Algebra I, An introductory course

V. G. Tkachev, Linköping University, Sweden

E-mail address: vladimir.tkatjev@liu.se

Contents

Chapter 1

Groups

1.1. Monoids

Let S be a set with a **law of composition**: $S \times S \to S$. The image of the pair under this mapping is called their **product**, denoted by xy, or $x \cdot y$ or $x + y$. We write resp. S, $(S, \cdot)$ or $(S, +)$.

The law of composition is called **associative** (resp. **commutative**) if $(xy)z = x(yz)$ (resp. $xy = yx$).

An element $e \in S$ is called a **unit element** if $ex = xe = x$ for all $x \in S$.

When $(S, +)$ then e is called a zero element.

A unit is unique: $ee' = e = e'$.

Definition 1.1. A monoid is a set $(G, \cdot, \text{associative}, \text{a unit element } e)$. If $\cdot$ is commutative, G is called **abelian**. A **submonoid** is a subset H of a monoid G containing the unit e and such that $\forall x, y \in H \Rightarrow xy \in H$.

Proposition (The total commutativity)**.** *If G is an abelian monoid and ϕ is a bijection of $\{1, 2, \ldots, n\}$ onto itself then $\prod_{i=1}^{m} x_i = \prod_{j=1}^{m} x_{\phi(j)}$*

Proof. By induction. □

Example 1.1.

- $(\mathbb{N}, +)$ is a monoid.
- Given a monoid G, the set $\{x^n, n \in \mathbb{N}\}$ is a submonoid.
- $G = (e, x, y)$ with the composition law $x \cdot x = x \cdot y = x$, $y \cdot x = y \cdot y = y$ is a noncommutative monoid.

1.2. Groups

Definition 1.2. A **group** G is a monoid, such that $\forall x \in G\ \exists y \in G : xy = yx = e$. Such an element is called an **inverse** for x, denoted by x^{-1}. Also, $x^{-n} := (x^{-1})^n$.

An inverse is unique: $y' = y'e = y'(xy) = (y'x)y = ey = y$.

Example 1.2.

- The **groups of permutations** $\mathrm{Perm}(S)$: the set of all bijective mappings of a set S.
- The **general linear group** $GL(V, k)$ is the set of all invertible linear mappings of a vector space V over a field k, together with the operation of ordinary composition.
- The **special linear group** $SL_2(k)$ is the group of 2×2 matrices with entries in a field k and determinant one.
- The **dihedral group** D_n: the symmetry group of an n-sided regular polygon.
- **The group of automorphisms:** If $\mathscr{A}$ is a category and A is an object in $\mathscr{A}$ then the set of automorphisms $\mathrm{Aut}(A)$ is a group.

Example 1.3 (Cayley Tables)**.** For example, a group with two elements $G = \{e, a\}$:

	e	a
e	e	a
a	a	e

A subset $S \subset G$ of a group G is called a **set of generators** of G, denoted $G = \langle S \rangle$ if, if every element of G can be expressed as a product of elements of S or inverses of elements of S. In other words, any element $x \in G$ can be written as a finite product

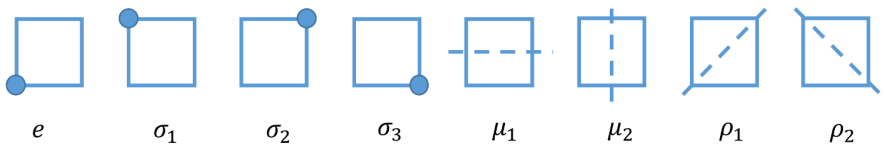
$$x = x_1^{n_1} \cdots x_m^{n_m}, \qquad x_i \in S, n_i \in \mathbb{Z}. \tag{1.1}$$

Example 1.4 (A cyclic group)**.** The integers $\mathbb{Z}$ is an abelian additive group with unit 0. Since $\forall n \in \mathbb{Z}$: $n = 1^n$ (in the additive sense!), $\mathbb{Z} = \langle 1 \rangle$. Also note that $\mathbb{Z} = \langle -1 \rangle$. The elements 1 and -1 are called **cyclic generators**.

Definition 1.3. A group G is called **cyclic** if there exists $a \in G$ such that $G = \langle a \rangle$.

Any cyclic group is abelian.

Example 1.5 (Generators)**.** The dihedral group D_4 (the group of symmetries of a square) consists of the unit e, rotations $\sigma_1, \sigma_2, \sigma_3$, two mirrors μ_1, μ_2 and the flips ρ_1, ρ_2:



Here are some of the group identities:

$$\begin{aligned} \sigma_1^k &= \sigma_k, \quad k = 1, 2, 3, \\ \sigma_1^4 &= e, \\ \mu_i^2 &= \rho_i^2 = e, \quad i = 1, 2 \\ \mu_1 \sigma_1^3 &= \sigma_1 \mu_1. \end{aligned}$$

The figure below shows *how* the elements $\sigma = \sigma_1$ and $\mu = \mu_1$ generates the group D_4.

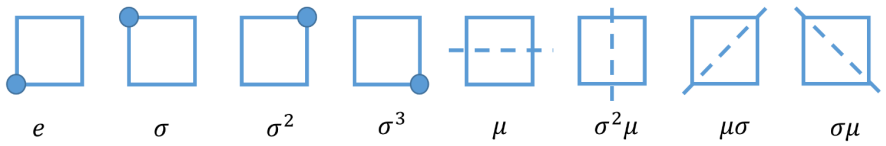


Figure 1. $D_4 = \langle \sigma, \mu \rangle$

Given two groups G_1, G_2, let us define their **direct product** as the set theoretic product

$$G_1 \times G_2 = \{(x_1, x_2) : x_i \in G_i\}$$

equipped with the componentwise multiplication: $(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2)$. Then $G_1 \times G_2$ is a group whose unit element is (e_1, e_2), where e_i is the unit in G_i, $i = 1, 2$.

Definition 1.4. Let H be a subset of a group G. If H is a group with the same operation as G, then H is called a **subgroup** of G. A subgroup H is called **trivial** if $H = \{e\}$.

"H is a subgroup of G" is written for short as $H \leqslant G$.

Example 1.6. Let $\mathbb{Z}$ be the additive group of integers. Given $m\mathbb{Z}$, define $m\mathbb{Z}$ in an obvious way. *Any nontrivial subgroup H of $\mathbb{Z}$ is $m\mathbb{Z}$ for some integer m.* (Prove!)

Given a subset $S \subset G$, there holds

$$\langle S \rangle = \bigcap_{S \subset H \leqslant G} H$$

(i.e. H runs over subgroups of G containing S).

Let G, G' be groups. A **homomorphism** G into G' is a mapping $f : G \to G'$ such that $f(xy) = f(x)f(y)$ for all $x, y \in G$. If f is a homomorphism then $f(e) = f(e^2) = f(e)f(e)$, hence $f(e) = e'$. Also, since $e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1})$ we have

$$f(x^{-1}) = f(x)^{-1}.$$

A homomorphism is called **isomorphism** if f is bijective. If f is an isomorphism then the inverse is so (why?). If $G = G'$ then an isomorphism is called an **automorphism**. Two groups are called **isomorphic** if there exists an isomorphism between them: $G \approx G'$.

Example 1.7 (Inner automorphism)**.** Let G be an group and $a \in G$. Define $f(x) = a^{-1}xa : G \to G$. Then $f(x)f(y) = a^{-1}xaa^{-1}ya = a^{-1}xya = f(xy)$, i.e. f is an endomorphism (i.e. a homomorphism of G into itself). Further, if $g(x) = axa^{-1}$ then $f \circ g = \mathrm{id}_G$, i.e. $g = f^{-1}$, which implies that f is an automorphism. Such an automorphism is called an **inner automorphism**; otherwise it is called **outer**.

Proposition 1.1. *Let G be a group, S a set of generators for G, and G' another group. Let $f : S \to G'$ be a map. If there exists a homomorphism $\bar{f} : G \to G'$ whose restriction to S is f, then there is only one. In other words, f has at most one extension to a homomorphism of G into G'.*

Proof. By (1.1) and the homomorphism definition,

$$\bar{f}(x) = \bar{f}(x_1^{n_1} \cdots x_m^{n_m}) = \bar{f}(x_1)^{n_1} \cdots \bar{f}(x_m)^{n_m} = f(x_1)^{n_1} \cdots f(x_m)^{n_m},$$

hence $\bar{f}(x)$ is uniquely defined by the values on S. □

• If $f : G \to G'$ and $g : G' \to G''$ be group homomorphisms then so is $g \circ f : G \to G''$.

• If $f : G \to G'$ and $g : G' \to G''$ be isomorphisms then so is $g \circ f : G \to G''$. In particular, the set $\mathrm{Aut}(G)$ of all automorphisms of G is a group.

Definition 1.5. Given a homomorphism $f : G \to G'$, define its **kernel** $\mathrm{Ker}\, f = \{x \in G : f(x) = e'\}$ and **image** $\mathrm{Im}\, f = f(G)$.

Proposition 1.2.

(i) $\mathrm{Ker}\, f$ *and* $\mathrm{Im}\, f$ *are subgroups of G and G', respectively.*

(ii) The homomorphism f is injective if and only if $\mathrm{Ker}\, f = \{e\}$.

(iii) A surjective homomorphism with ***trivial*** *kernel is an isomorphism.*

Proof. (ii) If f is injective and $x \in \mathrm{Ker}\, f$ then $f(e) = f(x) = e'$ implies $x = e$. Conversely, if $\mathrm{Ker}\, f$ is trivial and $f(x) = f(y)$ we have

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(y)f(y^{-1}) = f(yy^{-1}) = f(e) = e'.$$

It follows that $xy^{-1} = e$, thus $x = y$. □

• An injective homomorphism is denoted by $f : G \hookrightarrow G'$.

Proposition 1.3 (The splitting property)**.** *Let G be a group and let H, K be two subgroups such that $H \cap K = e$, $HK = G$, and such that $hk = kh$ for all $h \in H$ and $k \in K$. Then the map $\rho : H \times K \to G$ such that $(h, k) \mapsto hk$ is an isomorphism.*

Proof. The direct product $H \times K$ is a group and

$$\rho((h,k) \cdot (h',k')) = \rho((hh', kk')) = hh'kk' = hkh'k' = \rho((h,k)) \cdot \rho((h',k')),$$

thus ρ is a homomorphism. If $\rho((h,k)) = e$ then $hk = e$, i.e. $H \ni h = k^{-1} \in K$ implying $h = k = e$, thus $\mathrm{Ker}\, \rho$ is trivial. Since $HK = G$ we also have $\mathrm{Im}\, \rho = G$, thus ρ is an isomorphism. □

1.3. Exercises

Exercise 1.1.

(1) Show that the set $H_3(\mathbb{Z})$ of matrices

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \qquad a, b, c \in \mathbb{Z}$$

is a (multiplicative) group. Describe all normal subgroups of $H_3(\mathbb{Z})$.

(2) Let $G = \mathbb{Z}^3$ with the composition law $x \cdot y = (x_1 + y_1, x_2 + y_2, x_3 + y_3 + x_1 y_2)$. Show that G is a group. Prove that $G \approx H_3(\mathbb{Z})$

Exercise 1.2. Prove that every group of order 4 is abelian.

Exercise 1.3. Describe all subgroups of D_4. Describe all normal subgroups of D_4.

Exercise 1.4. Show that the isometry group of a cube in $\mathbb{R}^3$ (octahedral group or cube group) is isomorphic to the symmetric group S_4

Exercise 1.5. Let G be a group. A commutator in G is an element of the form $aba^{-1}b^{-1}$ with $a, b \in G$. Let G^c be the subgroup generated by the commutators. Then G^c is called the commutator subgroup. Show that G^c is normal. Show that any homomorphism of G into an abelian group factors through G/G^c.

1.4. Cosets

Let $H \leqslant G$. A **left coset** of H in G is a subset of G of type aH, for some element $a \in G$. An element of aH is called a **coset representative** of aH.

Proposition 1.4.

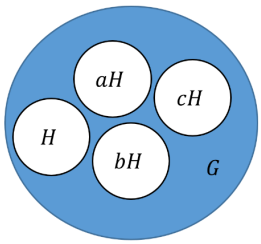
(i) *The map $x \mapsto ax$ induces a bijection of H onto aH.*

(ii) *Any two left cosets have the same cardinality:*

$$|H| = |aH|, \quad \forall a \in G. \tag{1.2}$$

(iii) *If $aH \cap bH \neq \emptyset$ then $aH = bH$.*

Proof. (i) Indeed, $ax = ay$ implies $x = a^{-1}ax = y$. (i) $\Rightarrow$ (*ii*). (iii) If $ax = by \in aH \cap bH$ then $a = byx^{-1} = bz \in bH$, where $yx^{-1} \in H$ hence $aH \subset bHH = bH$. By symmetry, $bH \subset aH$. This yields the claim. □



Thus, a group G is the *disjoint union* of the left cosets of a subgroup H. A similar remark applies to **right cosets** (i.e. subsets of G of type Ha). The number of left cosets of H in G is denoted by $(G : H)$, and is called the (left) **index** of H in G. The index of the trivial subgroup is called the **order** of G and is written

$$\text{order of } G = (G : 1) = |G|.$$

Theorem 1.1 (Lagrange's Theorem)**.** *If $H \leqslant G$ then*

$$(G : H)(H : 1) = (G : 1)$$

in the sense that if two of these indices are finite, so is the third. In particular, if $(G : 1) < \infty$ then the order of H divides the order of G.

Proof. Let $S \subset G$ be a set of (left) coset representatives of H in G. Then $|S| = (G : H)$. By the disjointedness property $G = \bigsqcup_{x \in S} xH$, where by (1.2) each coset xH has the same cardinality as H. It follows that $|S| \cdot |H| = |G|$, the claim follows. □

Example 1.8. Given an element $e \neq a \in G$, $\langle a \rangle$ is a nontrivial cyclic subgroup of G. If G is finite, $\langle a \rangle$ is too, hence there exists the smallest integer $m \geq 2$ such that $a^m = e$. This m is called the **period** of a. By Lagrange's theorem, m divides $|G|$.

Example 1.9. *A group of prime order is cyclic.* Indeed, let $(G:1)=p$ and let $a\in G$, $a\neq e$. Then the order α of $\langle a\rangle$ divides p and ≥ 2, so $\alpha=p$ and so $\langle a\rangle=G$, which is therefore cyclic.

Example 1.10. In the notation of Example 1.5, note that $S=\{e,\sigma_1,\sigma_2,\sigma_3\}$ and $M_1=\{e,\mu_1\}$, are subgroups of D_4. An easy argument yields the left and right cosets for M_1

left cosets	right cosets
$eM_1=\mu_1M_1=\{e,\mu_1\}$	$M_1e=M_1\mu_1=\{e,\mu_1\}$
$\sigma_1M_1=\rho_2M_1=\{\sigma_1,\rho_2\}$	$M_1\sigma_1=M_1\rho_1=\{\sigma_1,\rho_1\}$
$\sigma_2M_1=\mu_2M_1=\{\sigma_2,\mu_2\}$	$M_1\sigma_2=M_1\mu_2=\{\sigma_2,\mu_2\}$
$\sigma_3M_1=\rho_1M_1=\{\sigma_3,\rho_1\}$	$M_1\sigma_3=M_1\rho_2=\{\sigma_3,\rho_2\}$

and S:

$$eS=\sigma_1S=\sigma_2S=\sigma_3S=\{e,\sigma_1,\sigma_2,\sigma_3\}=Se=S\sigma_1=S\sigma_2=S\sigma_3$$
$$\mu_1S=\mu_2S=\rho_1S=\rho_2S=\{\mu_1,\mu_2,\rho_1,\rho_2\}=S\mu_1=S\mu_2=S\rho_1=S\rho_2.$$

In particular, $(D_4:1)=8$, $(D_4:M_1)=(S:1)=4$, $(D_4:S)=(M_1:1)=2$. See figure below.

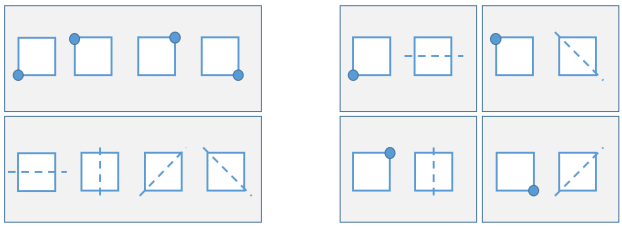


Figure 2. The **left** cosets for M_1 and S respectively in D_4

1.5. Normal subgroups

Definition 1.6. A subgroup H of a group G is called a **normal subgroup**, $H\trianglelefteq G$, if $xHx^{-1}=H$ holds for any $x\in G$.

By the definition, *any subgroup of an abelian group is normal.*

Definition 1.7. A group is called **simple** if it is non-trivial , and has no normal subgroups other than $\{e\}$ and G itself.

Proposition 1.5.

(i) A subgroup $H\leqslant G$ is normal if and only if $xHx^{-1}\subset H$ for all $x\in G$.

(ii) A subgroup $H\leqslant G$ is normal if and only if $xH=Hx$ for all $x\in G$.

Proof. (i) ($\Rightarrow$) : trivial. ($\Leftarrow$) : let $xHx^{-1} \subset H$ implies $Hx^{-1} \subset x^{-1}H$, and next $H \subset x^{-1}Hx = yHy^{-1} \subset H$ for $y = x^{-1}$. Thus $xHx^{-1} = H$.

(ii) ($\Rightarrow$) Let $x \in G$ and $H \trianglelefteq G$. By the assumption and Example 1.7, $g(h) := xhx^{-1} : H \to H$ is an isomorphism and $g(h)x = xh$. This yields $xH = Hx$. ($\Leftarrow$) Conversely, let $xH = Hx$ for any $x \in G$. Let $g(h) = xhx^{-1}$. Then by the assumption there exists $h' \in H$ such that $h'x = xh = g(h)x$, hence $h' = g(h)$. It follows that $g : H \to H$ and since g is a bijection, we have $g(H) = H$, as desired. □

Example 1.11. It follows from Example 1.10 that $M_1 \trianglelefteq D_4$, while $S \not\trianglelefteq D_4$.

We need not distinguish between left and right cosets for a normal group and say just a coset. It follows from Proposition 1.5 that

$$Hx \cdot Hy = xHHy = xHy = xyH,$$

hence the product of two cosets is a coset. Furthermore, $xH \cdot x^{-1}H = eH = H$. This readily yields that the set G' of cosets of H is a group with unit H: $xH \cdot H = xH$. The group G' is called the **factor group** of G by H and denoted by G/H (reads as 'G modulo H'). Given two elements $x, y \in G$, we write

$$x \equiv y \mod H \quad \Leftrightarrow xy^{-1} \in H.$$

The **canonical map**

$$f(x) = xH : G \to G/H$$

is a group-homomorphism.

Proposition 1.6. *A subgroup is normal iff it is the kernel of some homomorphism of G.*

Proof. Let $f : G \to G'$ be a group-homomorphism. By Proposition 1.2, $H = \operatorname{Ker} f$ is a subgroup. If $x \in G$ and $h \in H$ then $f(h) = e'$, hence

$$f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)e'f(x)^{-1} = e'.$$

This yields $xhx^{-1} \in \operatorname{Ker} f$ implying that H is normal. Conversely, if $H \leqslant G$ is normal then H is the kernel of the canonical map $G \to G/H$. □

Example 1.12 (The center)**.** Given a group G, let

$$Z_G = \{x \in G : xy = yx, \quad \forall y \in G\}$$

Clearly, $e \in Z_G$. If $x, x' \in Z_G$ then $xx' = x'x$ and for any $y \in G$ $xx'y = xyx' = yxx'$, hence $xx' \in Z_G$. Finally,

$$x^{-1}y = (y^{-1}x)^{-1} = (xy^{-1})^{-1} = yx^{-1},$$

hence $x^{-1} \in Z_G$. This shows that Z_G is a group. It is called the **center** of G. Since $xZ_G = Z_Gx$,

$$\boxed{Z_G \trianglelefteq G}$$

Example 1.13 (The normalizer)**.** Given a group G and $S \subset G$, let

$$N_S = \{x \in G : xS = Sx\}.$$

Then $e \in Z_G$ and if $x, x' \in N_S$ then $xx'S = xSx' = xx'S$, therefore $xx' \in N_S$. Also $S = x^{-1}Sx$, hence $Sx^{-1} = x^{-1}S$, thus $x^{-1} \in Z_G$ and it follows that N_S is a group. It is called the **normalizer** of the set S.

The normalizer need not to be a normal subgroup.

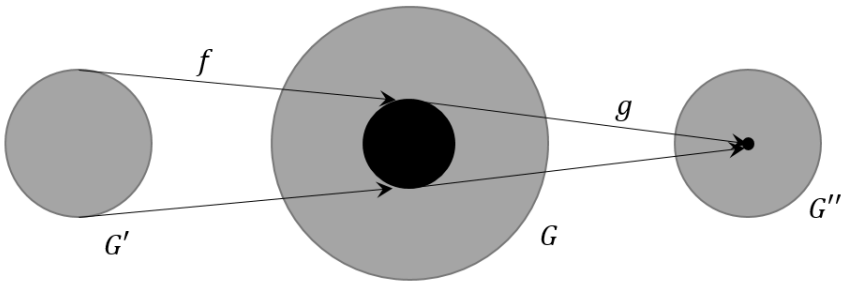
Example 1.14. The determinant $\det : GL(V,k) \to k$ is obviously a homomorphism between the general linear group and the multiplication group of the ground field k. Then $\operatorname{Ker}\det = SL(V,k) = \{x \in GL(V,k) : \det x = 1\}$ is a normal subgroup.

1.6. Exact sequences and commutative diagrams

A sequence of homomorphisms

$$G' \xrightarrow{f} G \xrightarrow{g} G''$$

is called **exact** if $\operatorname{Im} f = \operatorname{Ker} g$.



Example 1.15. A homomorphism $f : G \to G'$ is surjective (resp. injective) if and only if the sequence $G \xrightarrow{f} G' \xrightarrow{i} 0$ (resp. $0 \xrightarrow{i} G \xrightarrow{f} G'$) is exact.

In general, a sequence of homomorphisms

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} \dots \xrightarrow{f_{n-1}} G_n$$

is called exact if $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$.

For example, if H is a normal subgroup of G then the (long) sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \xrightarrow{j} & G & \xrightarrow{\phi} & G/H & \longrightarrow & 0 \\ & & \text{inclusions} & & & & \text{canonical} & & \text{trivial} \end{array}$$

is exact, where 0 stands for a trivial group consisting of a unit.

Proposition 1.7. *Let the sequence*

$$0 \xrightarrow{i} G' \xrightarrow{f} G \xrightarrow{g} G'' \xrightarrow{j} 0$$

be exact. Then $G'' \approx G/f(G')$. Furthermore, the following diagram is commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G' & \xrightarrow{f} & G & \xrightarrow{g} & G'' & \xrightarrow{i} & 0 \\ \downarrow & & \downarrow{\scriptstyle f\approx} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle g^*\approx} & & \downarrow \\ 0 & \longrightarrow & f(G') & \xrightarrow{j} & G & \xrightarrow{\phi} & G/f(G') & \longrightarrow & 0 \end{array}$$

Here, the vertical maps are isomorphisms, and the rows are exact.

Proof. We have $\operatorname{Ker} f = \operatorname{Im} i = \{e'\}$, hence f is an injection. Also $H := f(G') = \ker g$. Clearly, $G' \approx H$ (since f is injection). By Proposition 1.6, H is a normal subgroup of G. This yields the second row. Further, $g(G) = \operatorname{Ker} i = G''$, hence g is a surjection. Let $x'' \in G''$ and let $x \in G$ be chosen arbitrary such that $g(x) = x''$. Define $g^*(x'') = xH \in G/H$. If $g(x) = g(y) = x''$ then $xy^{-1} \in \operatorname{Ker} g = H$, hence $xH = yH$, hence g^* is well-defined. Furthermore, if $x'' = g(x)$ and $y'' = g(y)$ then $x''y'' = g(xy)$, hence $g^*(x'')g^*(y'') = (xH)(yH) = xyH = g^*(x''y'')$, thus g^* is a homomorphism. Next, $x'' \in \operatorname{Ker} g^* \Leftrightarrow x'' = g(x)$ and $x \in H$ implying $g(x) = e''$, hence g^* is injection. Finally, given a $xH \in G/H$, $g^*(g(x)) = xH$, thus g^* is a surjection. This proves that g^* is an isomorphism making the diagram commutative. □

Proposition 1.8 (The 3rd Isomorphism Theorem)**.** *If $H = \operatorname{Ker} f$, where $f : G \to G'$ is a homomorphism then there exists a unique injective homomorphism $f_* : G/H \to G'$ such that $f_* \circ \phi = f$. In other words, the following diagram holds:*

$$\begin{array}{ccccc} H & \xrightarrow{j} & G & \xrightarrow{\phi} & G/H \\ & & & \searrow^{f} & \downarrow{\scriptstyle f_*(induced)} \\ & & & & G' \end{array}$$

In particular, the image $f(G) \approx G/\operatorname{Ker} f$.

Proof. Similarly as above: define $f_*(xH) \stackrel{\text{def}}{=} f(x)$. □

Proposition 1.9 (Simplifying factors)**.** *If $K \trianglelefteq H \trianglelefteq G$ then $K \trianglelefteq H$ and*

$$(G/K) \,/\, (H/K) \approx G/H.$$

Proof. The verification of the fact that K is normal in H is tautological. Next, define a map of $f : G/K \mapsto G/H$ by associating with each coset xK the coset xH. Then f is a homomorphism, and $\operatorname{Ker} f = \{xK : xH = H\} = \{xK : x \in H\}$. This yields the exact sequence

$$0 \longrightarrow H/K \xrightarrow{i} G/K \xrightarrow{f} G/H \longrightarrow 0$$

which by Proposition 1.7 implies the desired property. □

Proposition 1.10 (Normal lifting)**.** *Let $f : G \to G'$ be a surjective homomorphism, let H' be a normal subgroup of G'. Then $H := f^{-1}(H')$ is normal in G and*

$$G/H \approx G'/H'.$$

Proof. H is obviously a subgroup of G. If $x \in G$ then

$$f(xHx^{-1}) = f(x)f(H)f(x)^{-1} = yH'y^{-1} = H', \quad \text{where } y = f(x),$$

hence $xHx^{-1} = H$, thus H is normal. Since $f(xH) = f(x)H'$, the map

$$\bar{f}(xH) = f(x)H' : G/H \to G'/H' \tag{1.3}$$

is a well-defined homomorphism. Its kernel:

$$xH \in \operatorname{Ker} \bar{f} \quad \Leftrightarrow \quad f(x)H' = H' \quad \Leftrightarrow \quad f(x) \in H' \quad \Leftrightarrow \quad x \in H$$

i.e. $\bar{f}$ is injective. Furthermore, given an arbitrary $x' \in G'$ there exists $x \in G$ with $x' = f(x)$, hence $\bar{f}(xH) \subset x'H'$, i.e. $\bar{f}$ is surjection, and therefore an isomorphism. □

The homomorphism (1.3) is called **canonical**, see also the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f\text{(onto)}} & & \downarrow{\scriptstyle \bar{f}\text{(canonical)}} & & \\ 0 & \longrightarrow & H' & \longrightarrow & G' & \longrightarrow & G'/H' & \longrightarrow & 0 \end{array}$$

Proposition 1.11. *Let $G \to G'$ be an injective homomorphism. Then if G' be abelian (resp. cyclic) G is abelian (resp. cyclic).*

Proof. By the injectivity $G \approx f(G)$, the latter being a subgroup of G', and thus abelian (resp. cyclic) if G' is so. □

Exercises

Exercise 1.6. (a) Show that elements xy and yx in an arbitrary (not necessarily abelian!) group has the same period.

(b) Show that xyz and zyx may have distinct periods.

Exercise 1.7. The element $[x, y] = xyx^{-1}y^{-1}$ is called the commutator of x, y. Prove that $[x, yz] = [x, y][x, z]([y, [z, x]])^{-1}$.

Exercise 1.8. Give an example when the normalizer of a group is not a normal subgroup.

Exercise 1.9. Prove that the group of inner automorphisms of a group G is normal in $\operatorname{Aut}(G)$.

Exercise 1.10. Let G be a group such that $\operatorname{Aut}(G)$ is cyclic. Prove that G is abelian.

Exercise 1.11. Prove (vii) in Proposition 1.14.

1.7. Cyclic groups

Let G be an arbitrary group and $x \in G$. An integer $m \in \mathbb{Z}^+$ such that $x^m = e$ is called an **exponent** of x. The smallest *positive* exponent is called the **period** of x and denoted by $o(x)$.

Proposition 1.12. *In a finite group any element has a finite period. If $x^m = e$ then $o(x)|m$.*

Proof. The first claim is trivial. Next, without loss of generality $m > 0$. Then $m \geq n = o(x)$ and $m = kn + r$, $0 \leq r \leq n - 1$, thus $x^r = 0$, hence $r = 0$ by the minimality of the period. □

Example 1.16. If $G = D_4$ then $o(\sigma_1) = o(\sigma_3) = 4$, $o(\sigma_2) = o(\mu_i) = o(\rho_i) = 2$.

Proposition 1.13. *Let $G = \langle a \rangle$ be a cyclic group. Then every nontrivial subgroup H of G is cyclic and $H = \langle a^m \rangle$ for some $m \in \mathbb{Z}^+$.*

Proof. Let $G = \langle a \rangle$. Define m to be the smallest *positive* integer such that $g := a^m \in H$ (there are such powers because H contains some non-zero power of a, which becomes a positive power after inversion, if necessary.) If $h \in H$ is chosen arbitrarily then there exists $n \in \mathbb{Z}$ such that $h = a^n$. Write $n = mk + r$ with $0 \leq r \leq m - 1$ and $k \in \mathbb{Z}$. Then $h = a^{mk+r} = g^j \cdot a^r$ $\Rightarrow a^r = h \cdot g^{-j} \in H$ implying by the definition of m and $r < m$ that $r = 0$, thus $h = g^k$ as desired. In particular, $H = \langle g \rangle = \langle a^m \rangle$. □

Corollary 1.1. *If H is a nontrivial subgroup of $(\mathbb{Z}, +)$ then $\exists m \in Z$: $H = \langle m \rangle = m\mathbb{Z}$.*

Note that the problem to describe all subgroups of $(\mathbb{Z}^2, +)$ is not so trivial.

Corollary 1.2. *Any cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$ for some integer $m \geq 1$. In particular, two cyclic groups of the same order are isomorphic.*

Proof. Let $G = \langle a \rangle$ be a cyclic group and $f_a : \mathbb{Z} \to G$ be given by $f_a(n) = a^n : \mathbb{Z} \to G$. Then f_a is a surjective homomorphism. First let G be infinite cyclic. Then $f_a(n) = f_a(m)$ yields $f_a(n - m) = e \Leftrightarrow a^{n-m} = e$ implying $n - m = 0$, thus f_a is injective. Hence f_a is an isomorphism and $G \approx \mathbb{Z}$. Next, let G be finite cyclic and let m is the smallest positive integer such that $a^m = e$. Then the same argument shows that Ker $f_a = m\mathbb{Z}$, hence

$$0 \xrightarrow{i} m\mathbb{Z} \xrightarrow{\text{in}} \mathbb{Z} \xrightarrow{f_a} G \xrightarrow{j} 0 \tag{1.4}$$

is exact. By Proposition 1.7 $G \approx \mathbb{Z}/m\mathbb{Z}$, as claimed. □

Proposition 1.14.

(i) *If G is a cyclic group and $f : G \to G'$ is a homomorphism then $f(G)$ is cyclic.*

(ii) *An infinite cyclic group has exactly two generators (if a is a generator, then a^{-1} is the only other generator).*

(iii) *Let G be a finite cyclic group of order n, and let x be a generator. The set of generators of G consists of those powers x^ν such that ν is relatively prime to n.*

(iv) *Let G be a cyclic group, and let a, b be two generators. Then there exists an automorphism of G mapping a onto b. Conversely, any automorphism of G maps a on some generator of G.*

(v) *Let G be a cyclic group of order n. Let d be a positive integer dividing n. Then there exists a unique subgroup of G of order d.*

(vi) *Let G_1, G_2 be cyclic of orders m, n respectively. If m, n are relatively prime then $G_1 \times G_2$ is cyclic.*

(vii) *Let G be a finite abelian group. If G is not cyclic, then there exists a prime p and a subgroup of G isomorphic to $C \times C$, where C is cyclic of order p.*

Proof. **(i)** Let $G = \langle a \rangle$. Then $f(a)$ is obviously a generator of $f(G)$ which is therefore cyclic.

(ii) obvious.

(iii) Let $G = \langle x \rangle$, $o(x) = |G| = n$ and let $G = \langle x^\nu \rangle$. Then $x = (x^\nu)^k$ for some integer k, hence $x^{\nu k - 1} = e$, implying $\nu k \equiv 1 \mod n$, thus $\gcd(n, \nu) = 1$. Conversely, if $\gcd(n, \nu) = 1$ then there exist $k \in \mathbb{Z}$ such that $k\nu \equiv 1 \mod n$, implying $(x^\nu)^k = x$. It follows that $G = \langle x^\nu \rangle$.

(iv) Let $G = \langle a \rangle = \langle b \rangle$. If $|G| = \infty$ then by (i) $b = a^{\pm 1}$, and the claim holds for $f_+(x) = x$ or $f_-(x) = x^{-1}$. Now let $n = |G| < \infty$. Then by (ii) there exist $\nu, k \in \mathbb{Z}$ such that $b = a^\nu$ and $k\nu - n = 1$. Define $f(x) = x^\nu : G \to G$. Clearly, f is a homomorphism and $f(a) = b$. If $x \in \operatorname{Ker} f$ then $e = x^\nu$, hence $e = x^{k\nu} = x^{n+1} = x$ which yields $x = e$. Therefore f is injective endomorphism, thus an isomorphism. In the converse direction, if f is an automorphism of $G = \langle a \rangle$ then $b = f(a)$ is a generator of $f(G) = G$.

(v) The existence: let $d|n$ and $m = n/d$, then $H = \langle a^m \rangle$ has order d. Let $H' \leqslant G$ be another subgroup of order d. Let $f_a : \mathbb{Z} \to G$ be a surjective homomorphism as in (1.4). Then $H = f_a(m\mathbb{Z})$. Furthermore, $f_a^{-1}(H')$ is a (cyclic) subgroup of $\mathbb{Z}$, hence by Corollary 1.1 there exists $k \in \mathbb{Z}^+$ such that $f_a^{-1}(H') = k\mathbb{Z}$. So $H' = f_a(k\mathbb{Z})$.

(vi) Let $G_1 = \langle a \rangle$ and $G_2 = \langle b \rangle$ be cyclic groups of orders m, n, relatively prime. Consider the homomorphism $f(k) = (a^k, b^k) : \mathbb{Z} \to G_1 \times G_2$. Then

$$k \in \operatorname{Ker} f \quad \Leftrightarrow \quad a^k = e_1 \text{ and } b^k = e_2 \quad \Leftrightarrow \quad k|m \text{ and } k|n \quad \Leftrightarrow \quad k|nm \quad \Leftrightarrow \quad k \in mn\mathbb{Z}.$$

Thus $\operatorname{Ker} = mn\mathbb{Z}$. In order to prove the surjectivity, notice that the cardinality of $|G_1 \times G_2| = |G_1| \cdot |G_2| = nm$. On the other hand, note that $\{f(i) : 1 \leq i \leq mn\}$ contains pairwise distinct elements, because otherwise there exist $1 \leq i < j \leq mn$ such that $f(i) = f(j) \Leftrightarrow i - j \in \operatorname{Ker} f = mn\mathbb{Z}$, a contradiction. Hence $f(\mathbb{Z}) = G_1 \times G_2$. This proves that f is an isomorphism.

(vii) Is left as an exercise. □

Corollary 1.3. *In summary, there exists a natural bijection*

subgroups of a cyclic group $G \longleftrightarrow$ all divisors of $|G|$

Corollary 1.4 (Cauchy's theorem)**.** *If G is a finite abelian group and a prime p divides $|G|$ then there exists a (cyclic) subgroup of order p.*

Proof. Proof is by induction of $\pi(n)$, where $\pi(n) = \sum_{i=1}^{s} k_i$ if $n = \prod_{i=1}^{s} p_i^{k_i}$; in particular, $\pi(n) = 1$ iff p is prime). If $\pi(n) = 1$ then n is prime, hence G is a simple cyclic group of order n, the claim is trivial. Let our claim is valid for all groups with order such that $\pi(|G|) \leq n-1$. Suppose that $\pi(|G|) = n$ and p be a prime divisor of n. Let $e \neq x \in G$. (a) If $p|o(x)$ then by (v) in Proposition 1.14 there exists (a unique) subgroup of $\langle x \rangle$ of order p. (b) If not, i.e. $p \nmid m := o(x)$, then since G is abelian $H = \langle x \rangle \trianglelefteq G$ and $|H| > 1$. Let $G' = G/H$ then $|G'| = |G|/|H| = |G|/m$, hence $\pi(|G'|) < \pi(|G|)$ and on the other hand p divides $|G'|$ because m is coprime with p. Thus the statement is valid for G', implying the existence of an element $yH \in G'$ of order p. But $o(yH)|o(y)$ because $(yH)^{o(y)} = y^{o(y)}H = H$. By Proposition 1.12, $p|o(y)$, therefore we are in position of (a), the claim follows. □

1.8. Operations of a group on a set

Let G be a group and let S be a set. An **operation** or an **action** of G on S is a homomorphism is a map

$$(x, s) \mapsto xs : G \times S \to S. \tag{1.5}$$

such that

(a) $x(ys) = (xy)s$

(b) $es = s$ for all $s \in S$.

- A map $f : S \to S'$ between two G-sets is called a **morphism of G-sets**, or a **G-map**, if
$$f(xs) = xf(s), \qquad \forall x \in G, s \in S.$$
- Given $s \in S$, the **stabilizer** (or the **isotropy group**)) of s is the subgroup
$$G_s = \{x \in G : xs = s\}.$$
- For any $s, s' \in S$, $y \in G$ such that $ys = s'$ there holds $G_{s'} = yG_sy^{-1}$. Indeed,
$$G_{s'} = \{x \in G : xs' = s'\} = \{x \in G : xys = ys\} = \{x \in G : y^{-1}xys = s\} \overset{\text{why?}}{=} yG_sy^{-1}.$$
- An action is called **faithful** if for any $x, y \in G$, there exists $s \in S$ such that $xs \neq ys$, in other words, if $\bigcap_{s \in S} G_s = \{e\}$.
- $s \in S$ is called a **fixed point** if $G_s = G$. The set of fixed points is denoted by $\mathrm{Fix}(S)$
- The set Gs is called an **orbit** of s under G. The set or orbits under the action of G form a partition of S.
- The action is **transitive** if and only if it has only one orbit. The set of all orbits of S under the action of G is written as S/G.

Proposition 1.15 (The Orbit-stabilizer formula)**.** *Let $s \in S$. Then there exists a natural bijection $f : G/G_s \to Gs$. In particular,*

$$|Gs| = (G : G_s) = |G|/|G_s| \tag{1.6}$$

and

$$|S| = \sum_{i \in I} (G : G_{s_i}), \tag{1.7}$$

where s_i are representatives of distinct orbits.

Proof. Note that

$$xs = ys \quad \Leftrightarrow \quad s = x^{-1}ys \quad \Leftrightarrow \quad x^{-1}y \in G_s \quad \Leftrightarrow \quad x \equiv y \mod G_s.$$

This shows that $f(xG_s) = xs : G/G_s \to Gs$ is well defined and also that f is a bijection onto the s-orbit. This yields (1.6), and therefore by the disjointedness of orbits also (1.7) □

Definition 1.8. Let p be a prime number. A group G of finite order is called a p-**group** if $|G| = p^k$, where $k \geq 1$. A subgroup of an arbitrary group is a p-**subgroup** if it is a p-group.

Corollary 1.5 (**The p-group fixed point theorem**)**.** *If G is a p-group and S is a finite G-set then*

$$|\operatorname{Fix}(S)| \equiv |S| \mod p.$$

Proof. We have that s is a fixed point if and only if $(G : G_s) = 1$, otherwise $G_s \neq G$, hence G_s is a proper subgroup of G, therefore $|G_s| = p^i \equiv 0 \mod p$, $1 \leq i \leq k$. Using (1.7),

$$|S| = \sum_{i \in I} (G : G_{s_i}) \equiv \sum_{G_{s_i} = G} (G : G_{s_i}) \equiv |\operatorname{Fix}(S)| \mod p.$$

□

The actions of a group G on itself defined by $x * y = xy$ (resp. by $x.y = xyx^{-1}$) is called **translation** (resp. **conjugation**).

Given a subset $E \subset G$, the set xEx^{-1} (where $x \in G$) is called a **conjugate** to E. The **conjugacy class** $Cl(E)$ of E is the set of all conjugates of E.

A conjugacy class of a subgroup $H \leq G$ is a subgroup.

Corollary 1.6. *If $H \leq G$ then $|Cl(H)| = (G : N_H)$.*

Proof. Note that G acts on the set $\mathcal{G}$ of all subgroups of G by conjugation: for any $H \in \mathcal{G}$ and $x \in G$: $xHx^{-1} \in \mathcal{G}$. Thus $\mathcal{G}$ is a G-set. The stabilizer of $H \in \mathcal{G}$ is $G_H = \{x \in G : xHx^{-1} = H\} = N_H$, i.e. the normalizer of H. Then by (1.6), the order of the orbit $G.H$ is equal the index $(G : N_H)$. □

The next formula expresses the order of a group in terms of the order of its *center* and the number of *cosets of the normalizers* of certain elements in the group.

Proposition 1.16 (**Class equation**). *Let G be a group. Then*

$$|G| = |Z_G| + \sum_{i\in I}(G : N_{x_i}) = |Z_G| + |G|\sum_{i\in I}\frac{1}{|N_{x_i}|} \tag{1.8}$$

where $x_i \in G$ are representatives of the distinct conjugacy classes of size > 1 (so the x_i are not elements of Z_G). Furthermore, for any x, $Z_G \trianglelefteq N_x$.

Proof. Let G act on itself by conjugations. Then the stabilizer $G_x = \{y \in G : yxy^{-1} = x\} = N_x$, the normalizer of x. Furthermore, $N_x = G$ if and only if $x \in Z_G$ which is equivalent to that the orbit of x is trivial. This proves (1.8). The last claim follows from the fact that Z_G commutes with all elements of G, thus $Z_G \trianglelefteq N_x$ for any x. □

1.9. Sylow's theorem

The classification: there exists a complete classification of all *finite simple* groups. Every such group belongs to one of 18 countably infinite families, or is one of 26 **sporadic** groups that do not follow such a systematic pattern. The largest is the Monster of order

$$\begin{aligned}|G| &= 2^{46}\cdot 3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71\\ &= 808017424794512875886459904961710757005754368000000000\end{aligned}$$

Given a group G, H is a p-**Sylow subgroup** if the order of H is p^n and if p^n is the highest power of p dividing the order of G.

Theorem 1.2. *Let a prime p divide $|G| < \infty$. Then there exists a p-Sylow subgroup of G.*

Proof. By induction by the order $\pi(|G|)$. If $\pi(|G|) = 1$ then $|G|$ is prime, hence G is cyclic, and the p-Sylow subgroup is G itself. Let the statement is true for all $\pi(|G|) \le n-1$, $n \ge 2$. Let $\pi(|G|) = n$ and let p^k is the highest power of p dividing the order of G.

Case a. If there exists a subgroup $H \lneqq G$ such that $p \nmid (G : H)$ then $\pi(|H|) < n$ and p^k is the highest power of p dividing $|H|$, thus by induction there exists a p-Sylow subgroup $H' \leqslant H$ of order p^k. Then $H' \leqslant G$ is a desired p-Sylow subgroup of G.

Case b. If not then for any *proper* subgroup $H \lneqq G$, $(G : H)$ is divisible by p. Then by the class equation (1.8) p divides $|Z_G|$, in particular $|Z_g| \ge p \ge 2$. Since the center Z_G is a commutative subgroup, Cauchy's theorem (Corollary 1.4 above) yields the existence of en element $a \in Z_G$ with $o(a) = p$. Then $\langle a\rangle \trianglelefteq Z_G \trianglelefteq G$ (since Z_G commute with any element of G). Let $G' = G/\langle a\rangle$. Then $|G'| = |G|/o(a) = |G|/p$, hence $\pi(|G'|) < \pi(|G|)$, therefore by induction there exists a p-Sylow subgroup H' of G'. Clearly, $|H'| = p^{k-1}$. If $H = f^{-1}(H)$, where $f : G \to G/\langle a\rangle$ is the canonical projection, then $\langle a\rangle \trianglelefteq H \leqslant G$, $|H| = p|H'| = p^k$. The H is a desired p-Sylow subgroup of G. □

Theorem 1.3.

(i) *If H is a p-subgroup of G then it is contained in a p-Sylow subgroup.*

(ii) *Given a finite group G and a prime number p, all Sylow p-subgroups of G are conjugate to each other.*

(iii) *The number n_p of p-Sylow subgroups of G is $|G|/|N_P|$, where P is any p-Sylow subgroup. In particular, if $|G| = mp^k$ then $n_p|m$.*

(iv) $n_p \equiv 1 \mod p$.

Proof. (i) Let P be a p-Sylow subgroup of G, i.e. $|G| = p^k m$, $p \nmid m$ and $|P| = p^k$. Let H act on G/P (which may not be a group!) by the left multiplication. The the action is well-defined and by Corollary 1.5,

$$\mathrm{Fix}(G/P) \equiv |G/P| = (G : P) = |G|/|P| = m \not\equiv 0 \mod p$$

thus $\mathrm{Fix}(G/P) \neq \emptyset$, implying the existence of some $x \in G$ such that xP is a fixed point of the action, i.e. $hxP = xP$ for all $h \in H$. The latter yields $x^{-1}hx \in P$, i.e. $x^{-1}Hx \subset P$. Since the conjugate $P' = xPx^{-1}$ is a p-Sylow subgroup, we have (i). In particular, if $|H| = |P| = p^k$ then obviously $x^{-1}Hx = P$, implying (ii).

(iii) Let G act on the set of subgroups by conjugation. Then by (ii) the set $Syl_p(G)$ of all p-Sylow subgroups of G is an orbit. The orbit-stabilizer formula yields the desired relation:

$$n_p = |Syl_p(G)| = \frac{|G|}{|G_P|} = \frac{|G|}{|N_P|}.$$

Also, since $P \leqslant N_P$, we have $|N_P| = |P|l = p^k l$ for some integer l, thus $n_p = m/l$, i.e. divides m.

(iv) Finally, let a p-Sylow subgroup P act on $Syl_p(G)$ by conjugation. By Corollary 1.5, $|\mathrm{Fix}(Syl_p(G))| \equiv n_p \mod p$. Since $xPx^{-1} = P$ for any $x \in P$, P is a fixed point of the action. Let $Q \in \mathrm{Fix}(Syl_p(G))$ be an fixed point. Then $xQx^{-1} = Q$ for any $x \in P$ implying that $P \subset N_Q$, and thus $P \leqslant N_Q$. Also $Q \leqslant N_Q$. Since P and Q are obviously p-Sylow subgroups of N_Q, by (ii) they conjugate in N_Q. But Q is a normal subgroup of N_Q, therefore its conjugate (in N_Q) is necessarily Q itself, thus $P = Q$. This proves that $|\mathrm{Fix}(Syl_p(G))| = 1$, thus $n_p \equiv 1 \mod p$.

□

Corollary 1.7. *$n_p = 1$ if and only if the (unique) p-Sylow subgroup is normal subgroup of G.*

Proof. Indeed, by (ii) $n_p = 1$ iff $xPx^{-1} = P$ for any x, i.e. P is normal. □

Example 1.17. Show that there is no simple group of order 200.

Solution: Since $200 = 2^3 \cdot 5^2$, the number of Sylow 5-subgroups $n_5 \equiv 1 \mod 5$ and a divisor of 8. Thus there is only one Sylow 5-subgroup, and it is a proper nontrivial normal subgroup.

Example 1.18. How many elements of order 7 are there in a *simple* group of order 168?

Solution: $|G| = 168 = 2^3 \cdot 3 \cdot 7$. The number of Sylow 7-subgroups: $n_7 \equiv 1 \mod 7$ (i.e. $1, 8, 15, 22, \ldots$) and n_7 divides $|G|/7 = 24$. The only possibilities are 1 and 8. Since the group

is simple, there is no proper normal subgroups, hence $n_7 \neq 1$, i.e. $n_7 = 8$. The subgroups all have the identity in common (only!), leaving $8 \cdot (7-1) = 48$ elements of order 7.

Exercises

Exercise 1.12. Prove that if $|G| = pq$ with $p < q$, both odd primes, and $p \nmid q - 1$, then G is cyclic.

Exercise 1.13. (a) Prove that any p-group has a nontrivial center.

(b) Prove that any group of order p^2 is abelian.

Exercise 1.14. Show that any group of order 992 must have a proper normal subgroup.

1.10. Free abelian groups

All abelian groups will be in additive notation in this section with 0 being the identity.

Given a family $\{A_i\}_{i\in I}$ of additive abelian groups, we define the **direct sum**

$$A = \bigoplus_{i\in I} A_i$$

to be the subset of the direct product $\prod_{i\in I} A_i$ consisting all families $\mathbf{x} = (x_i)_{i\in I}$ with $x_i \in A_i$ and $x_i = 0$ a.e., i.e. for all but finitely many $i \in I$. Then A is a subgroup of $\prod_{i\in I} A_i$. Define the imbedding map:

$$\lambda_i : A_i \to A : \lambda_i(x_i) = 0 + \ldots + 0 + x_i + \ldots.$$

Then λ_i is an injective homomorphism.

Proposition 1.17 (The **universal property of the direct sum**). *Let $\{f_i : A_i \to B\}$ be a family of homomorphisms into an abelian group B. Then there exists a unique homomorphism*

$$f : \bigoplus_{i\in I} A_i \to B \tag{1.9}$$

such that $f \circ \lambda_i = f_i$.

Proof. Define a map $f : \bigoplus_{i\in I} A_i \to B$ by $f(\mathbf{x}) = \sum_{i\in I} f(x_i)$, where the last sum is well-defined. Then f is a homomorphism and $f \circ \lambda_i(x_i) = f_i(x_i)$, $\forall x_i \in A_i$. Conversely, if a homomorphism g satisfies (1.9) then $f \equiv g$. □

If A is an abelian group and B, C are subgroups of A such that $B + C = A$ and $B \cap C = \{0\}$ then the map $(x, y) \mapsto x + y : B \times C \to A$ is an isomorphism. We write then $A = B \oplus C$. The latter is expressed as A is the **internal direct sum** of B and C. Similarly one defines $A = \bigoplus_{i=1}^{n} B_i$.

Definition 1.9. A subset $\{e_i\}_{i\in I}$ of an abelian group A is called a **basis** for A if $\forall x \in A$ there exists a unique representation $x = \sum_{i\in I} x_i e_i$ with $x_i \in \mathbb{Z}$ and almost all $x_i = 0$. An abelian group is called **free** if it has a basis.

It is easy to see that the following conditions are equivalent:

- $\{e_i\}_{i\in I}$ is a basis of an abelian group A;
- $\langle\{e_i\}_{i\in I}\rangle = A$ and $\sum_{i\in I} x_i e_i = 0$ implies $x_i = 0$;

Example 1.19. $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ is not free because the representation is not unique.

Example 1.20. $\mathbb{Z}\oplus\mathbb{Z}$ is a free abelian group with a basis $\{e_1 = (1,0), e_2 = (0,1)\}$.

Proposition 1.18. *A is free if and only if $A \approx \bigoplus_{i\in I}\mathbb{Z}$. Furthermore, if A is a finitely generated abelian group with a basis $\{e_1,\dots,e_n\}$ then every basis consists of n elements.*

Proof. Indeed, the factor group $A/2A$ consists of all cosets of the form

$$a_1e_1 + \ldots + a_ne_n + 2A, \quad (a_1,\dots,a_n)\in\{0,1\}^n,$$

thus $(A : 2A) = 2^n$. The left hand side does not depend on a choice of a basis, this proves the claim. □

Definition 1.10. The number of elements in a basis of a free abelian group A will be called the **rank** of A.

Proposition 1.19. *Let $\{e_i\}_{1\le i\le n}$ be a basis of a free abelian group A of rank n. Given an integer matrix $(a_{ij})_{1\le i,j\le n}$, the set $\{v_i\}_{1\le i\le n}$, where $v_i = \sum_{j=1}^n a_{ij}e_j$, is a basis of A if and only if* $\det A = \pm 1$.

Proof. If $\det A = \pm1$ then $A^{-1} = (a^{ij})$ is also integer valued, thus $e_i = \sum_{j=1}^n a^{ij}v_j$, hence if $x = \sum_{i=1}^n m_ie_i$ ($m_i\in\mathbb{Z}$) is the decomposition of an arbitrary $x\in A$ then $x = \sum_{i,j=1}^n a^{ij}m_iv_i$ is the representation of x in $(v_1,\dots,v_n)$ with integer coefficients. The uniqueness is by virtue of $\det A\neq 0$. Conversely, if $(v_1,\dots,v_n)$ is a basis then for each e_k there exist integer numbers b_{ki} such that $e_k = \sum_{i=1}^n b_{ki}v_i$. Thus $e_k = \sum_{i=1}^n b_{ki}\sum_{j=1}^n a_{ij}e_j$, hence by the uniqueness $\sum_{i,j=1}^n b_{ki}a_{ij} = \delta_{ij}$, i.e. $B = A^{-1}$, implying that A^{-1} is integer valued. Since $1 = \det I = \det A\det A^{-1}$ and the both latter determinants are integer, we have $\det A = \pm1$. □

Example 1.21. Since $\mathbb{Z}$ is a free Abelian group of rank 1, the previous theorem shows that every basis for $\mathbb{Z}$ has cardinality 1. Since the only cyclic generators of $\mathbb{Z}$ are ±1 we have that the only basis for $\mathbb{Z}$ are 1 and -1. Thus note that $\{2,3\}$ is a generating set for $\mathbb{Z}$ (why?) which does not contain a $\mathbb{Z}$-basis of $\mathbb{Z}$ *as a subset*. Similarly note that $\{2\}$ is a $\mathbb{Z}$-independent subset of $\mathbb{Z}$ which cannot be *extended* to a $\mathbb{Z}$-basis of $\mathbb{Z}$. So in these two respects, Z-basis are different than basis in vector spaces.

The main result of the classification theory is

Theorem 1.4 (The fundamental theorem of finitely generated abelian groups)**.**

- (Invariant factor decomposition) *If A is a finitely generated abelian group, then*

$$A \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \mathbb{Z}_{n_s}$$

where the integers $r\ge 0$ and $2\le n_1|n_2|\dots|n_s$. Moreover, this expression is unique.

- (Primary decomposition) *One can also write A as*

$$A \cong \mathbb{Z}^r \times \mathbb{Z}_{p_1^{i_1}} \times \cdots \mathbb{Z}_{p_m^{i_m}}$$

where the numbers p_i are (not necessarily distinct) prime numbers and the representation is unique. In particular, A is finite if and only if $r = 0$.

The latter statements are equivalent.

Example 1.22. $\mathbb{Z}_{24} \cong \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3$

The integer r is called the free **rank** or **Betti number** of A and the integers $n_1, n_2, \ldots, n_s$ are called the **invariant factors** of A. The description is called the invariant factor decomposition of A. If A is finite, we call s the rank, and A is of type $(n_1, n_2, \ldots, n_s)$.

Given a S, define $Z\langle S\rangle$ (or $F_{\text{ab}}(S)$) the **free abelian group generated by** S as the set of all maps $\phi : S \to \mathbb{Z}$ such that $\phi(x) = 0$ for almost all $x \in S$. Clearly, $Z\langle S\rangle$ is an abelian group. Let $k \cdot x$ denote the map

$$(k \cdot x)(y) = \begin{cases} k, \text{ if } y = x; \\ 0, \text{ otherwise.} \end{cases}$$

Then for any $\phi \in Z\langle S\rangle$ there exist $k_1, \ldots, k_n \in \mathbb{Z}$ and $x_1, \ldots, x_n \in S$ (all distinct) such that

$$\phi = \sum_{i=1}^{n} k_i \cdot x_i.$$

Such a representation is obviously unique. Then the set S maps into $\mathbb{Z}\langle S\rangle$ by $f(x) = 1 \cdot x$. Then

$$\langle f(S)\rangle = \mathbb{Z}\langle S\rangle$$

Theorem 1.5 (Structure of subgroups of $\mathbb{Z}^n$)**.** *Let H be a nontrivial subgroup of $\mathbb{Z}^n$. Then there exists a basis $x_1, \ldots, x_n$ of $\mathbb{Z}^n$ and integers $1 \le d_1 | d_2 | \ldots | d_s$ for some $1 \le r \le n$ such that $d_1 x_1, \ldots, d_r x_r$ is a basis of H.*

Proof. The proof is by induction on the rank. For $n = 1$ the claim follows from the fact that any subgroup of $\mathbb{Z}$ has the form $\mathbb{Z}d$ for some $d \ge 1$. Suppose that the theorem is valid for any rank $\le n - 1$, where $n \ge 2$.

Let $H \leqslant \mathbb{Z}^n$ be a nontrivial subgroup. Let $E \subset \mathbb{Z}^+$ denote the set of all possible *positive* coordinates of all $0 \ne h \in H$ in any basis of $\mathbb{Z}^n$. The set E is nonempty because if $h = \sum_{i=1}^{n} m_i x_i$ is the decomposition in an arbitrary basis $(x_1, x_2, \ldots, x_n)$ of $\mathbb{Z}^n$ then $m_i \ne 0$ for some i, therefore choosing $-h$ instead of h if needed, one can assume that $m_i > 0$. Thus $m_i \in E$. Let $d_1 = \min E$. In other words, d_1 is the smallest positive integer than occurs as a component of an element $h \in H$ with respect to some basis of $\mathbb{Z}^n$. We shall repeatedly use the following principle: If $0 \ne h \in H$, $(x_1, x_2, \ldots, x_n)$ is a basis of $\mathbb{Z}^n$ then

$$h = a_1 x_1 + \ldots + a_n x_n \text{ and } 0 \le a_1 \le d_1 - 1 \text{ implies } a_1 = 0. \qquad (*)$$

By the definition of d_1, there exists a basis $(y_1, y_2, \ldots, y_n)$ of $\mathbb{Z}^n$ and $0 \ne h \in H$ such that $h = d_1 y_1 + s_2 y_2 + \ldots + s_n y_n$ (we reorder the basis elements if needed to ensure that d_1 is the

first coordinate). Now let us write $s_k = q_k d_1 + r_k$, where $q_k \in \mathbb{Z}$ and $0 \leq r_k \leq d_1 - 1$. This yields

$$h = d_1(y_1 + q_2 y_2 + \ldots + q_n y_n) + r_2 y_2 + \ldots r_n y_n.$$

By Proposition 1.19, $(z_1, z_2, \ldots, z_n)$ with $z_1 = y_1 + q_2 y_2 + \ldots + q_n y_n$ and $z_i = y_i$ for $2 \leq i \leq n$ is a basis of $\mathbb{Z}^n$. By $(*)$ $r_i = 0$ for all $2 \leq i \leq n$, implying the existence of a basis $(z_1, z_2, \ldots, z_n)$ such that $d_1 z_1 \in H$.

Let $G = \langle z_2, \ldots, z_n \rangle$. Let $T = H \cap G$. If T is trivial then $H \subset \langle z_1 \rangle$ and we are done. Let T is a nontrivial subgroup of G. Since G is free abelian of rank $n-1$, by the induction assumption there exists a basis $(w_2, \ldots, w_n)$ of G and positive integers $d_2 | \ldots | d_r$ such that $(d_2 w_2, \ldots, d_r w_r)$ is a basis of T. Since $(w_1, w_2, \ldots, w_n)$ with $w_1 = z_1$ is a basis of G (why?), we have for any $h \in T$:

$$h = a_1 w_1 + \ldots + a_n w_n, \quad a_i \in \mathbb{Z}.$$

Write $a_1 = d_1 q + r$, $q \in \mathbb{Z}$ and $0 \leq r \leq d_1 - 1$. Since $w_1 = z_1$ we have

$$h - q(d_1 z_1) = r z_1 + a_2 w_2 + \ldots + a_n w_n,$$

where the left hand side $h - q(d_1 z_1) \in H$, therefore by $(*)$ we have $r = 0$, thus

$$h - q(d_1 z_1) = a_2 w_2 + \ldots + a_n w_n \in G \cap H = T = \langle d_2 w_2, \ldots, d_r w_r \rangle$$

so $h \in \langle d_1 z_1, d_2 w_2, \ldots, d_r w_r \rangle$. Thus $H \leqslant \langle d_1 z_1, d_2 w_2, \ldots, d_r w_r \rangle \leqslant H$. The system $\{d_i z_i\}_{1 \leq i \leq r}$ obviously $\mathbb{Z}$-linearly independent, thus is a basis of H. Finally, to show that $d_1 | d_2$ let us consider $h = d_1 w_1 + d_2 w_2 \in H$ and write $d_2 = q d_1 + r$, with $0 \leq r \leq d_1 - 1$. Then $h = d_1(w_1 + q w_2) + r w_2$ and $(w_1 + q w_2, w_2 \ldots, w_n)$ is a new basis of $\mathbb{Z}^n$, thus by $(*)$ $r = 0$, hence $d_1 | d_2$, and the theorem is proved. □

Lemma 1.1. *Let $f : A \to A'$ be a surjective homomorphism of two abelian groups, where A' is free. Let $B = \operatorname{Ker} f$. Then there exists a free abelian subgroup $C \leqslant A$ and $f : C \to A'$ is an isomorphism, and such that $A = B \oplus C$.*

Proof. Let $\{x'_i\}_{i \in I}$ be a basis of A'. Let $x_i \in A$ such that $f(x_i) = x'_i$. Define $C = \langle \{x_i\}_{i \in I} \rangle$. Then $\{x_i\}_{i \in I}$ is a basis of C. Indeed, it generates C and if $\sum_{i \in I} n_i x_i = 0$ then

$$0 = f(\sum_{i \in I} n_i x_i) = \sum_{i \in I} n_i f(x_i) = \sum_{i \in I} n_i x'_i,$$

implying all $n_i = 0$. Furthermore, if $x \in B \cap C$ then $x = \sum_{i \in I} n_i x_i$ and $f(x) = 0$, again implying $n_i = 0$. Thus $B \cap C = \{0\}$. Finally, if $x \in A$ an arbitrary element then $f(x) = \sum_{i \in I} n_i x'_i$, thus setting $c = \sum_{i \in I} n_i x_i$ and $b = x - c$ we have $f(b) = 0$, i.e. $c \in C$ and $b \in B$. This yields $A = B \oplus C$. □

Theorem 1.6. *Let A be a free abelian group of finite rank and $B \leqslant A$. Then B is also a free abelian group and the rank of $B \leq$ rank of A.*

Proof. The proof is by induction by the rank of A. For $\operatorname{rank}(A) = 1$, $A \cong \mathbb{Z}$ and the claim is trivial: any subgroup B of $\mathbb{Z}$ is $m\mathbb{Z}$ for some integer m, thus $B = \langle m \rangle$. Now suppose the claim

holds true for all free abelian groups of rank $\leq n$, where $n \geq 2$. Let $\{x_i\}_{1 \leq i \leq n}$ be a basis of A and define the projection homomorphism

$$\pi(m_1x_1 + \ldots + m_nx_n) = m_1x_1 : A \mapsto A' \cong \mathbb{Z}x_1$$

Define $B_1 = \operatorname{Ker}(\pi|_B) = \{x \in B : \pi(x) = 0\}$. Then $B_1 \leqslant A'' = \langle x_2, \ldots, x_n \rangle$. A'' is a free abelian group of rank $n-1$, thus by induction B_1 is free of rank $\leq n-1$. Now, applying Lemma 1.1 to $\pi : B \to B'$, we have $B' \leqslant A'$ and there exists a free abelian subsgroup $C \cong B'$ and such that $B = B_1 \oplus C$. In particular B is free and since $\operatorname{rank} C \leq 1$ (0 or 1), we have $\operatorname{rank} B \leq \operatorname{rank} B_1 + 1 = n = \operatorname{rank} A$, as desired. □

Definition 1.11. If A is an abelian group, $x \in A$ has a finite order (period) if $nx = 0$ for some $n \in \mathbb{Z}^\times$. The set of all elements A_{tor} of finite order in A is called the **torsion subgroup**. An abelian group is called a **torsion group** if $A = A_{\text{tor}}$, that is all elements of A are of finite order.

A_{tor} is indeed a subgroup because if $x, y \in T$ and $n = o(x)$, $m = o(y)$ then $mn(x+y) = 0$, hence $o(x+y) < \infty$. If A_{tor} is trivial then A is called **torsion-free**. A free abelian is torsion-free. (But not conversely!)

A *finitely generated* torsion abelian group is obviously finite.

Theorem 1.7. *Let A be a finitely generated torsion-free abelian group. Then A is free.*

Proof. Assume $S \neq \emptyset$ be a finite set of generators of A. Note that for any $x_1 \in S$, $mx_1 \neq 0$ for any $m \neq 0$ because A is torsion-free. By adding a new element, one can find a maximal subset $x_1, \ldots, x_n$ of S having the property that whenever $m_i \in \mathbb{Z}$ are such that

$$m_1x_1 + \ldots + m_nx_n = 0$$

then all $m_i = 0$. Let $B = \langle x_1, \ldots, x_n \rangle$, then B is free. Given $x \in S \setminus \{x_1, \ldots, x_n\}$, by the maximality condition there exist integers m and $m_1, \ldots, m_n$ such that

$$mx + m_1x_1 + \ldots + m_nx_n = 0.$$

Also $m \neq 0$, otherwise all $m_i = 0$. Thus $mx \in B$ for some $m \neq 0$. Since S is finite, there exists an integer $M \neq 0$ such that $Mx \in B$ for all $x \in S$, therefore $MA \in B$. This yields the existence of a homomorphism

$$\phi(x) = Mx : A \mapsto B' \leqslant B,$$

and $\operatorname{Ker}\phi$ obviously trivial by virtue of the torsion-free property of A. Thus $A \cong B' \leqslant B$, and by Theorem 1.6, B' is free. Thus A is also a free group. □

Now we study torsion groups in more details.

Definition 1.12. If A is an abelian group and p a prime number, we denote by $A(p)$ the set of all elements $x \in A$ whose period is a power of p.

Then $A(p)$ is a torsion group, and is a p-group if it is finite.

Proof. It suffices to show that $A(p)$ is a subgroup of A. To this end, if $o(x) = p^k$ and $o(y) = p^m$ then $p^{k+m}(x+y) = 0$, hence $o(x+y) = p^i$ for some $0 \le i \le k+m$, as desired. □

Theorem 1.8. *Let A be a torsion abelian group. Then A is the direct sum of its subgroups $A(p)$ for all primes p such that $A(p) \neq 0$.*

Proof. Define $A' = \bigoplus_p A(p)$ and let $f(\oplus_p x_p) = \sum_p x_p : A' \to A$. Then f is a homomorphism. Let $x \in \operatorname{Ker} f$, i.e. $\sum_p x_p = 0$. Then for a prime number q, $x_q = -\sum_{p \neq q} x_p$. Since the latter sum is finite, there exists an integer $m \neq 0$ and $(m, q) = 1$ such that $mx_q = 0$. If $x_q \neq 0$ then $q^k x_q = 0$ for some $k \ge 0$, implying (because m and q^k are coprime) that $x_q = 0$, a contradiction. Thus $\operatorname{Ker} f$ is trivial.

Next, if $(r, s) = 1$ then $A_{rs} = A_r \oplus A_s$, where $A_k = \{x \in A : kx = 0\}$. Indeed, $A_r \oplus A_s \leqslant A_{rs}$, and on the other hand there exist integers i, k such that $ir + ks = 1$, therefore $x = irx + ksx \in A_r \oplus A_s$, hence $A_{rs} \leqslant A_r \oplus A_s$. This yields by induction that

$$A_m = \bigoplus_{p|m} A_{p^{k_p}}, \quad m = \prod_{p|m} p^{k_p}$$

Since $A_{p^{k_p}} \leqslant A(p)$, f is surjective and the theorem is proved. □

Example 1.23. Let $A = \mathbb{Q}/\mathbb{Z}$. Then for any $x \in A$ represented by the coset of $m/n \in \mathbb{Q}$ then $nx = 0$ in A, thus A is a torsion abelian group. By the theorem, A isomorphic to the direct sum of its subgroups $A(p)$. Now, each $A(p)$ consists of those elements $x \in A$ which can be represented by a rational number m/p^k, where $k \in \mathbb{Z}^+$.

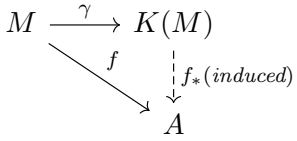
Exercises

Exercise 1.15. Finish the proof of Theorem 1.4 (in the invariant factors form) by using Theorem 1.5.

Exercise 1.16. [1], Problem 43: Let H be a subgroup of a finite abelian group G. Show that G has a subgroup that is isomorphic to G/H.

1.10.1. Appendix*.

Proposition 1.20 (The Grothendieck Group). *Let $(M, +)$ be a commutative monoid. There exists an abelian group $K(M)$ and a monoid homomorphism $\gamma : M \to K(M)$ having the following universal property: if $f : M \to A$ is a homomorphism into an abelian group A, then there exists a unique homomorphism $f_* : K(M) \to A$ making the following diagram commutative:*



Proof. Let $B \leqslant F_{\mathrm{ab}}(M)$ be the subgroup generated by

$$1 \cdot (x+y) - 1 \cdot x - 1 \cdot y.$$

Let $K(M) = F_{\mathrm{ab}}(M)/B$ and let $\gamma : M \to K(M)$ is the composing of

$$\gamma(x) = [1 \cdot x] : M \hookrightarrow F_{\mathrm{ab}}(M) \xrightarrow{\mathrm{can}} F_{\mathrm{ab}}(M)/B.$$

Then γ is a homomorphism and f_* is (uniquely)defined by

$$f_*((1 \cdot x)B) = f(x).$$

□

The universal group $K(M)$ is called the **Grothendieck group**.

1.11. Rings

Exercises

Exercise 1.17. Exercises 2,3,7,11 in [1]

1.12. Polynomials

Exercises

Exercise 1.18. Give an example of a commutative ring with only one maximal ideal.

Exercise 1.19. Let A be a commutative ring. Define $M_2(A)$ as the set of all 2×2-matrices with entries in A.

a) Show that $M_2(A)$ is ring (w.r.t. the natural operations).

b) Prove that the ideals ideal[1] of $M_2(A)$ are precisely the subsets $M_2(\mathfrak{a})$, where $\mathfrak{a}$ is an ideal of A.

Exercise 1.20. Are the following polynomials irreducible in $\mathbb{Q}[x]$:

a) $x^7 + 4x^6 - 18x^5 + 42x^3 - 6$

a) $x^6 + x^3 + 1$?

Exercise 1.21. Show that $x^2 + y^2 + z^2$ is irreducible in $\mathbb{Q}[x, y, z]$.

[1] Two-side ideals

1.13. Modules

1.14. Categories and functors

A **category** $\mathscr{A}$ consists of collection of **objects** $\mathrm{Ob}(\mathscr{A})$. For two objects $A, B \in \mathrm{Ob}(\mathscr{A})$ a set $\mathrm{Mor}(A, B)$ called the set of **morphisms** of A into B. For three objects $A, B, C \in \mathrm{Ob}(\mathscr{A})$ it is defined a law of composition

$$\mathrm{Mor}(A, B) \times \mathrm{Mor}(B, C) \to \mathrm{Mor}(A, C)$$
$$\text{i.e. } (f, g) \mapsto f \circ g$$

satisfying the following axioms:

CAT 1. Two sets $\mathrm{Mor}(A, B)$ and $\mathrm{Mor}(A', B')$ are disjoint unless $A = A'$ and $B = B'$, in which case they are equal.

CAT 2. $\forall A \in \mathscr{A}$ there exists a morphism $\mathrm{id}_A \in \mathrm{Mor}(A, A)$ (the **identity** on A) such that $f \circ \mathrm{id}_B = f = \mathrm{id}_A \circ f$ for all $f \in \mathrm{Mor}(A, B)$.

CAT 3. The law of composition is **associative**, i.e.

$$(h \circ g) \circ f = h \circ (g \circ f), \qquad \forall f \in \mathrm{Mor}(A, B), g \in \mathrm{Mor}(B, C), h \in \mathrm{Mor}(C, D)$$

for any objects $A, B, C, D \in \mathscr{A}$.

Remark 1.1. Category theory was founded by Saunders MacLane and Samuel Eilenberg around 1940.

The collections of all morphisms in a category $\mathscr{A}$ is denoted by $\mathrm{Ar}(\mathscr{A})$ ("arrows of $\mathscr{A}$") and

$$f \in \mathrm{Mor}(A, B) \quad \Leftrightarrow \quad f : A \to B \quad \Leftrightarrow \quad A \xrightarrow{f} B$$

A morphism $f : A \to B$ is called **isomorphism** if there exists $g : B \to A$ such that $f \circ g = \mathrm{id}_A$ and $g \circ f = \mathrm{id}_B$. If $A = B$ then an isomorphism $f : A \to A$ is called **automorphism**.

In general, a morphism of an object A into itself is called an **endomorphism**. The set of endomorphisms of A is denoted $\mathrm{End}(A)$.

Example 1.24.

Set: the category of sets whose morphisms are maps between sets.

Mon: the category of all monoids (morphisms are monoid-homomorphisms). Similarly one defines the category of groups **Grp**.

Vect$_k$: the category of vector spaces over field k (morphisms are linear maps).

Top: the category of topological spaces (morphisms are continuous maps).

We would like to define arrows between categories. Such arrows are called functors. Let $\mathscr{A}$ and $\mathscr{B}$ be categories. A **covariant functor** F of $\mathscr{A}$ into $\mathscr{B}$ is a rule which to each object A in $\mathscr{A}$ associates an object $F(A)$ in $\mathscr{B}$, and to each morphism $f : A \to B$ associates a morphism $F(f) : F(A) \to F(B)$ such that

FUN1. For all A in $\mathscr{A}$ we have $F_{\mathrm{id}_A} = \mathrm{id}_{F(A)}$.

FUN2. If $f : A \to B$ and $g := B \to C$ are two morphisms of $\mathscr{A}$ then $F(f \circ g) = F(f) \circ F(g)$.

In other words, a functor preserves compositions and identity morphisms.

Note that functors can be composed in an obvious way. Also, any category has the **identity functor**.

Example 1.25. A *forgetful* functor **Grp**→**Set**.

Chapter 2

Rings

2.1. Exercises

Exercise 2.1. Prove that if A is a commutative ring and $\mathfrak{a}, \mathfrak{b}$ are two ideals then $\mathfrak{a} + \mathfrak{b} = A$ implies $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

Exercise 2.2. Let A be a ring such that $x^2 = x$ for any $x \in A$. Prove that A is commutative.

Exercise 2.3. Give an example of a ring A such that xA is not a two-sided ideal for some $x \in A$.

Exercise 2.4. Given a commutative ring A, prove that the set $B = \{x \in A | \text{there exists } n \in \mathbb{Z}^+ : x^n = 0\}$ is an ideal of A. Prove that if $\bar{x} \in A/B$ and $\bar{x}^n = 0$ for some integer $n \geq 1$ then $\bar{x} = 0$.

Exercise 2.5. Exercise 11, p.115 in [1]

Bibliography

1. Lang, Serge. Algebra. Graduate Texts in Mathematics, Vol. 211. Springer-Verlag, New York, 2002. xvi+914