi_i \colon X \to p_i(X) \to p_i(X)/k_i(X)$ of the projection map p_i and the natural epimorphism induces an isomorphism $\overline{\pi}_i \colon X/(k_1(X) \times k_2(X)) \xrightarrow{\sim} p_i(X)/k_i(X)$.

(b) Let $K_1 \trianglelefteq P_1 \leqslant G$, let $K_2 \trianglelefteq P_2 \leqslant H$, and let $\eta \colon P_1/K_1 \xrightarrow{\sim} P_2/K_2$ be an isomorphism. Define

$$X := \{(g,h) \in P_1 \times P_2 \mid \eta(gK_1) = hK_2\} \,.$$

Show that X is a subgroup of $G \times H$.

(c) Use the constructions in (a) and (b) to show that the set of subgroups of $G \times H$ is in bijection with the set of all quintuples $(P_1, K_1, \eta, P_2, K_2)$ such that $K_1 \trianglelefteq P_1 \leqslant G$, $K_2 \trianglelefteq P_2 \leqslant H$, and $\eta \colon P_1/K_1 \xrightarrow{\sim} P_2/K_2$ is an isomorphism.

12. Let $f \colon G \to H$ be a homorphism. Show that f can be written as a composition $f = i \circ g \circ p$ of homomorphisms with the property that p is a natural epimorphism from G onto a factor group of G, g is an isomorphism, and i is the inclusion of a subgroup of H into H.

13. A *short exact sequence* of groups is a sequence of group homomorphisms

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1\,,$$

where 1 denotes a trivial group, such that at A, B and C the image of the incoming arrow is equal to the kernel of the outgoing arrow.

Let A, B, C be groups. Show that there exists a short exact sequence as above if and only if there exists a normal sugroup N of B such that $N \cong A$ and $B/N \cong C$.

More category theory

Definition Let $\mathcal{C}$ be a category. Its *opposite* category $\mathcal{C}^{\mathrm{op}}$ has the same objects as $\mathcal{C}$ and for objects C and D of $\mathcal{C}^{\mathrm{op}}$, one sets

$$\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(C, D) := \mathrm{Hom}_{\mathcal{C}}(D, C)\,.$$

A morphism $f\colon D \to C$ is denoted by $f^{\mathrm{op}}\colon C \to D$, if considered in the category $\mathcal{C}^{\mathrm{op}}$. The composition of morphism $g^{\mathrm{op}}\colon E \to D$ and $f^{\mathrm{op}}\colon D \to C$ in the category $\mathcal{C}^{\mathrm{op}}$ is defined by

$$f^{\mathrm{op}} \circ g^{\mathrm{op}} := (g \circ f)^{\mathrm{op}}\,.$$

14. Let $\mathcal{C}$ be a category.

(a) Show that for every object C of $\mathcal{C}$ one has $(\mathrm{id}_C)^{op} = \mathrm{id}_C$.

(b) Show that $(\mathcal{C}^{\mathrm{op}})^{\mathrm{op}} = \mathcal{C}$.

15. Let $\mathcal{C}$ be a category. Prove the following statements:

(a) A morphism $f\colon C \to D$ in $\mathcal{C}$ is a isomorphism if and only if $f^{\mathrm{op}}\colon D \to C$ is an isomorphism in $\mathcal{C}^{\mathrm{op}}$. In this case $(f^{\mathrm{op}})^{-1} = (f^{-1})^{\mathrm{op}}$.

(b) A morphism $f\colon C \to D$ in $\mathcal{C}$ is a monomorphism (resp. epimorphism) if and only if $f^{\mathrm{op}}\colon D \to C$ is an epimorphism (resp. monomorphism) in $\mathcal{C}^{\mathrm{op}}$.

(c) An object C of $\mathcal{C}$ is an initial (resp. final) object of $\mathcal{C}$ if and only if C is a final (resp. initial) object in $\mathcal{C}^{\mathrm{op}}$.

(d) An object C of $\mathcal{C}$ is a zero object in $\mathcal{C}$ if and only if C is a zero object in $\mathcal{C}^{\mathrm{op}}$.

Definition Let $\mathcal{C}$ be a category and let X and Y be objects of $\mathcal{C}$. A *product* of X and Y is an object P of $\mathcal{C}$ together with morphisms $p\colon P \to X$ and $q\colon P \to Y$ in $\mathcal{C}$ such that for any object Z of $\mathcal{C}$ the function

$$\mathrm{Hom}_{\mathcal{C}}(Z, P) \to \mathrm{Hom}_{\mathcal{C}}(Z, X) \times \mathrm{Hom}_{\mathcal{C}}(Z, Y)\,, \quad f \mapsto (p \circ f, q \circ f)\,,$$

is bijective. In other words, for every $g\colon Z \to X$ and every $h\colon Z \to Y$ in $\mathcal{C}$ there exists a unique $f\colon Z \to P$ in $\mathcal{C}$ such that $g = p \circ f$ and $h = q \circ f$. In. this case p and q are called the *projections* of the product. (Note: Given X and Y, a product of X and Y might not exist.)

16. Assume that $\mathcal{C}$ is a category and that X and Y are objects of $\mathcal{C}$. Assume further that an object Z together with morphisms $p\colon Z \to X$ and $q\colon Z \to Y$ is a product of X and Y and assume further that also an object Z' together with morphisms $p'\colon Z' \to X$ and $q'\colon Z' \to Y$ is a product of X and Y in $\mathcal{C}$. Show that there exists an isomorphism $f\colon Z \to Z'$ such that $p' \circ f = p$ and $q' \circ f = q$. In this sense, products are *unique up to unique isomorphism.*

17. Let $\mathcal{C}$ be a category and let P together with $p\colon P \to X$ and $q\colon P \to Y$ be a product of the objects X and Y of $\mathcal{C}$. Show that p and q are epimorphisms in $\mathcal{C}$.

18. Show that the cartesian product $X \times Y$ of two sets X and Y, together with the projections maps $p\colon X \times Y \to X$ and $q\colon X \times Y \to Y$, given by $p(x, y) = x$ and $q(x, y) = y$, for $(x, y) \in X \times Y$, is a product in the category Set.

19. Let G and H be groups. Does there exist a product of G and H in Gr?

20. Let $\mathcal{C}$ be a category and let X and Y be objects of $\mathcal{C}$. A *coproduct* of X and Y is an object C of $\mathcal{C}$ together with two morphisms $i\colon X \to C$ and $j\colon Y \to C$ in $\mathcal{C}$ such that, for every object Z in $\mathcal{C}$, the function

$$\mathrm{Hom}_{\mathcal{C}}(C, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z)\,, \quad f \mapsto (f \circ i, f \circ j)\,,$$

is bijective. In this case i and j are called the *injections* of the coproduct.

21. Let $\mathcal{C}$ be a category and let X and Y be objects in $\mathcal{C}$. Moreover, let P be an object of $\mathcal{C}$ and let $p\colon P \to X$ and $q\colon P \to Y$ be morphisms in $\mathcal{C}$. Show that the following are equivalent:

(i) The object P together with p and q is a product of X and Y in $\mathcal{C}$.

(ii) The object P together with $p^{\mathrm{op}}\colon X \to P$ and $q^{\mathrm{op}}\colon Y \to P$ is a coproduct of X and Y in $\mathcal{C}^{\mathrm{op}}$.

22. Find a coproduct of X and Y in the category Set.