GROUP THEORY (MATH 33300)

COURSE NOTES

CONTENTS

Recommended text to complement these notes: J.F. Humphreys, A Course in Group Theory (OUP, 1996).

Date: January 11, 2010.

These notes are mainly based on K. Meyberg's Algebra, Chapters 1 & 2 (in German).

$\longrightarrow$

1. BASICS

1.1. **Definition.** Let G be a non-empty set and fix a map $\circ : G \times G \to G$. The pair $(G, \circ)$ is called a **group** if

(1) for all $a, b, c \in G$: $(a \circ b) \circ c = a \circ (b \circ c)$ (associativity axiom).
(2) there is $e \in G$ such that $e \circ a = a$ for all $a \in G$ (identity axiom).
(3) for every $a \in G$ there is $a' \in G$ such that $a' \circ a = e$ (inverse axiom) .

$\circ$ is called the **composition** (sometimes also **multiplication**) and e is called the **identity element** (or **neutral element**) of G, and a' the **inverse** of a. Where there is no ambiguity, we will use the notation G instead of $(G, \circ)$, and ab instead of $a \circ b$. We will denote by a^n ($n \in \mathbb{N}$) the n-fold product of a, e.g., $a^3 = aaa$.

1.2. **Example.** The simplest examples of groups are:

(1) $E = \{e\}$ (the **trivial group**).
(2) $(\{0\}, +\})$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, where $+$ is the standard addition.
(3) $(\{1\}, \cdot)$, $(\{-1, 1\}, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, where $\cdot$ denotes the usual multiplication and $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ etc.

1.3. **Lemma.** Let a be an element of the group G such that $a^2 = a$. Then $a = e$.

Proof. We have

$$\begin{aligned} a &= ea && \text{(identity axiom)} \\ &= (a'a)a && \text{for some } a' \in G \text{ (inverse axiom)} \\ &= a'a^2 && \text{(associativity axiom)} \\ &= a'a && \text{(by assumption)} \\ &= e && \text{(by definition of } a'). \end{aligned} \tag{1.1}$$

□

1.4. **Exercise.** Show that

(1) If a' is an inverse of a, then $aa' = e$.
(2) $ae = a$ for all $a \in G$.
(3) The neutral element of G is unique.
(4) For every a there is a unique inverse a'. We will denote it by $a^{-1} := a'$.
(5) $(a^{-1})^{-1} = a$.
(6) $(ab)^{-1} = b^{-1}a^{-1}$.

We extend the definition a^n to negative integers $n < 0$ by setting $a^n := (a^{-1})^{-n}$. We also set $a^0 = e$.

1.5. **Definition.** The number of elements of a group G is called the **order** of G and is denoted $|G|$. G is called a **finite** group if $|G| < \infty$ and **infinite** otherwise.

1.6. **Example.** Let $\mathbb{Z}_n$ denote the set $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, where $\overline{m}$ is the residue class modulo n (that is, the equivalence class of integers congruent to m mod n). Then:

(1) $(\mathbb{Z}_n, +)$ is a finite group of order n.
(2) $(\mathbb{Z}_n^*, \cdot)$, with $\mathbb{Z}_n^* = \{\overline{m} \in \mathbb{Z}_n : \gcd(m, n) = 1\}$, is a finite group of order $\varphi(n)$ = the number of integers $< n$ that are coprime to n (Euler's φ function).

1.7. **Definition.** A group G is called **abelian** (or **commutative**), if $ab = ba$ for all $a, b \in G$.

1.8. **Example.** All of the above examples are abelian groups. An example of a non-abelian group is the set of matrices

$$T = \left\{ \begin{pmatrix} x & y \\ 0 & 1/x \end{pmatrix} : x \in \mathbb{R}^*,\ y \in \mathbb{R} \right\} \tag{1.2}$$

where the composition is matrix multiplication.

Proof. We have

$$\begin{pmatrix} x_1 & y_1 \\ 0 & 1/x_1 \end{pmatrix} \begin{pmatrix} x_2 & y_2 \\ 0 & 1/x_2 \end{pmatrix} = \begin{pmatrix} x_3 & y_3 \\ 0 & 1/x_3 \end{pmatrix} \tag{1.3}$$

where $x_3 = x_1 x_2$ and $y_3 = x_1 y_2 + y_1/x_2$. Hence T is closed under multiplication. Matrix multiplication is well known to be associative. The identity element corresponds to $x = 1$, $y = 0$. As to the inverse,

$$\begin{pmatrix} x & y \\ 0 & 1/x \end{pmatrix}^{-1} = \begin{pmatrix} 1/x & -y \\ 0 & x \end{pmatrix} \in T. \tag{1.4}$$

Therefore T is a group. It is non abelian since for example

$$\begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & \frac{1}{2} \end{pmatrix} \neq \begin{pmatrix} 2 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}. \tag{1.5}$$

□

1.9. **Exercise.** Prove the following:

(1) The set

$$\mathrm{SO}(2) = \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} : x, y \in \mathbb{R},\ x^2 + y^2 = 1 \right\} \tag{1.6}$$

forms an abelian group with respect to matrix multiplication. (SO stands for "special orthogonal".)

(2) Let K be a field and $K^{n\times n}$ the set of $n \times n$ matrices with coefficients in K. Then

$$\mathrm{GL}(n, K) := \{A \in K^{n\times n} : \det A \neq 0\} \tag{1.7}$$

is a group with respect to matrix multiplication. (GL stands for "general linear".)

1.10. The easiest description of a finite group $G = \{x_1, x_2, \ldots, x_n\}$ of order n (i.e., $x_i \neq x_j$ for $i \neq j$) is often given by an $n \times n$ matrix, the **group table**, whose coefficient in the ith row and jth column is the product $x_i x_j$:

$$\begin{pmatrix} x_1x_1 & x_1x_2 & \ldots & x_1x_n \\ x_2x_1 & x_2x_2 & \ldots & x_2x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_nx_1 & x_nx_2 & \ldots & x_nx_n \end{pmatrix}. \tag{1.8}$$

The group table completely specifies the group.

1.11. **Theorem.** In a group table, every group element appears precisely once in every row, and once in every column.

Proof. Suppose in the ith row we have $x_i x_j = x_i x_k$ for $j \neq k$. Multiplying from the left by x_i^{-1} we obtain $x_j = x_k$, which contradicts our assumption that x_j and x_k are distinct group elements. The proof for columns is analogous. □

1.12. **Example.** Consider a finite group $G = \{e, a, b\}$ of order 3. If e is the identity, the first row and column are already specified:

$$\begin{pmatrix} e & a & b \\ a & \boxed{?} & ? \\ b & ? & ? \end{pmatrix}. \tag{1.9}$$

If the central coefficient $\boxed{?}$ is chosen to be e, then the ? below can, in view of Theorem 1.11 applied to the second column, only be b—but then there are two b's in the final row. Hence the only possibility is:

$$\begin{pmatrix} e & a & b \\ a & b & e \\ b & e & a \end{pmatrix}. \tag{1.10}$$

We have thus shown that there exists only one group of order 3.

1.13. **Example.** Let $G = \{e, a, b, c\}$ and assume $a^2 = b^2 = e$. Then the group table is

$$\begin{pmatrix} e & a & b & c \\ a & e & \boxed{?} & ? \\ b & ? & e & ? \\ c & ? & ? & ? \end{pmatrix}. \tag{1.11}$$

The only possibility for $\boxed{?}$ is c, otherwise there would be two c's in the last column. Hence

$$\begin{pmatrix} e & a & b & c \\ a & e & c & b \\ b & \boxed{?} & e & ? \\ c & ? & a & ? \end{pmatrix}. \tag{1.12}$$

Again $\boxed{?}$ must be c, and thus

$$\begin{pmatrix} e & a & b & c \\ a & e & c & b \\ b & c & e & a \\ c & b & a & e \end{pmatrix}. \tag{1.13}$$

Hence the group table is completely determined by the relations $a^2 = b^2 = e$. The associativity of the composition law can easily be checked (this is a tedious but instructive exercise). The resulting group is called **Klein four group**.

1.14. **Exercise.** Write down the group tables for all residue class groups $\mathbb{Z}_p^*$ for all primes $p \leq 17$.

1.15. **Exercise.** Let G be the set of symmetries of the regular n-gon (i.e., G comprises reflections at diagonals and rotations about the center). Show that G forms a group of order $2n$, if the composition is the usual composition law for maps.

[This group is called the **dihedral group** D_n; we will meet it again later in the lecture.]

1.16. **Exercise.** Let K be a finite field with q elements. Determine the order of $GL(n, K)$.

2. HOMOMORPHISMS

2.1. **Definition.** Let $(G, \circ)$, $(H, *)$ be groups. The map $\varphi : G \to H$ is called a **homomorphism** from $(G, \circ)$ to $(H, *)$, if for all $a, b \in G$

$$\varphi(a \circ b) = \varphi(a) * \varphi(b). \tag{2.1}$$

2.2. **Example.**

(1) Let e' be the identity element of H. Then map $\varphi : G \to H$ defined by $\varphi(a) = e'$ is a homomorphism.
(2) The map $\exp : \mathbb{R} \to \mathbb{R}^*$, $x \mapsto e^x$, defines a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^*, \cdot)$, since $e^{x+y} = e^x e^y$.
(3) The map $\pi : \mathbb{Z} \to \mathbb{Z}_n$, $m \to \overline{m}$, defines a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_n, +)$.

2.3. **Exercise.** Show that

(1) the maps $\varphi_1, \varphi_2 : \mathbb{R} \to T$ defined by

$$\varphi_1(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \qquad \varphi_2(t) = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}, \tag{2.2}$$

are homomorphisms.
(2) the map $\varphi_3 : \mathbb{R} \to SO(2)$ defined by

$$\varphi_3(t) = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}, \tag{2.3}$$

is a homomorphism.

2.4. **Definition.** A homomorphism $\varphi : G \to H$ is called

(1) **monomorphism** if the map φ is injective,
(2) **epimorphism** if the map φ is surjective,
(3) **isomorphism** if the map φ is bijective,
(4) **endomorphism** if $G = H$,
(5) **automorphism** if $G = H$ and the map φ is bijective.

2.5. **Definition.** Two groups G, H are called **isomorphic**, if there is an isomorphism from G to H. We write $G \simeq H$.

2.6. **Exercise.** Show that $(\mathbb{Z}, +) \simeq (2\mathbb{Z}, +)$.

2.7. **Exercise.** Decide whether the homomorphisms in Exercise 2.3 are mono-, epi-, or isomorphisms.

2.8. **Lemma.** Let $\varphi : G \to H$ be a homomorphism, and let e, e' denote the identity elements of G and H, respectively. Then

(1) $\varphi(e) = e'$.
(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$.
(3) $\varphi(a^n) = \varphi(a)^n$ for all $a \in G$, $n \in \mathbb{Z}$.

[(1) and (2) are of course special cases of (3).]

Proof. (1) We have $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$ and (1) follows from Lemma 1.3.
(2) $\varphi(e) = \varphi(a^{-1}a) = \varphi(a^{-1})\varphi(a)$, which proves (2) in view of (1).
(3) follows from (1) trivially when $n = 0$, and by induction for $n > 0$. For $n < 0$

$$\begin{aligned} \varphi(a^n) &= \varphi((a^{-1})^{-n}) \qquad \text{(by definition)} \\ &= \varphi(a^{-1})^{-n} \qquad \text{(as we have just proved)} \\ &= (\varphi(a)^{-1})^{-n} \qquad \text{(by (2))} \\ &= \varphi(a)^n \qquad \text{(by definition).} \end{aligned} \tag{2.4}$$

□

2.9. **Definition.** Let φ be a homomorphism from $(G, \circ)$ to $(H, *)$, and denote by e, e' denote the respective identity elements. The set

$$\operatorname{im} \varphi = \{\varphi(a) : a \in G\} \subseteq H \tag{2.5}$$

is called the **image** of φ, and

$$\ker \varphi = \{a \in G : \varphi(a) = e'\} \subseteq G \tag{2.6}$$

the **kernel** of φ.

2.10. **Exercise.** Prove that $(\operatorname{im} \varphi, *)$ and $(\ker \varphi, \circ)$ are groups.
[We will return to this problem in the discussion of subgroups.]

2.11. **Theorem.** φ is a monomorphism if and only if $\ker \varphi = \{e\}$.

Proof. Assume φ is injective. If $a \in \ker \varphi$, then $\varphi(a) = e' = \varphi(e)$ and hence by injectivity $a = e$.

Conversely, assume $\ker \varphi = \{e\}$. Let $a, b \in G$ such that $\varphi(a) = \varphi(b)$. We need to show that $a = b$.

$$\begin{aligned} e' &= \varphi(b)\varphi(a)^{-1} \\ &= \varphi(b)\varphi(a^{-1}) \qquad \text{(Lemma 2.8)} \\ &= \varphi(ba^{-1}). \end{aligned} \tag{2.7}$$

Thus $ba^{-1} \in \ker \varphi$, and hence, by our assumption $\ker \varphi = \{e\}$ we conclude $ba^{-1} = e$, i.e., $a = b$. □

2.12. **Theorem.**

(1) If $\varphi : G \to H$ and $\psi : H \to K$ are homomorphisms, then so is $\psi \circ \varphi : G \to K$.
(2) If $\varphi : G \to H$ and $\psi : H \to K$ are isomorphisms, then so is $\psi \circ \varphi : G \to K$.
(3) If $\varphi : G \to H$ is an isomorphism, then so is $\varphi^{-1} : H \to G$.
(4) The identity map $\mathrm{id} : G \to G$, $a \mapsto a$ is an automorphism.

Proof. (1) We have

(2.8)
$$(\psi \circ \varphi)(ab) = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) = \psi(\varphi(a))\psi(\varphi(b)) = (\psi \circ \varphi)(a)(\psi \circ \varphi)(b).$$

(2) In view of (1) it remains to be shown that $\psi \circ \varphi$ is bijective—this is evident and left as an exercise.

(3) Let $x = \varphi(a)$, $y = \varphi(b)$, and so $a = \varphi^{-1}(x)$, $b = \varphi^{-1}(y)$. Now

$$\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y). \tag{2.9}$$

(4) This is evident. □

2.13. The above theorem has an important consequence: If $G \simeq H$ then by (3) $H \simeq G$. If $G \simeq H$ and $H \simeq K$ then by (2) $G \simeq K$. Finally, by (4) we have $G \simeq G$. Hence $\simeq$ defines an equivalence relation on groups.

Recall: Given a set X, an **equivalence relation** R is defined as a subset of $X \times X$ with the properties:

(1) $(x, x) \in R$ for all $x \in R$ (reflexivity axiom).
(2) $(x, y) \in R$ implies $(y, x) \in R$ (symmetry axiom).
(3) $(x, y), (y, z) \in R$ implies $(x, z) \in R$ (transitivity axiom).

If $(x, y) \in R$ we say x and y are **equivalent** and write $x \sim y$.

2.14. Let $\mathrm{Aut}\, G$ be the set of automorphisms $\varphi : G \to G$. Because of Theorem 2.12 (2) and (3) we find that if $\varphi, \psi \in \mathrm{Aut}\, G$, then $\varphi \circ \psi \in \mathrm{Aut}\, G$ and $\varphi^{-1} \in \mathrm{Aut}\, G$. (4) says that $\mathrm{id} \in \mathrm{Aut}\, G$. Hence $(\mathrm{Aut}\, G, \circ)$ is a group, called the **automorphism group** of G.

2.15. **Lemma.** Given $g \in G$, define the map $\varphi_g : G \to G$ by $\varphi_g(a) = gag^{-1}$. Then $\varphi_g \in \mathrm{Aut}\, G$.

Proof. φ_g is a homomorphism since

$$\varphi_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \varphi_g(a)\varphi_g(b). \tag{2.10}$$

It is in fact invertible:

$$\varphi_g^{-1} = \varphi_{g^{-1}} \tag{2.11}$$

since $\varphi_g \circ \varphi_{g^{-1}}(a) = g(g^{-1}ag)g^{-1} = a$, and so φ_g is bijective. □

2.16. **Definition.** $\varphi \in \operatorname{Aut} G$ is called an **inner automorphism** if there is a $g \in G$ such that $\varphi = \varphi_g$. Two elements $a, b \in G$ are called **conjugate** if there is a $g \in G$ such that $\varphi_g(a) = b$. We write $a \sim b$.

2.17. **Exercise.** Show that $\sim$ is an equivalence relation.

2.18. **Exercise.** Show that for $a, b \in G$ the elements ab and ba are conjugate.

2.19. **Theorem.** The map $\Phi : G \to \operatorname{Aut} G$, $a \mapsto \varphi_a$, is a homomorphism.

Proof. We have for any fixed $g \in G$

$$\varphi_{ab}(g) = abg(ab)^{-1} = abgb^{-1}a^{-1} = \varphi_a(bgb^{-1}) = \varphi_a \circ \varphi_b(g), \tag{2.12}$$

so $\varphi_{ab} = \varphi_a \circ \varphi_b$, i.e., $\Phi(ab) = \Phi(a) \circ \Phi(b)$. □

2.20. **Definition.** The kernel of Φ is called the **center** of G and is denoted by $Z(G)$.

Explicitly,

$$\begin{aligned} Z(G) &= \{a \in G : \varphi_a = \mathrm{id}\} \qquad \text{(by definition)} \\ &= \{a \in G : aba^{-1} = b \text{ for all } b \in G\} \\ &= \{a \in G : ab = ba \text{ for all } b \in G\}. \end{aligned} \tag{2.13}$$

Hence $Z(G)$ is the set of elements in G that commute with all elements in G. Note that obviously $Z(G)$ is a group, cf. also Exercise 2.10.

2.21. We have $Z(G) = G$ if and only if G is abelian.

2.22. **Exercise.** Determine all automorphisms of the Klein four group.

2.23. **Exercise.** Show that the symmetry group of a rectangle (that is not a square) is the Klein four group.

2.24. **Exercise.** Set $\zeta := e^{2\pi i/n}$, and let $G = \{\zeta^k : k = 1, \dots, n\}$ be the group of the nth roots of unity, where the composition is standard multiplication in $\mathbb{C}$.

(1) Show that $\varphi : \mathbb{Z} \to G$, $m \mapsto \zeta^m$, is a homomorphism.
(2) Calculate $\ker(\varphi)$.

2.25. **Exercise.** Let G be a group. Show that:

(1) If $\operatorname{Aut} G = \{\mathrm{id}\}$ then G is abelian.
(2) If $x \mapsto x^2$ defines an homomorphism of G, then G is abelian.
(3) If $x \mapsto x^{-1}$ defines an automorphism of G, then G is abelian.

3. SUBGROUPS

3.1. **Definition.** A non-empty subset $H \subseteq G$ is called a **subgroup**, if H is a group with respect to the same composition as in G; we will write in this case $H \leq G$.

H is called a **proper subgroup** if $H \neq G$; we write $H < G$.

3.2. **Example.**

(1) $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.
(2) If $d \in \mathbb{N}$ divides $n \in \mathbb{N}$, then $(n\mathbb{Z}, +) \leq (d\mathbb{Z}, +)$.
(3) The groups in Example 1.8 and Exercise 2.3 are subgroups of $GL(2, \mathbb{R})$.

3.3. **Theorem.** Let G be a group and $H \subseteq G$ a non-empty subset. Then H is a subgroup if and only if

$$(a, b \in H) \Rightarrow (ab \in H \text{ and } a^{-1} \in H). \tag{3.1}$$

Proof. Assume H is a subgroup. Then the image of $H \times H$ under the composition $\circ : G \times G \to G$ satisfies $\circ(H, H) \subseteq H$, i.e., $ab \in H$ for all $a, b \in H$. If e is the identity in H, we have $e^2 = e$, but this means by Lemma 1.3 that e is also the identity in G. Hence the inverse of a in H is also the inverse of a in G, and so $a^{-1} \in H$.

Conversely, assume (3.1). Then the composition $\circ$ on G, restricted to H, yields a map $H \times H \to H$, $(a, b) \mapsto ab$. The map is clearly associative (since this is true in the full set G), and we only need to show that the identity e in G is contained in H. But this follows from taking $b = a^{-1}$ in (3.1). □

3.4. **Corollary.** Let G be a group and $H \subseteq G$ a non-empty subset. Then H is a subgroup if and only if

$$(a, b \in H) \Rightarrow (ab^{-1} \in H). \tag{3.2}$$

Proof. Assume H is a subgroup. Let $a, b \in H$. Then, by Theorem 3.3, $b^{-1} \in H$ and $ab^{-1} \in H$. On the other hand, assume (3.2) holds. In particular (for $a = e$) $b \in H$ implies $b^{-1} \in H$ and hence $(a, b \in H) \Rightarrow (a, b^{-1} \in H) \Rightarrow (ab \in H)$ by (3.2). Thus by Theorem 3.3 H is a subgroup. □

3.5. **Theorem.** Let G be a group and $H \subseteq G$ a **finite** non-empty subset. Then H is a subgroup if and only if

$$(a, b \in H) \Rightarrow (ab \in H). \tag{3.3}$$

Proof. The first implication follows from the previous theorem. Hence assume (3.3) holds. Since G is a group, for every fixed $a \in G$ the map $G \to G$, $x \mapsto ax$, is injective. If $a \in H$, then the restriction of this map to H yields, in view of (3.3), a the map $H \to H$, $x \mapsto ax$, which is still injective. But since H is finite, injective implies surjective and hence bijective. Hence if $y = ax \in H$, the inverse map is $H \to H$,

$y \mapsto x = a^{-1}y$. The choice $y = a$ implies $e \in H$ and the choice $y = e$ implies $a^{-1} \in H$. □

3.6. **Example.** Let $G = \{e, a, b, c\}$ be the Klein four group as defined in 1.13. The above theorem shows that $\{e, a\}, \{e, b\}, \{e, c\}$ are subgroups of G.

3.7. **Theorem.** Consider the groups $H_1 \leq G_1$, $H_2 \leq G_2$ and let $\varphi : G_1 \to G_2$ be a homomorphism. Then

(1) the image $\varphi(H_1)$ is a subgroup of G_2.
(2) the pre-image $\varphi^{-1}(H_2)$ is a subgroup of G_1.

Proof. (1) $\varphi(H_1)$ is evidently non-empty. We have for $a, b \in H_1$ that $\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(H_1)$ and $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H_1)$. The claim follows from Theorem 3.3.

(2) Clearly $e \in \varphi^{-1}(H_2)$ and the latter is non-empty. $a, b \in \varphi^{-1}(H_2)$ implies $\varphi(a), \varphi(b) \in H_2$ and hence $\varphi(ab) = \varphi(a)\varphi(b) \in H_2$ and $\varphi(a)^{-1} = \varphi(a^{-1}) \in H_2$. Therefore $ab, a^{-1} \in \varphi^{-1}(H_2)$, and claim (2) follows from Theorem 3.3. □

3.8. **Corollary.** Let $\varphi : G_1 \to G_2$ be a homomorphism.

(1) $\operatorname{im}\varphi$ is a subgroup of G_2.
(2) $\ker\varphi$ is a subgroup of G_1.

Proof. Apply Theorem 3.7 with $H_1 = G_1$, $H_2 = \{e\}$. □

3.9. With the special choice $\varphi = \varphi_g : x \mapsto gxg^{-1}$ (the inner automorphism, 2.16) the above shows that for every $H \leq G$ and $g \in G$ we have $gHg^{-1} \leq G$.

3.10. **Definition.** Two subgroups $H_1, H_2 \leq G$ are called **conjugate** if there is a $g \in G$ such that $H_1 = gH_2g^{-1}$.

3.11. **Theorem.** Let $H_1, H_2 \leq G$. Then the set

$$H_1H_2 = \{ab : a \in H_1,\ b \in H_2\} \tag{3.4}$$

is a subgroup if and only if $H_1H_2 = H_2H_1$.

Proof. Suppose H_1H_2 is a subgroup. Then, for all $a \in H_1$, $b \in H_2$, we have $b^{-1}a^{-1} = (ab)^{-1} \in H_1H_2$, i.e., $H_2H_1 \subseteq H_1H_2$. But also for $h \in H_1H_2$ we find $a \in H_1$, $b \in H_2$ such that $h^{-1} = ab$, and then $h = b^{-1}a^{-1} \in H_2H_1$. So $H_1H_2 \subseteq H_2H_1$, that is, $H_1H_2 = H_2H_1$.

On the other hand, assume that $H_1H_2 = H_2H_1$. Then, for all $a, a' \in H_1$, $b, b' \in H_2$ we have $aba'b' \in aH_2H_1b' = aH_1H_2b' = H_1H_2$. Furthermore, for all $a \in H_1$, $b \in H_2$ we have $(ab)^{-1} = b^{-1}a^{-1} \in H_2H_1 = H_1H_2$. □

3.12. **Theorem.** Let $\{H_\alpha\}$ be a (possibly uncountable) family of subgroups of G parametrized by α. Then

$$H := \bigcap_\alpha H_\alpha \leq G. \tag{3.5}$$

Proof. If $a, b \in H$, so $a, b \in H_\alpha$ for all α. Then $ab, a^{-1} \in H_\alpha$ for all α and hence $ab, a^{-1} \in H$. □

3.13. **Exercise.** Show that if $H_1, H_2 < G$ then $H_1 \cup H_2 \neq G$.

4. GENERATORS

4.1. **Definition.** Let G be a group and $S \subseteq G$ a subset. The group

$$\langle S \rangle := \bigcap \{H : H \leq G \text{ such that } S \subseteq H\} \tag{4.1}$$

is called **the group generated by** S.

4.2. **Definition.** If $G = \langle S \rangle$, then S is called a **generating set** of G. G is called **finitely generated** if the set S is finite, i.e., $S = \{a_1, a_2, \ldots, a_n\}$. In this case we write $G = \langle a_1, a_2, \ldots, a_n \rangle$. The elements of S are called **generators** of G.

Note that, by definition, $\langle \{\,\} \rangle = \{e\}$ and $\langle G \rangle = G$.

4.3. **Theorem.** Let G be a group and $S \subseteq G$ a non-empty subset. Then $\langle S \rangle$ consists of all finite products of elements from $S \cup S^{-1}$, where $S^{-1} := \{a^{-1} : a \in S\}$.

Proof. Let

$$H = \{h_1 h_2 \cdots h_n : h_i \in S \cup S^{-1},\ n \in \mathbb{N}\}. \tag{4.2}$$

We want to show that $H = \langle S \rangle$. Evidently, $H \subseteq \langle S \rangle$. On the other hand, H is a subgroup of G (why?). Since H contains S and H is a group, we have $\langle S \rangle \subseteq H$, and hence $H = \langle S \rangle$. □

4.4. **Corollary.** A homomorphism $\varphi : \langle S \rangle \to H$ is uniquely determined by $\varphi(S)$, i.e., the image of the map φ restricted to the set S.

Proof. By Theorem 4.3, we can write every $a \in \langle S \rangle$ as $a = a_1 a_2 \ldots a_n$ with $a_i \in S \cup S^{-1}$. Then $\varphi(a) = \varphi(a_1)\varphi(a_2)\ldots\varphi(a_n)$ where $\varphi(a_i) \in \varphi(S)$ or $\varphi(a_i)^{-1} = \varphi(a_i^{-1}) \in \varphi(S)$. □

4.5. **Exercise.** Let $H < G$. Show that $G = \langle G \setminus H \rangle$.

4.6. **Exercise.**

(1) Fix $\epsilon > 0$. Show that $(\mathbb{R}, +)$ is generated by the set $(0, \epsilon]$.
(2) Give an example of a generating set $S \neq \mathbb{Q}$ for $(\mathbb{Q}, +)$. Justify your answer.

4.7. **Exercise.** Let us define the **special linear group** over a field K by

$$\mathrm{SL}(2, K) := \{A \in K^{2\times 2} : \det A = 1\}. \tag{4.3}$$

Show that

$$\mathrm{SL}(2, K) = \left\langle \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in K \right\} \cup \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\} \right\rangle. \tag{4.4}$$

Hint: Verify that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} \begin{pmatrix} 1 & a/c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & cd \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & 1/c \end{pmatrix} & (c \neq 0) \\ \begin{pmatrix} 1 & ab \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} & (c = 0) \end{cases} \tag{4.5}$$

and furthermore

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1/a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{4.6}$$

5. Cyclic groups

5.1. **Definition.** A group G is called **cyclic**, if there is $g \in G$ such that $G = \langle g \rangle$. The element g is called the **generator** of G.

Note that $G = \{g^n : n \in \mathbb{Z}\}$, and that every cyclic group is abelian (since $g^m g^n = g^{m+n} = g^n g^m$).

5.2. **Example.**

(1) $(\mathbb{Z}, +)$ is generated by 1 and thus cyclic. The subgroups $(n\mathbb{Z}, +)$ for some fixed $n \in \mathbb{Z}$ are generated by n and hence also cyclic.
(2) $(\mathbb{Z}_n, +)$ is generated by $\overline{1}$ and thus cyclic.

5.3. **Theorem.** Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle g \rangle$ and $H < G$. Every $h \in H$ can be expressed as $h = g^m$ for some $m \in \mathbb{Z}$. Since the trivial group $H = \{e\}$ is cyclic we may exclude this case from now on and assume $h \neq e$. Thus there exists an element $g^m \in H$ with $m \neq 0$. Since inverse axiom $g^m \in H$ implies $g^{-m} \in H$ there is $g^m \in H$ with $m > 0$, and hence the set $I = \{k \in \mathbb{N} : g^k \in H\}$ is non-empty. Let s be the smallest element of I and g^m an arbitrary element of H. Let $q, r \in \mathbb{Z}$ be such that $m = qs + r$, $0 \leq r < s$. Now $g^r = g^{m-qs} = g^m (g^s)^{-q} \in H$. If $r \neq 0$ then $r \in I$ and we have a contradiction with s being minimal. If $r = 0$, then $m = qs$, so $g^m = (g^s)^q$, that is, $H \subseteq \langle g^s \rangle$. Since $g^s \in H$ we also have $\langle g^s \rangle \subseteq H$ and thus $H = \langle g^s \rangle$. □

Since $\mathbb{Z}$ is cyclic, we have the following classification of subgroups of $\mathbb{Z}$.

5.4. **Corollary.** Every subgroup of $\mathbb{Z}$ is of the form $s\mathbb{Z} := \{sm : m \in \mathbb{Z}\}$ with $s \in \mathbb{Z}_{\geq 0}$.

This follows directly from the previous proof: recall that 1 is the generator of $\mathbb{Z}$, and our explicit construction of the cyclic subgroups H shows that $H = s\mathbb{Z}$ in the present case.

Note that if $s > 0$ then s is the smallest integer > 0 in the subgroup.

5.5. **Definition.** Let G be a group. The **order** of $a \in G$ is the order of the cyclic group $\langle a \rangle$ and is denoted by $\operatorname{ord} a := |\langle a \rangle|$.

5.6. **Theorem.** The order of $a \in G$ is either infinite or equal to the smallest integer $s > 0$ such that $a^s = e$. In the latter case $\langle a \rangle = \{e, a, a^2, \ldots, a^{s-1}\}$.

Proof. If $a^i \neq a^j$ for all $i \neq j$, then $\operatorname{ord} a = \infty$. Otherwise there are $i < j$ such that $a^i = a^j$, and hence $a^k = e$ with $k = j - i > 0$. Let $s > 0$ be the smallest integer such that $a^s = e$. Then all elements in the set $H = \{e, a, a^2, \ldots, a^{s-1}\}$ are distinct (otherwise there would be a smaller element $k < s$ such that $a^k = e$) and is closed under multiplication since $a^s = e$. Since H is finite, this implies H is a group and thus $H = \langle a \rangle$. □

5.7. **Corollary.** Suppose ord $a = s$. Then $a^k = e$ if and only if $k \in s\mathbb{Z}$.

Proof. If $k = sm$ for some $m \in \mathbb{Z}$ then $a^k = (a^s)^m = e$. On the other hand, if $a^k = e$ then $H = \{k \in \mathbb{Z} : a^k = e\}$ is a subgroup of $\mathbb{Z}$ and hence $H = s'\mathbb{Z}$ for some integer $s' > 0$ (Corollary 5.4). By Theorem 5.6 s is the smallest integer > 0 such that $a^s = e$ and so $s = s'$. □

5.8. **Theorem.** Suppose ord $a = n$. Then for all $m \in \mathbb{Z}$

$$\text{ord } a^m = \frac{n}{\gcd(m, n)}. \tag{5.1}$$

Proof. Let $d = \gcd(m, n)$, $m = dm'$, $n = dn'$, with m', n' coprime. Set $r = \text{ord } a^m$. Since $e = (a^m)^r = a^{mr}$ we have by Corollary 5.7 $mr = nt$ for some $t \in \mathbb{Z}$. Divide by d to obtain $m'r = n't$. Since m', n' are coprime n' divides r, so $n' \leq r$. On the other hand $(a^m)^{n'} = (a^n)^{m'} = e^{m'} = e$ so $r \leq n'$. We conclude $r = n'$. □

The following two corollaries follow directly from the above theorem.

5.9. **Corollary.** If ord $a = n$ then $\langle a \rangle = \langle a^m \rangle$ if and only if m, n are coprime.

5.10. **Corollary.** A cyclic group of order n has $\varphi(n)$ generators, where φ is Euler's φ function.

5.11. **Theorem.** If G is a cyclic group of order n, then for every divisor d of n there exists precisely one subgroup of order d.

Proof. Suppose $G = \langle a \rangle$, ord $a = n = dm$. So ord $a^m = \frac{dm}{\gcd(m, dm)} = d$ and $\langle a^m \rangle$ has order d. Suppose now there is a further subgroup $H \leq G$ of order d. By Theorem 5.3 $H = \langle a^k \rangle$ for some $k \geq 1$. Now $d = \text{ord } a^k$ by assumption, which equals ord $a^k = \frac{dm}{\gcd(k, n)}$, so $\gcd(n, k) = m$. This means m divides k, set $k = mk'$. Hence $a^k = (a^m)^{k'} \in \langle a^m \rangle$, i.e., $H = \langle a^k \rangle \leq \langle a^m \rangle$. But since H has the same order as $\langle a^m \rangle$, we in fact have $H = \langle a^m \rangle$. □

Note that the above theorem in fact gives a complete classification of all subgroups of a cyclic group G, since (a) every subgroup is cyclic (Theorem 5.3) and (b) the order of every cyclic subgroup divides the order of G; this follows from Theorem 5.8.

5.12. **Exercise.** Let G be a group. Show that:

(1) If G is abelian, then the elements $a \in G$ of finite order form a subgroup. Provide a counter example that shows that this is not true in general.
(2) If for every $a \in G$, ord $a \leq 2$, then G is abelian.
(3) If a is the only element of order 2 in G, then $a \in Z(G)$.

5.13. **Exercise.** Let G be a group, $a, b \in G$, $\varphi \in \operatorname{Aut} G$. Show that:

(1) $\operatorname{ord} \varphi(a) = \operatorname{ord} a$.
(2) $\operatorname{ord} aba^{-1} = \operatorname{ord} b$.
(3) $\operatorname{ord} ab = \operatorname{ord} ba$.
(4) $\operatorname{ord} a^{-1} = \operatorname{ord} a$.

5.14. **Exercise.** Let $G = \langle a \rangle$ be a cyclic group of order n. Show that:

(1) If $\varphi \in \operatorname{Aut} G$ then there exists $k \in \mathbb{N}$ with $\gcd(k, n) = 1$ and $\varphi(a) = a^k$.
(2) $\operatorname{Aut} G \simeq \mathbb{Z}_n^*$.

6. Cosets and Lagrange's Theorem

6.1. **Definition.** Given a subgroup $H \leq G$ we define the **relation** $R_H \subseteq G \times G$ by

$$(x, y) \in R_H \Leftrightarrow xy^{-1} \in H. \tag{6.1}$$

Note that $R_G = G \times G$ and $R_{\{e\}} = \{(x, y) \in G \times G : x = y\}$.

6.2. **Example.** For $G = \mathbb{Z}$ and $H = n\mathbb{Z}$ we have

$$(x, y) \in R_{n\mathbb{Z}} \Leftrightarrow x - y \in n\mathbb{Z} \Leftrightarrow x \equiv y \bmod n. \tag{6.2}$$

6.3. **Theorem.** For every $H \leq G$ the relation R_H defines an equivalence relation which is consistent with right multiplication, i.e., for all $x, y, a \in G$,

$$(x, y) \in R_H \Leftrightarrow (xa, ya) \in R_H. \tag{6.3}$$

Proof. Clearly $xx^{-1} \in H$, so $(x, x) \in R_H$. Secondly, if $xy^{-1} \in H$ then $(xy^{-1})^{-1} = yx^{-1} \in H$, so $(x, y) \in R_H$ implies $(y, x) \in R_H$. Thirdly, if $xy^{-1} \in H$, $yz^{-1} \in H$, then $xy^{-1}yz^{-1} = xz^{-1} \in H$. So $(x, y) \in R_H$, $(y, z) \in R_H$ implies $(x, z) \in R_H$. We have shown R_H is an equivalence relation. To show the consistency with right multiplication, note that

$$xy^{-1} \in H \Leftrightarrow (xa)(ya)^{-1} \in H \tag{6.4}$$

since $(xa)(ya)^{-1} = xaa^{-1}y^{-1} = xy^{-1}$. □

6.4. Let us consider the equivalence classes for the relation R_H. The equivalence class of $g \in G$ is

$$\begin{aligned} [g]_H &= \{x \in G : (x, g) \in R_H\} \qquad \text{(by definition)} \\ &= \{x \in G : xg^{-1} \in H\} \\ &= \{yg \in G : y \in H\} \qquad (y = xg^{-1}) \\ &= Hg. \end{aligned} \tag{6.5}$$

6.5. **Definition.** For a given subgroup $H \leq G$ the sets Hg, $g \in G$ are called the **right cosets** of H.

6.6. **Example.** In the case $G = \mathbb{Z}$, $H = n\mathbb{Z}$, the right cosets $m + n\mathbb{Z}$ are the residue classes modulo n.

6.7. **Theorem.** Let $H \leq G$. Then

(1) $G = \bigcup_{g \in G} Hg$,
(2) for all $a, b \in G$: $Ha \cap Hb \neq \emptyset \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$.

Proof. This is a direct consequence of elementary properties of equivalence relations. □

6.8. **Lemma.** The map $Ha \to Hb$, $g \mapsto g' = ga^{-1}b$, is a bijection.

Proof. The inverse image of $g' \in Hb$ is $g = g'b^{-1}a$. So if $g' \in Hb$ then $g \in Ha$ hence the map is surjective. The formula for the inverse image also implies that if $g_1 \mapsto g'$ and $g_2 \mapsto g'$, then $g_1 = g_2$ and so the map is injective. □

The lemma implies that $|Ha| = |Hb|$ for all $a, b \in G$.

6.9. **Definition.** Let $H \leq G$. The number of distinct right cosets is called the **index** of H in G and denoted by $|G : H|$. [The index can be infinite.]

6.10. **Lagrange's Theorem.** Let $H \leq G$ be finite groups. Then

$$|G| = |G : H|\,|H|. \tag{6.6}$$

[Note that the statement also formally holds if $|G|$ and $|G : H|$ or $|H|$ are infinite.]

Proof. We have $G = \bigcup_{g \in G} Hg$, which is a disjoint union of $|G : H|$ cosets. Since $|Hg| = |H|$, the result follows. □

A direct consequence is:

6.11. **Corollary.** If G is a finite group, then the order of every subgroup divides $|G|$.

A special case of this for cyclic subgroups:

6.12. **Corollary.** If G is a finite group, then $\operatorname{ord} a$ divides $|G|$ for every $a \in G$.

6.13. **Exercise.** Using Corollary 5.7, prove Fermat's Little Theorem:

6.14. **Corollary.** (Fermat's Little Theorem.) If G is a finite group, then $a^{|G|} = e$ for all $a \in G$.

A special case of this is the following, which is due to Euler.

6.15. **Corollary.** Let $n \in \mathbb{N}$ and $m \in \mathbb{Z}$ with $\gcd(m, n) = 1$. Then

$$m^{\varphi(n)} \equiv 1 \bmod n. \tag{6.7}$$

Proof. Let $\mathbb{Z}_n^*$ be the group of integers modulo n that are coprime to n. Since $|\mathbb{Z}_n^*| = \varphi(n)$ we have $\overline{m}^{\varphi(n)} = \overline{1}$ by Fermat's Little Theorem 6.14. Recall that $\overline{m}^r = \overline{m^r}$ for any $r \in \mathbb{N}$, and so $m^{\varphi(n)} \equiv 1 \bmod n$. □

6.16. A particularly important case is when $n = p$ a prime number. Then $\varphi(p) = p - 1$. If $\gcd(p, m) = 1$ we have therefore $m^{p-1} \equiv 1 \bmod p$, i.e., $m^p \equiv m \bmod p$. But if $\gcd(p, m) \neq 1$ then p divides m and the $m^p \equiv m \bmod p$ holds trivially. We have proved a result by Fermat:

6.17. **Corollary.** Let p be prime and $m \in \mathbb{Z}$. Then $m^p \equiv m \bmod p$.

6.18. **Corollary.** Let G be a group of prime order. Then G is cyclic.

Proof. Prime order means that $|G|$ is a prime number. So for $a \in G \setminus \{e\}$ we have $\operatorname{ord} a \neq 1$. By Corollary 6.12 $\operatorname{ord} a$ divides $|G|$ so $\operatorname{ord} a = |G|$ is the only possibility, and hence $\langle a \rangle = G$ since G is finite. □

6.19. **Corollary.** Let $H_1, H_1 \leq G$ be finite subgroups with coprime orders. Then $H_1 \cap H_2 = \{e\}$.

Proof. $H_1 \cap H_2$ is a subgroup of both H_1 and H_2. By Corollary 6.11 $|H_1 \cap H_2|$ divides therefore both $|H_1|$ and $|H_2|$, but since these are coprime we have $|H_1 \cap H_2| = 1$. □

6.20. **Definition.** For a given subgroup $H \leq G$ the sets gH, $g \in G$ are called the **left cosets** of H.

One could of course repeat the above calculations for left cosets (and this is recommended as an exercise), but the following theorem offers a shortcut.

6.21. **Theorem.** Let $H \leq G$. Then there is a bijection from the set of right cosets to the set of left cosets, defined by $Hg \mapsto g^{-1}H$.

Proof. Let us first show the map is well defined. We have

$$Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1}b^{-1} \in H \Leftrightarrow a^{-1}H = b^{-1}H. \tag{6.8}$$

Hence $Ha = Hb$ implies $a^{-1}H = b^{-1}H$ and so the map is well defined. The reverse implication implies injectivity, and surjectivity is obvious (the inverse map is given by $gH \mapsto Hg^{-1}$). □

Here is a generalization of Lagrange's Theorem, which provides information also for infinite groups.

6.22. **Theorem.** Let $K \leq H \leq G$ be groups. If two of the quantities $|G : K|$, $|G : H|$, $|H : K|$ are finite, so is the third, and

$$|G : K| = |G : H|\,|H : K|. \tag{6.9}$$

Proof. Let

$$G = \bigcup_{\alpha \in I} g_\alpha H, \qquad H = \bigcup_{\beta \in J} h_\beta K \tag{6.10}$$

be unions of distinct cosets, where I, J denote suitable index sets. We claim that

$$G = \bigcup_{\alpha \in I, \beta \in J} g_\alpha h_\beta K \tag{6.11}$$

is a union of distinct cosets. To prove this claim, suppose that $g_\alpha h_\beta K = g_{\tilde{\alpha}} h_{\tilde{\beta}} K$. This implies that

$$g_\alpha h_\beta KH = g_{\tilde{\alpha}} h_{\tilde{\beta}} KH \Rightarrow g_\alpha h_\beta H = g_{\tilde{\alpha}} h_{\tilde{\beta}} H \Rightarrow g_\alpha H = g_{\tilde{\alpha}} H \tag{6.12}$$

since $KH = H$ for $K \leq H$ and $h_\beta H = H$ for $h_\beta \in H$ (cf. Theorem 6.7). Since we have chosen in the above union one representative g_α for each coset $g_\alpha G$ we have $g_\alpha = g_{\tilde{\alpha}}$. But then $g_\alpha h_\beta K = g_{\tilde{\alpha}} h_{\tilde{\beta}} K$ implies $h_\beta K = h_{\tilde{\beta}} K$, and by the same argument as before $h_\beta = h_{\tilde{\beta}}$. The claim is proved.

We have by definition $|G : H| = |I|$ and $|H : K| = |J|$. In view of (6.11), we conclude that $|G : K| = |I|\,|J|$ and the theorem follows. □

6.23. **Lemma.** Let K, H be subgroups of G. Then for every $g \in G$

$$Kg \cap Hg = (K \cap H)g. \tag{6.13}$$

Proof. The inclusion $(K \cap H)g \subseteq Kg \cap Hg$ is obvious. Let $a \in Kg \cap Hg$, so $a = kg = hg$ for suitable $k \in K$, $h \in H$. Multiply by g^{-1}, and we have $k = h$, which is in $K \cap H$. Hence $a \in (K \cap H)g$, i.e., $Kg \cap Hg \subseteq (K \cap H)g$. □

6.24. **Poincaré's Subgroup Theorem.** Let K, H be subgroups of G. Then

(1) $|G : K \cap H| \leq |G : K|\,|G : H|$,
(2) $|G : K \cap H| = |G : K|\,|G : H|$, if the indices of K, H in G are finite and coprime.

Proof. (1) The coset $(K \cap H)g$ can be written $Kg \cap Hg$ (Lemma 6.23), and hence there are at most $|G : K|\,|G : H|$ such cosets.

(2) $K \cap H$ is a subgroup of both K and H. Applying Theorem 6.22, we have

$$|G : K \cap H| = |G : K|\,|K : K \cap H|, \qquad |G : K \cap H| = |G : H|\,|H : K \cap H|. \tag{6.14}$$

Thus $|G : K|$ and $|G : H|$ divide $|G : K \cap H|$; since they are coprime also $|G : K|\,|G : H|$ divide $|G : K \cap H|$, and hence in particular $|G : K|\,|G : H| \leq |G : K \cap H|$. Together with (1) this yields (2). □

By induction we have:

6.25. **Corollary.** For subgroups $H_i \leq G$, $1 \leq i \leq n$, we have

$$\Big|G : \bigcap_{i=1}^{n} H_i\Big| \leq \prod_{i=1}^{n} \big|G : H_i\big|. \tag{6.15}$$

This says in particular that if the H_i have finite index in G, so does their intersection.

6.26. **Exercise.**

(1) Write down the decomposition of $\mathbb{Z}_{15}^*$ into left cosets with respect to the subgroup $\langle \overline{7} \rangle$.
(2) Calculate in $\mathbb{Z}_{15}^*$: $\overline{7}^{350}$, $\overline{2}^{1000}$.

7. Normal subgroups and quotient groups

Recall the equivalence relation $R_H \subseteq G \times G$ defined by

$$(x, y) \in R_H \Leftrightarrow xy^{-1} \in H \tag{7.1}$$

(recall 6.1), which, as we have shown, is compatible with right multiplication in G.

7.1. **Theorem.** Let $H \leq G$. Then R_H is compatible with multiplication in G, if and only if

$$aHa^{-1} \subseteq H \qquad \text{for all } a \in G. \tag{7.2}$$

Proof. Assume R_H is compatible, then it is in particular left compatible, i.e.,

$$(x, y) \in R_H \Leftrightarrow (ax, ay) \in R_H. \tag{7.3}$$

So $axy^{-1}a^{-1} \in H$. Since $h \in H \Leftrightarrow (h, e) \in R_H$, we can choose $x = h$, $y = e$ to obtain $aha^{-1} \in H$ for all $a \in G$.

On the other hand assume $aHa^{-1} \subseteq H$. If $xy^{-1} \in H$, then $ax(ay)^{-1} = axy^{-1}a^{-1} \in H$ and hence R_H is left compatible. Since we already know it is right compatible, the proof is complete. □

Subgroups H for which R_H is compatible with multiplication have a special name:

7.2. **Definition.** A subgroup $H \leq G$ for which $aHa^{-1} \subseteq H$ for all $a \in G$ is called **normal**. We write $H \trianglelefteq G$, and $H \triangleleft G$ if $H \neq G$.

7.3. **Example.**

(1) $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$.
(2) If $H \leq G$ and G is abelian, then $H \trianglelefteq G$.

7.4. **Exercise.** Show that:

(1) $H, K \trianglelefteq G$ implies $HK \trianglelefteq G$.
(2) If $H \leq G$ then the subgroup $\bigcap_{x \in G} xHx^{-1}$ is normal in G.

7.5. **Theorem.** Let $\{H_\alpha\}_{\alpha \in I}$ be a family of normal subgroups in G. Then

$$H := \bigcap_{\alpha \in I} H_\alpha \trianglelefteq G. \tag{7.4}$$

Proof. By Theorem 3.12, H is a subgroup. If $a \in G$ and $h \in H$, then $h \in H_\alpha$ and $aha^{-1} \in H_\alpha$ for all $\alpha \in I$, and therefore $aha^{-1} \in H$. □

7.6. **Theorem.** Let $\varphi : G_1 \to G_2$ a homomorphism.

(1) If $H_2 \trianglelefteq G_2$, then $\varphi^{-1}(H_2) \trianglelefteq G_1$.
(2) If $H_1 \trianglelefteq G_1$ and φ is an epimorphism then $\varphi(H_1) \trianglelefteq G_2$.

Proof. For the subgroup properties recall Theorem 3.7.

(1) If $x \in \varphi^{-1}(H_2)$ and $a \in G_1$, then $\varphi(x) \in H_2$ and so $\varphi(axa^{-1}) = \varphi(a)\varphi(x)\varphi(a)^{-1} \in H_2$ since H_2 is normal. We conclude $axa^{-1} \in \varphi^{-1}(H_2)$.

(2) Since H_1 is normal, we have $\varphi(a)\varphi(H_1)\varphi(a)^{-1} \subseteq \varphi(H_1)$. Since we assume φ is surjective, every $b \in G_2$ can be written as $b = \varphi(a)$, $a \in G_1$. Therefore $b\varphi(H_1)b^{-1} \in \varphi(H_1)$. □

7.7. Note that with the choice $H_2 = \{e\}$ the theorem says that $\ker \varphi \trianglelefteq G_1$.

7.8. **Definition.** Let G be a group and $X \subseteq G$ a subset. The set

$$N_G(X) := \{g \in G : gX = Xg\} \tag{7.5}$$

is called the **normaliser** of X in G.

7.9. **Exercise.** Prove that

(1) For every subset $X \subseteq G$, $N_G(X) \leq G$.
(2) $H \trianglelefteq G$ if and only if $N_G(H) = G$.
(3) If $H \leq G$ then $H \trianglelefteq N_G(H)$.
(4) If $K \trianglelefteq H$ then $H \leq N_G(K)$.

7.10. **Theorem.** Let $H \trianglelefteq G$. Then

(1) $G/H := \{aH : a \in G\}$ with $(aH)(bH) := (ab)H$ is a group (the **quotient group** of G by H),
(2) $|G/H| = |G : H|$,
(3) The map $\pi : G \to G/H$, $g \mapsto gH$, is a homomorphism with kernel $\ker \pi = H$.

[Quotient groups are also often referred to as **factor groups**.]

Proof. (1) Since H is normal, $(aH)(bH) = a(bH)H \in G/H$. The neutral element is $eH = H$, and the inverse of aH is $a^{-1}H$.

(2) follows directly from the definitions.

(3) We have $\pi(ab) = (ab)H = (aH)(bH) = \pi(a)\pi(b)$, so π is a homomorphism. As to the kernel,

$$\begin{aligned} a \in \ker \pi &\Leftrightarrow \pi(a) = H \qquad \text{(by definition, since } H \text{ is the identity in } G/H) \\ &\Leftrightarrow aH = H \qquad \text{(by definition of } \pi) \\ &\Leftrightarrow a \in H \qquad \text{(Theorem 6.7 (2))} \end{aligned} \tag{7.6}$$

□

7.11. **Definition.** The above map π is called the **canonical epimorphism**.

7.12. It is often convenient to use the notation $\overline{G} := G/H$, and $\overline{a} := aH$. The group multiplication in $\overline{G}$ is then given by $\overline{a}\ \overline{b} = \overline{ab}$, the identity is $\overline{e}$, and the inverse of $\overline{a}$ is given by $\overline{a^{-1}}$.

7.13. **Theorem.** Let $H \subseteq G$ be a non-empty subset. Then $H \trianglelefteq G$, if and only if there exists a homomorphism $\varphi : G \to G'$ with $H = \ker \varphi$.

Proof. One implication follows from 7.7, and the reverse from 7.10 (3). □

7.14. **Example.**

(1) Since $\mathbb{Z}$ is abelian, every subgroup $n\mathbb{Z}$ is normal. The quotient groups $\mathbb{Z}/n\mathbb{Z}$ are easily seen to be equal to $\mathbb{Z}_n$ (the residue classes modulo n).

(2) The map $\mathrm{GL}(n, K) \to K^* = K \setminus \{0\}$, $A \mapsto \det A$ is a homomorphism since $\det AB = \det A \det B$. Its kernel is $\mathrm{SL}(n, K) := \{A \in K^{n\times n} : \det A = 1\}$ and we have $\mathrm{GL}(n, K)/\mathrm{SL}(n, K) \simeq K^*$.

(3) For the trivial normal subgroup $\{e\} \trianglelefteq G$ we have $G/\{e\} = \{g\{e\} : g \in G\} = \{\{g\} : g \in G\}$ with composition $\{a\}\{b\} = \{ab\}$. Clearly $G \to G/\{e\}$ $a \mapsto \{a\}$ defines an isomorphism. In the opposite extreme $G \trianglelefteq G$, we have $G/G = \{G\}$ and thus $G/G \simeq \{e\}$.

8. Isomorphism Theorems

8.1. The following theorems are useful in the classification of quotient groups of a given group G, or (vice versa) its normal subgroups.

8.2. **Homomorphism Theorem.** If $\varphi : G \to G'$ is a homomorphism, then

$$G/\ker\varphi \simeq \varphi(G). \tag{8.1}$$

Proof. Set $K = \ker\varphi$. We know $K \trianglelefteq G$. Define the map

$$\Phi : G/K \to \varphi(G), \qquad gK \mapsto \varphi(g). \tag{8.2}$$

The following proves the maps is well defined ($\Rightarrow$) and injective ($\Leftarrow$):

$$aK = bK \Leftrightarrow b^{-1}a \in K \Leftrightarrow \varphi(b^{-1}a) = e' \Leftrightarrow \varphi(a) = \varphi(b) \Leftrightarrow \Phi(aK) = \Phi(bK). \tag{8.3}$$

Φ is trivially surjective (by construction), and it is a homomorphism because

$$\Phi((aK)(bK)) = \Phi(abK) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(aK)\Phi(bK). \tag{8.4}$$

We conclude Φ is an isomorphism. □

8.3. **Example.**

(1) The isomorphisms given in Example 7.14 follow directly from the homomorphism theorem.
(2) Recall the inner automorphism $\varphi_x(g) = xgx^{-1}$, and that the homomorphism $G \to \operatorname{Aut} G$, $x \mapsto \varphi_x$ has as its kernel the center $Z(G)$ of G. Its image $I(G)$ is called the **group of inner automorphisms**. The homomorphism theorem shows that $G/Z(G) \simeq I(G)$.
(3) For $m, n \in \mathbb{N}$, the map $\varphi : m\mathbb{Z} \to \mathbb{Z}_n$, $mr \mapsto \bar{r}$, is an epimorphism with kernel $mn\mathbb{Z}$. The homomorphism theorem shows $m\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$.

8.4. **Corollary.** If $\varphi : G \to G'$ is a monomorphism, then $G \simeq \varphi(G)$.

This is a straightforward consequence of the above theorem. We also achieve a classification of all cyclic groups:

8.5. **Theorem.** Every cyclic group of order $n \in \mathbb{N}$ is isomorphic to $(\mathbb{Z}_n, +)$, and every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

Proof. Let $G = \langle a \rangle$ be cyclic. We have $G = \{a^m : m \in \mathbb{Z}\}$. The map $\mathbb{Z} \to G$, $m \mapsto a^m$ defines an epimorphism, with kernel $s\mathbb{Z}$ and $s = 0$ or the smallest positive integer such that $a^s = e$ (Corollary 5.4), i.e., $s = \operatorname{ord} a = |G|$. The homomorphism theorem implies that $G \simeq \mathbb{Z}/\{0\} \simeq \mathbb{Z}$ if G is infinite and otherwise $G \simeq \mathbb{Z}_s = \mathbb{Z}/s\mathbb{Z}$ with $s = |G|$. □

8.6. **First Isomorphism Theorem.** Let $H \leq G$, $N \trianglelefteq G$. Then $HN \leq G$, $(H \cap N) \trianglelefteq H$ and

$$HN/N \simeq H/(H \cap N). \tag{8.5}$$

Proof. Since N is normal, $aN = Na$ for all $a \in G$. So

$$HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH \tag{8.6}$$

and by Theorem 3.11 HN is a subgroup. Note that $N \trianglelefteq HN$, and consider the restriction of the canonical epimorphism $\pi : G \to G/N$ to H, which we denote by $\pi_0 : H \to G/N$, $h \mapsto hN$. For the image,

$$\pi_0(H) = \{hN : h \in H\} = \{hnN : hn \in HN\} = HN/N. \tag{8.7}$$

Recall N is the identity in G/N, and $aN = N$ if and only if $a \in N$. So

$$\ker \pi_0 = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N. \tag{8.8}$$

Therefore $H \cap N$ is normal (Theorem 7.13), and the isomorphism follows from the homomorphism theorem (take $\varphi = \pi_0$). □

8.7. **Example.** Isomorphism theorems are for instance useful in the calculation of group orders, since isomorphic groups have the same order. If $H \leq G$ and $K \trianglelefteq G$ so that HK is finite, then Lagrange's Theorem with Theorem 7.10 (2) and the first isomorphism theorem yield

$$\frac{|HK|}{|K|} = |HK : K| = |HK/K| = |H/H \cap K| = |H : H \cap K| = \frac{|H|}{|H \cap K|}, \tag{8.9}$$

that is

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}. \tag{8.10}$$

8.8. **Exercise.** Prove formula (8.10) for general finite subgroups $H, K \leq G$.

8.9. **Second Isomorphism Theorem.** Let $K \leq H \trianglelefteq G$, $K \trianglelefteq G$. Then $H/K \trianglelefteq G/K$ and

$$(G/K)/(H/K) \simeq G/H. \tag{8.11}$$

Proof. Let $\varphi : G/K \to G/H$, $gK \mapsto gH$. We have

$$aK = bK \Rightarrow ab^{-1} \in K \subseteq H \Rightarrow aH = bH, \tag{8.12}$$

so the map is well defined. Evidently, φ is a homomorphism, with image $\varphi(G/K) = G/H$ and kernel

$$\ker \varphi = \{gK : gH = H\} = \{gK : g \in H\} = H/K. \tag{8.13}$$

The theorem now follows from the homomorphism theorem. □

8.10. **Theorem.** Let $N \trianglelefteq G$ and $\pi : G \to G/N$ the canonical epimorphism.

(1) If $H \leq G$, then $\pi(H) = HN/N \leq G/N$.
(2) If $K \leq G/N$, then $N \leq \pi^{-1}(K) \leq G$ and $K = \pi^{-1}(K)/N$.
(3) Let $\mathfrak{U} = \{H \leq G : N \leq H\}$ (the set of subgroups of G that contain N) and $\overline{\mathfrak{U}} = \{K \leq G/N\}$ (the set of subgroups of G/N). Then the map

$$\mathfrak{U} \to \overline{\mathfrak{U}}, \qquad H \mapsto \pi(H) \tag{8.14}$$

is a bijection. Here $\pi(H) \trianglelefteq G/N$ if and only if $H \trianglelefteq G$, and in this case $|G : H| = |G/N : \pi(H)|$.

Proof. (1) and (2) follow from Theorem 3.7, with $\varphi = \pi$, $G_1 = G$, $H_1 = H$, $G_2 = G/N$, $H_2 = K$. In particular, Theorem 3.7 (2) says that $\pi^{-1}(K) \leq G$. The pre-image of the identity in G/N is N and hence $N \leq \pi^{-1}(K)$. Therefore, $K = \pi(\pi^{-1}(K)) = \pi^{-1}(K)/N$.

To prove (3), note that in view of (1) and (2) we have $N \leq \pi^{-1}(\pi(H)) \leq G$. Obviously $H \leq \pi^{-1}(\pi(H))$. Suppose there is an $a \in \pi^{-1}(\pi(H))$ with $a \notin H$. Then there exists $b \in H$ such that $\pi(a) = \pi(b)$, i.e., $aN = bN$, and so $b^{-1}a \in N$. By assumption $N \leq H$ so $b^{-1}a \in H$ and hence $a \in H$, a contradiction. We conclude $\pi^{-1}(\pi(H)) = H$, i.e., the map (8.14) is injective. As to the inverse, for $K \leq G/N$ we have $K = \pi(\pi^{-1}(K))$, and so the map (8.14) is a bijection.

The statement "$\pi(H) \trianglelefteq G/N$ if and only if $H \trianglelefteq G$" follows from Theorem 7.6, (1) and (2). The last statement of the theorem follows from the second isomorphism theorem, since $|G : H| = |(G/N) : (H/N)| = |G/N : \pi(H)|$. □

8.11. **Definition.** A sequence of homomorphisms

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} G_n \tag{8.15}$$

is called **exact** if $\operatorname{im}\varphi_i = \ker \varphi_{i+1}$ for all $i = 1, \ldots, n-2$.

8.12. **Example.** Consider the so-called **short** exact sequence

$$\{e\} \to H \xrightarrow{\varphi} G \xrightarrow{\psi} K \to \{e\}. \tag{8.16}$$

The first homomorphism $\{e\} \to H$ can only be defined by $e \mapsto e$. The same holds for the last $K \to \{e\}$. Assuming that the sequence is exact means that $\ker\varphi = \{e\}$, $\operatorname{im}\psi = K$ and $\operatorname{im}\varphi = \ker\psi$. Thus φ is injective and ψ surjective. Corollary 8.4 then says that $\varphi(H) \simeq H$, so $H \simeq \ker\psi$. The homomorphism theorem on the other hand yields $K = \psi(G) \simeq G/\ker\psi = G/\varphi(H)$, i.e., $K \simeq G/H$.

The standard example of a short exact sequence is

$$\{e\} \to N \xrightarrow{\iota} G \xrightarrow{\pi} G/N \to \{e\}. \tag{8.17}$$

where $N \trianglelefteq G$, π is the canonical epimorphism, and $\iota : g \mapsto g$ the inclusion map.

9. DIRECT PRODUCTS

9.1. **Definition.** Let $G_1, \dots, G_n$ be groups. We define their **direct product** (sometimes also referred to as **outer** direct product) as the set

$$G = G_1 \times \cdots \times G_n = \{(a_1, \dots, a_n) : a_i \in G_i \ (1 \le i \le n)\} \tag{9.1}$$

with composition defined by

$$(a_1, \dots, a_n) \circ (b_1, \dots, b_n) := (a_1 b_1, \dots, a_n b_n). \tag{9.2}$$

9.2. Clearly the multiplication is associative, the identity is $(e, \dots, e)$ and the inverse $(a_1^{-1}, \dots, a_n^{-1})$. Thus $(G, \circ)$ is a group. We will also use the notations

$$G = \prod_{i=1}^{n} G_i, \qquad G^n = G \times G \times \cdots \times G \quad (n \text{ times}). \tag{9.3}$$

If the group composition is addition, we write alternatively

$$G = \bigoplus_{i=1}^{n} G_i = G_1 \oplus \cdots \oplus G_n. \tag{9.4}$$

9.3. **Theorem.**

(1) $\left|\prod_{i=1}^n G_i\right| = \prod_{i=1}^n |G_i|$.
(2) $Z\left(\prod_{i=1}^n G_i\right) = \prod_{i=1}^n Z(G_i)$.
(3) $\prod_{i=1}^n G_i$ is abelian if and and only if every factor G_i is abelian.

Proof. (1) This is a standard result for products of sets.

(2) Set $G = \prod_{i=1}^n G_i$. $a = (a_1, \dots, a_n) \in Z(G)$ is equivalent to $ab = ba$ for all $b = (b_1, \dots, b_n) \in G$, i.e., $a_i b_i = b_i a_i$ for all i.

(3) This follows from (2), since G is abelian if and only if $Z(G) = G$. □

9.4. **Theorem.** Let G_i $(1 \le i \le n)$ be groups.

(1) For every permutation $\pi \in S_n$, we have $\prod_{i=1}^n G_i \simeq \prod_{i=1}^n G_{\pi(i)}$.
(2) Given integers $1 \le n_1 < n_2 < \ldots < n_r < n$, we have
$(G_1 \times \cdots \times G_{n_1}) \times (G_{n_1+1} \times \cdots \times G_{n_2}) \times \cdots (G_{n_r+1} \cdots \times G_n) \simeq \prod_{i=1}^n G_i$.
(3) If there are groups $\tilde{G}_i$ such that $\tilde{G}_i \simeq G_i$ for all i, then $\prod_{i=1}^n G_i \simeq \prod_{i=1}^n \tilde{G}_i$.

Proof. (1) The isomorphism is explicitly $(a_1, \dots, a_n) \mapsto (a_{\pi(1)}, \dots, a_{\pi(n)})$.

(2) The relevant isomorphism is $(a_1, \dots, a_n) \mapsto ((a_1, \dots, a_{n_1}), \dots, (a_{n_r+1}, \dots, a_n))$.

(3) Let $\varphi_i : G_i \to \tilde{G}_i$ be the corresponding isomorphisms. Then $(a_1, \dots, a_n) \mapsto (\varphi_1(a_1), \dots, \varphi_n(a_n))$ gives the desired isomorphism. □

9.5. As before, consider $G = \prod_i G_i$. Let us denote by $E = \{e\}$ the trivial group, and set

$$G_i' = E^{i-1} \times G_i \times E^{n-i} = \{(e, \dots, e, a_i, e, \dots, e) : a_i \in G_i\}. \tag{9.5}$$

The map $\varphi_i : G_i \to G$, $a_i \mapsto (e, \dots, e, a_i, e, \dots, e)$ defines an isomorphism from G_i to G_i'. Clearly G_i' is a subgroup of G. [This also follows abstractly from Theorem 3.7 (1).] In fact $G_i' \trianglelefteq G$, since $g(e, \dots, e, a_i, e, \dots, e)g^{-1} = (e, \dots, e, g_i a_i g_i^{-1}, e, \dots, e) \in G_i'$ for all $g = (g_1, \dots, g_n)$. Furthermore, $(a_1, \dots, a_n) = \varphi_1(a_1) \cdots \varphi_n(a_n)$ and therefore

$$G = G_1' G_2' \cdots G_n' = \prod_i G_i'. \tag{9.6}$$

[Note that here the symbol $\prod$ has a different meaning than in (9.3), but we will see later that the two are essentially the same (Theorem 9.12).]

Because the elements of G_i' are of the form $(e, \dots, e, a_i, e, \dots, e)$ and the elements of $\prod_{j \neq i} G_j'$ are of the form $(a_1, \dots, a_{i-1}, e, a_{i+1}, \dots, a_n)$, we see that

$$G_i' \cap \prod_{j \neq i} G_j' = E^n = \{e\}, \tag{9.7}$$

i.e., the trivial subgroup in G.

9.6. **Definition.** A group G is called **inner direct product** of the normal subgroups $N_1, \dots, N_k \trianglelefteq G$ if

(1) $G = N_1 N_2 \cdots N_k$,
(2) $N_i \cap \prod_{j \neq i} N_j = \{e\}$.

9.7. Note that our analysis in 9.5 shows that the outer direct product $G = G_1 \times \cdots \times G_n$ is in fact an inner direct product $G = G_1' \cdots G_n'$ with $G_i' \simeq G_i$.

9.8. **Example.** The Klein four group $\{e, a, b, c\}$ is an inner direct product of $\{e, a\}$ and $\{e, b\}$ and hence isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

9.9. **Theorem.** Let $G = N_1 N_2 \cdots N_k$ be an inner direct product of the normal subgroups $N_1, \dots, N_k$. Then:

(1) If $i \neq j$ then $ab = ba$ for all $a \in N_i$, $b \in N_j$.
(2) Every $a \in G$ has the unique factorization $a = a_1 \cdots a_k$ with $a_i \in N_i$.

9.10. **Exercise.** Prove Theorem 9.9.

Here is a reversal of the previous theorem.

9.11. **Theorem.** Let $G_1, \dots, G_k \leq G$ such that the following hold:

(1) If $i \neq j$ then $ab = ba$ for all $a \in G_i$, $b \in G_j$.
(2) Every $a \in G$ has the unique factorization $a = a_1 \cdots a_k$ with $a_i \in G_i$.

Then $G_1, \dots, G_k \trianglelefteq G$ and G is the inner direct product of the G_i.

Proof. Let $a = a_1 \cdots a_k$ be the unique factorization of $a \in G$. Due to the commutativity in (1) we have for every $b \in G_i$ that $aba^{-1} = a_i b a_i^{-1} \in G_i$. Hence $G_i \trianglelefteq G$. We also know (by assumption) that $G = G_1 \cdots G_n$. This proves condition 9.6 (1) is satisfied. Let $g \in G_i \cap \prod_{j \neq i} G_j$, i.e., we have both $g = e \cdots e g_i e \cdots e$ for some $g_i \in G_i$ and $g = g_1 \cdots g_{i-1} g_{i+1} \cdots g_k$, for $g_j \in G_j$. The uniqueness of factorization assumed in (2) implies that $g_i = e$ for all i and therefore $g = e$. This proves condition 9.6 (2) is satisfied. □

The following theorem says that the notion of an outer and inner direct product are essentially (i.e., up to isomorphism) the same.

9.12. **Theorem.** If $G = N_1 N_2 \cdots N_k$ is an inner direct product and every normal subgroup N_i are isomorphic to a group G_i, then G is isomorphic to the outer direct product $\prod_{i=1}^k G_i$.

Proof. Because the factorization $a = a_1 \cdots a_k \in G$, $a_i \in N_i$ is unique, the map

$$\varphi : G \to N_1 \times N_2 \times \cdots \times N_k, \qquad a \mapsto (a_1, a_2, \dots, a_k), \tag{9.8}$$

is well defined. To prove that φ is an isomorphism, note that for $a = a_1 \cdots a_k \in G$, $b = b_1 \cdots b_k \in G$, $a_i, b_i \in N_i$,

$$\begin{aligned} \varphi(ab) &= \varphi(a_1 \cdots a_k b_1 \cdots b_k) \\ &= \varphi(a_1 b_1 \cdots a_k b_k) \qquad (\text{since } a_i b_j = b_j a_i \text{ for } i \neq j) \\ &= (a_1 b_1, \dots, a_k b_k) \\ &= (a_1, \dots, a_k)(b_1, \dots, b_k) \\ &= \varphi(a)\varphi(b). \end{aligned} \tag{9.9}$$

So φ is a homomorphism. Since it is obviously bijective (the inverse map is $(a_1, \dots, a_k) \mapsto (a_1 \cdots a_k)$), it is an isomorphism. Hence $G \simeq N_1 \times \cdots \times N_k$. By Theorem 9.4 (3) $N_1 \times \cdots \times N_k \simeq G_1 \times \cdots \times G_k$, which proves $G \simeq G_1 \times \cdots \times G_k$. □

9.13. **Theorem.** Let $N_i \trianglelefteq G_i$ for $i = 1, \dots, k$, and set

$$G = \prod_{i=1}^k G_i, \qquad N = \prod_{i=1}^k N_i. \tag{9.10}$$

Then $N \trianglelefteq G$ and

$$G/N \simeq \prod_{i=1}^k G_i/N_i. \tag{9.11}$$

Proof. Let $\pi_i : G_i \to G_i/N_i$ be the canonical epimorphisms. Then

$$\pi : G \to \prod_{i=1}^{k} G_i/N_i, \qquad (a_1, \ldots, a_k) \mapsto (\pi_1(a_1), \ldots, \pi_k(a_k)), \tag{9.12}$$

is homomorphism with kernel N. By Theorem 7.13, N is normal and the Theorem follows from the Homomorphism Theorem. □

9.14. **Corollary.** Let $G = G_1 \times G_2$. Then $G_1 \simeq G/(E \times G_2)$.

9.15. **Theorem.**

(1) The direct product of two cyclic groups with coprime order is cyclic.
(2) If a cyclic group has order mn, with m, n coprime, then it is isomorphic to the direct product of two cyclic groups of order m and n, respectively.

We rewrite this theorem in following equivalent (by Theorem 8.5) form:

9.16. **Theorem.** If $m, n \in \mathbb{N}$ are coprime, then $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$.

Proof. Since $\mathbb{Z}_{mn}$ has order mn, we know that (cf. Theorem 5.11 and its proof) $\langle \overline{m} \rangle$ and $\langle \overline{n} \rangle$ are cyclic subgroups of $\mathbb{Z}_{mn}$ of order n and m respectively. Now by Corollary 6.19 $\langle \overline{m} \rangle \cap \langle \overline{n} \rangle = \{e\}$. Now since m, n are coprime, the Bézout's theorem says that there are integers $k, l \in \mathbb{Z}$ such that $km + ln = 1$. Hence $hkm + hln = h$ for all $h \in \mathbb{Z}$, and, modulo mn, we have $(hk)\overline{m} + (hl)\overline{n} = \overline{h}$. Therefore $\mathbb{Z}_{mn} = \langle \overline{m} \rangle + \langle \overline{n} \rangle$, and, by definition, $\mathbb{Z}_{mn}$ is an inner direct product and hence isomorphic to an outer direct product of $\langle \overline{m} \rangle \simeq \mathbb{Z}_n$ and $\langle \overline{n} \rangle \simeq \mathbb{Z}_m$. □

9.17. **Exercise.** Prove the following corollary:

9.18. **Corollary.** Let $p_1, \ldots, p_r$ be distinct primes. A group G of order $p_1^{k_1} \cdots p_r^{k_r}$ is cyclic if and only if

$$G \simeq \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_r^{k_r}} \tag{9.13}$$

9.19. **Corollary.** (Chinese Remainder Theorem.) Given $m, n \in \mathbb{N}$ coprime, and $a, b \in \mathbb{Z}$, then there is $x \in \mathbb{Z}$ such that

$$x \equiv a \bmod m, \qquad x \equiv b \bmod n. \tag{9.14}$$

Proof. The map $\varphi : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $x \mapsto (\overline{x}, \overline{x})$, is a homomorphism with kernel $mn\mathbb{Z}$. The homomorphism theorem and Theorem 9.16 imply that

$$\varphi(\mathbb{Z}) \simeq \mathbb{Z}/mn\mathbb{Z} = \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n. \tag{9.15}$$

This means φ is surjective, which proves the claim. □

9.20. **Definition.** A function $f : \mathbb{Z} \to \mathbb{C}$ is called **multiplicative**, if for all coprime $m, n \in \mathbb{Z}$,

$$f(m)f(n) = f(mn). \tag{9.16}$$

9.21. **Corollary.** Euler's φ function is multiplicative.

Proof. a, b are generators of $\mathbb{Z}_m, \mathbb{Z}_n$ respectively, if and only if (a, b) is a generator of $\mathbb{Z}_m \times \mathbb{Z}_n$. Because of Corollary 5.10 the number of generators is therefore $\varphi(m)\varphi(n)$. On the other hand, since $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$, the number of generators is $\varphi(mn)$. We conclude

$$\varphi(m)\varphi(n) = \varphi(mn). \tag{9.17}$$

□

9.22. **Exercise.** Let H, K be normal subgroups of the finite group G, with $\gcd(|H|, |K|) = 1$. Show that

(1) $H \cap K = \{e\}$.
(2) $hk = kh$ for all $h \in H$, $k \in K$.
(3) $HK \simeq H \times K$.

10. GROUP ACTIONS

10.1. **Definition.** Let G be a group and X a non-empty set. We say G **acts on** X, if there is a map $\cdot : G \times X \to X$ such that

(1) $(gh) \cdot x = g \cdot (h \cdot x)$,
(2) $e \cdot x = x$,

for all $g, h \in G$, $x \in X$. The map $\cdot$ is called the **group action**, or G **action**.

In other words, the above conditions ensure that a group action is compatible with group multiplication.

10.2. **Theorem.** Suppose G acts on X. Then

$$R(G) = \{(x, y) \in X \times X : (\exists g \in G)(g \cdot x = y)\} \tag{10.1}$$

is an equivalence relation.

Proof. Since $e \cdot x = x$ we have $(x, x) \in R(G)$ for all $x \in X$. Next, if $(x, y) \in R(G)$, i.e., $g \cdot x = y$ for some $g \in G$, then

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x, \tag{10.2}$$

and so $(y, x) \in R(G)$. Finally if $(x, y), (y, z) \in R(G)$, i.e., $g \cdot x = y$, $h \cdot y = z$ for some $g, h \in G$, then

$$(hg) \cdot x = h \cdot (g \cdot x) = h \cdot y = z, \tag{10.3}$$

and so $(x, z) \in R(G)$. □

10.3. Theorem 10.2 implies that X can be written as a disjoint union of equivalence classes with respect to $R(G)$. The equivalence class of $x \in X$ is explicitly

$$\begin{aligned} [x] &= \{y \in X : (x, y) \in R(G)\} && \text{(by definition)} \\ &= \{y \in X : (\exists g \in G)(g \cdot x = y)\} && \text{(by definition of } R(G)) \\ &= \{g \cdot x : g \in G\} \\ &= G \cdot x. \end{aligned} \tag{10.4}$$

Hence,

$$X = \bigcup_{x \in X} G \cdot x. \tag{10.5}$$

and

$$G \cdot x = G \cdot y \quad \Leftrightarrow \quad [(\exists g \in G)(g \cdot x = y)]. \tag{10.6}$$

10.4. **Definition.** The equivalence classes $G \cdot x$ are called the **orbits** of G in X.

10.5. **Definition.** The set $G_x := \{g \in G : g \cdot x = x\}$ is called the **stabiliser** of $x \in X$ in G.

10.6. **Theorem.** Let G act on X. Then $G_x \leq G$ for every $x \in X$ and

$$|G \cdot x| = |G : G_x|. \tag{10.7}$$

Proof. If $h \in G_x$ then also $h^{-1} \in G_x$, since

$$h^{-1} \cdot x = h^{-1} \cdot (h \cdot x) = (h^{-1}h) \cdot x = e \cdot x = x. \tag{10.8}$$

If $h, h' \in G_x$, we have $hh' \in G_x$, since

$$(hh') \cdot x = h \cdot (h' \cdot x) = h \cdot x = x. \tag{10.9}$$

Hence $G_x \leq G$.

To prove (10.7), consider the map

$$G \cdot x \to G/G_x, \qquad g \cdot x \mapsto gG_x. \tag{10.10}$$

This map is a well-defined and bijective, since

$$g \cdot x = g' \cdot x \Leftrightarrow g^{-1}g' \in G_x \Leftrightarrow gG_x = g'G_x. \tag{10.11}$$

□

10.7. **Corollary.** If G is finite, then for every $x \in X$ the number of elements in $G \cdot x$ divides $|G|$.

Proof. Apply (10.7) and Lagrange's Theorem. □

10.8. **Exercise.** Prove that:

(1) For every $g \in G$, $G_{g\cdot x} = gG_xg^{-1}$.
(2) $G_x \trianglelefteq G$ if and only if $G_x = G_y$ for all $y \in G \cdot x$.

10.9. **Definition.** The subset $V \subseteq X$ is called a **representative set** for the orbits $G \cdot x$, if

(1) For every $x \in X$ there is a $v \in V$ such that $G \cdot x = G \cdot v$,
(2) If $a \neq b$ for $a, b \in V$ then $G \cdot a \neq G \cdot b$.

The elements of V are called **representatives**.

10.10. With this notion we have

$$X = \bigcup_{x \in V} G \cdot x \quad \text{(disjoint union)}, \qquad |X| = \sum_{x \in V} |G : G_x|. \tag{10.12}$$

10.11. **Definition.** An element $x \in X$ is called a **fixed point** of the G action, if $g \cdot x = x$ for all $g \in G$. We denote by

$$\mathrm{Fix}_G(X) := \{x \in X : g \cdot x = x \text{ for all } g \in G\} \tag{10.13}$$

the **fixed point set** of the G action.

10.12. **Exercise.** Let $G = \mathrm{GL}(2,\mathbb{R})$ and $X = \mathbb{R}^2$.

(1) Show that the map

$$G \times X \to X, \qquad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}\right) \mapsto \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}, \tag{10.14}$$

defines a G action.

(2) What are the orbits and fixed point sets of this G action?

10.13. **Exercise.** Let $H \leq G$, and define H action by restricting the map (10.14) to $H \times X$. Calculate the orbits and fixed point sets in the following cases:

(1) $H = \mathrm{SO}(2)$.

(2) $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}$.

(3) $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}$.

(4) $H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\}$.

(5) $H = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$.

10.14. Note that $x \in \mathrm{Fix}_G(X)$ if and only if $G \cdot x = \{x\}$, i.e., $G_x = G$, i.e., $|G : G_x| = 1$. Therefore $x \in V$ and we can write (10.12) as

$$X = \mathrm{Fix}_G(X) \cup \bigcup_{\substack{x \in V \\ |G:G_x|>1}} G \cdot x, \qquad |X| = |\mathrm{Fix}_G(X)| + \sum_{\substack{x \in V \\ |G:G_x|>1}} |G : G_x|. \tag{10.15}$$

10.15. **Fixed Point Theorem.** Let G be a group of order p^r, p prime. If G acts on a finite set X, then

$$|X| \equiv |\mathrm{Fix}_G(X)| \bmod p. \tag{10.16}$$

In particular, if p does not divide $|X|$, there is at least one fixed point.

Proof. (10.15) says that

$$|X| - |\mathrm{Fix}_G(X)| = \sum_{\substack{x \in V \\ |G:G_x|>1}} |G : G_x|. \tag{10.17}$$

By Lagrange's Theorems every summand on the right hand side divides p^r. Since $|G : G_x| > 1$ we have $|G : G_x| = p^l$ for some $l \geq 1$. Hence $|G : G_x|$ is in particular divisible by p. □

10.16. **Example.** Let G be a group, $X \subseteq G$ a subset and $\mathcal{X} = \{gXg^{-1} : g \in G\}$ the family of subsets conjugate to X. The relation

$$g \cdot Y = gYg^{-1} \tag{10.18}$$

defines an action of G on $\mathcal{X}$. Note that there is only one orbit. In this case the stabiliser of X equals the normaliser of X,

$$G_X = N_G(X) = \{g \in G : gX = Xg\}. \tag{10.19}$$

Theorem 10.6 gives

$$|\mathcal{X}| = |G : N_G(X)|. \tag{10.20}$$

If we choose $X = H \leq G$ is a subgroup, we have the following.

10.17. **Theorem.** The number of distinct subgroups conjugate to H in G is equal to $|G : N_G(H)|$.

10.18. **Example.** The inner automorphism $g \cdot x := \varphi_g(x) = gxg^{-1}$ (recall Definition 2.16) defines a G action on itself (i.e., $G = X$). In this case the stabiliser G_x is the normalizer $N_G(x)$, and the fixed point set $\mathrm{Fix}_G(G)$ is the center $Z(G)$. Equation (10.15) translates to

$$|G| = |Z(G)| + \sum_{\substack{x \in V \\ |G:N_G(x)|>1}} |G : N_G(x)|. \tag{10.21}$$

This in turn implies:

10.19. **Theorem.** If G is a group of order p^r, p prime, then its center $Z(G)$ is non-trivial, i.e. $Z(G) \neq \{e\}$.

Proof. $Z(G)$, $N_G(x)$ are subgroups of G. By Lagrange's theorem, $|Z(G)| = p^k$ for some $k = 0, \ldots, r$, and also $|G : N_G(x)| = p^l$, for some $l = 1, \ldots, r$. In view of (10.21), $|Z(G)|$ is therefore divisible by p, and hence $k \geq 1$. That is, $|Z(G)| > 1$. □

10.20. **Definition.** A G action on X is called **transitive**, if for every $x, y \in X$ there is $g \in G$ such that $g \cdot x = y$.

10.21. **Example.** The translations $\mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}^d$, $(a, x) \mapsto (x + a)$ define a transitive group action of $G = (\mathbb{R}^d, +)$ on $X = \mathbb{R}^d$. This example is in fact a special case of the following general observation:

10.22. **Exercise.** Let $H \leq G$ and $X = G/H$. Show that

(1) The map $G \times X \to X$, $(g, aH) \mapsto gaH$, defines a G action on the left cosets G/H.
(2) G acts transitively on G/H.

11. Sylow's Theorems

11.1. **Lemma.** Let $n \in \mathbb{N}$ and p prime such that $n = p^r m$ for some $m \in \mathbb{N}$ with $\gcd(m,p) = 1$. Then, for every $s = 1, \dots, r$, p^{r-s+1} does not divide $\binom{n}{p^s}$.

Proof. We have

$$\begin{aligned}\binom{n}{p^s} &= \frac{n!}{p^s!(n-p^s)!} \qquad \text{(by definition)} \\ &= \frac{n(n-1)\cdots(n-p^s+1)}{1\cdot 2\cdots p^s} \\ &= mp^{r-s}\frac{(n-1)\cdots(n-p^s+1)}{1\cdot 2\cdots(p^s-1)} \\ &= mp^{r-s}\binom{n-1}{p^s-1}.\end{aligned} \tag{11.1}$$

We thus need to show that the integer

$$\binom{n-1}{p^s-1} = \prod_{i=1}^{p^s-1}\frac{mp^r-i}{i} \tag{11.2}$$

is not divisible by p. Let us write for each factor

$$\frac{mp^r-i}{i} = \frac{mp^{r-t_i}-\tilde{i}}{\tilde{i}} \tag{11.3}$$

where p^{t_i} is the highest power with $t_i \le r$ that divides i, and $i = p^{t_i}\tilde{i}$. Since $i \le p^s-1$, we have in fact $t_i < s$, so $r - t_i > 0$, and $\gcd(\tilde{i}, p) = 1$.

If we assume that (11.2) is divisible by p, than at least one factor, say for $i = j$,

$$\frac{mp^r-j}{j} = \frac{mp^{r-t_j}-\tilde{j}}{\tilde{j}} \tag{11.4}$$

is divisible by p, and in particular p divides $mp^{r-t_j} - \tilde{j}$. Since $r - t_j > 0$ (see above), p divides $\tilde{j}$. But this contradicts $\gcd(\tilde{j}, p) = 1$. □

11.2. **The First Sylow Theorem.** Let G be a finite group of order $n = p^r m$, with p prime and $\gcd(m,p) = 1$. Then, given any $s = 1, \dots, r$, there is a subgroup of order p^s.

Proof. Let

$$\mathcal{X}_s = \{A \subseteq G : |A| = p^s\} \tag{11.5}$$

be the family of subsets of G, which have precisely p^s elements. Elementary combinatorics tells us that $|\mathcal{X}_s| = \binom{n}{p^s}$. It is easy to check that $A \mapsto g \cdot A := gA$ defines an

action on the family $\mathcal{X}$ of subsets A of G. Since $|gA| = |A|$, it in fact defines an action on $\mathcal{X}_s$. We have therefore a decomposition into disjoint orbits,

$$\mathcal{X}_s = \bigcup_{A \in \mathcal{V}} GA \tag{11.6}$$

where $\mathcal{V}$ is a representative set. With Theorem 10.6 we have that

$$\binom{n}{p^s} = |\mathcal{X}_s| = \sum_{A \in \mathcal{V}} |GA| = \sum_{A \in \mathcal{V}} |G : G_A|. \tag{11.7}$$

By Lemma 11.1 the above is not divisible by p^{r-s+1}, hence at least one summand $|G : G_A|$ is not divisible by p^{r-s+1}. Thus p^{r-s} is the highest power of p that may divide $|G : G_A|$.

By assumption $p^r m = |G| = |G : G_A||G_A|$. We the previous observation this implies that p^s divides $|G_A|$, and so $|G_A| \geq p^s$.

Since G_A is the stabilizer of A we have $G_A A = A$, i.e., $G_A a \subseteq A$ for every $a \in A$. Therefore $|G_A| = |G_A a| \leq |A| = p^s$.

Combining this with the above inequality yields $|G_A| = p^s$. This proves the existence of a subgroup of order p^s. □

11.3. **Corollary.** (Cauchy's Theorem.) Let G be a finite group whose order is divisible by the prime p. Then G contains an element of order p.

Proof. By the First Sylow Theorem, G contains a subgroup H of order p. By Corollary 6.18 H is cyclic, and its generator thus has order p. □

11.4. **Definition.** Let p be a prime. A group G is called **p-group**, if the order of every element of G is a power of p.

That is, by Corollary 5.7, for every $g \in G$ there is a $k \geq 0$ such that $g^{p^k} = e$.

11.5. **Corollary.** A finite group is a p-group, if and only if its order is a power of p.

Proof. If $|G| = p^l$, then by Fermat's Little Theorem 6.14, $g^{p^l} = e$ for all g, and hence G is a p-group. If, on the other hand, $|G|$ would be divisible by a prime $q \neq p$, then (by the previous Theorem of Cauchy) G would have an element of order q, which contradicts the assumption that G is a p-group. □

11.6. **Definition.** Let G be a group. We say H is a **p-subgroup of** G if $H \leq G$ and H is a p-group.

11.7. **Definition.** Let G be a group. A subgroup $H \leq G$ is called a **p-Sylow group** of G, if

(1) H is a p-group.
(2) If K is is a p-subgroup of G such that $H \subseteq K$, then $H = K$.

Note that (2) says that p-Sylow groups are maximal in the family of p-subgroup. In particular, a p-group is equal to its (unique) p-Sylow group.

11.8. **Theorem.** Let G be a finite group of order $n = p^r m$, with p prime and $\gcd(m, p) = 1$. Then every subgroup of order p^r is a p-Sylow group.

Proof. Let $H \leq G$ with $|H| = p^r$. By Corollary 11.5 H is a p-group. Let K be a further p-group with $H \leq K \leq G$. By Corollary 11.5 $|K| = p^l$ for some l. Since by Lagrange's Theorem $|K|$ divides $p^r m$, we have $l \leq r$. Hence $|K| \leq |H|$ and thus $K = H$. □

11.9. **Corollary.** Let G be a finite group of order $n = p^r m$, with p prime and $\gcd(m, p) = 1$. Then G contains at least one p-Sylow group of order p^r.

Proof. The First Sylow Theorem shows that G contains a subgroup of order p^r, which by 11.8 is a p-Sylow group. □

11.10. **Lemma.** If $H \leq G$ is a p-subgroup (resp. p-Sylow group), then, for any $g \in G$, gHg^{-1} is a p-subgroup (resp. p-Sylow group).

Proof. Since x and gxg^{-1} have the same order, H is a p-subgroup if and only if gHg^{-1} is.

Let H be a p-Sylow group and assume $gHg^{-1} < K$ for some p-subgroup K. Then $H < K'$ with the p-subgroup $K' = g^{-1}Kg$. But $H < K'$ contradicts the assumption that H is a p-Sylow group, cf. Definition 11.7 (2). □

11.11. **The Second Sylow Theorem.** Let G be a finite group of order $n = p^r m$, with p prime and $\gcd(m, p) = 1$, and let P be a p-Sylow group of G. Then, every p-subgroup H of G is conjugate to a subgroup of P.

Proof. First assume P is a p-Sylow group of order p^r. Consider the left cosets

$$\mathcal{X} := \{gP : g \in G\}. \tag{11.8}$$

Let H be a p-subgroup of G, and consider the H action

$$H \times \mathcal{X} \to \mathcal{X}, \qquad (h, gP) \mapsto (hg)P. \tag{11.9}$$

We decompose $\mathcal{X}$ into disjoint orbits,

$$\mathcal{X} = \bigcup_{g \in \mathcal{V}} HgP, \qquad |\mathcal{X}| = \sum_{g \in \mathcal{V}} |HgP|. \tag{11.10}$$

Now

$$|\mathcal{X}| = |G : P| = \frac{|G|}{|P|} = \frac{p^r m}{p^r} = m, \tag{11.11}$$

and thus p does not divide $|\mathcal{X}|$. Therefore at least one of the summands in (11.10) is not divisible by p, say $|HaP|$. On the other hand, by Corollary 10.7, $|HaP|$ divides $|H|$,

but since $|H|$ is a power of p, we find $|HaP| = 1$. We conclude from this that gP is a fixed point under the H action, i.e., for all $h \in H$,

$$hgP = gP \Leftrightarrow g^{-1}hgP = P \Leftrightarrow g^{-1}hg \in P \Leftrightarrow g^{-1}Hg \subseteq P, \tag{11.12}$$

and we have proved the Theorem for p-Sylow groups of order p^r.

To extend the statement to a p-Sylow groups P' of arbitrary order, choose in the above $H = P'$. Then $g^{-1}P'g \subseteq P$. By Lemma 11.10 $g^{-1}P'g$ is a p-Sylow group, and hence by Definition 11.7 (2) $g^{-1}P'g = P$, which implies $|P'| = p^r$. So the above restriction to order p^r was in fact already dealing with the most general case. □

We highlight the last argument of the above proof in the following statement.

11.12. **Corollary.** Let G be a finite group of order $n = p^r m$, with p prime and $\gcd(m, p) = 1$. Then:

(1) Every p-Sylow group has order p^r.
(2) Every pair of p-Sylow groups of G are conjugate (and thus isomorphic).

11.13. **Corollary.** A p-Sylow group of a group G is normal in G if and only if P is the only p-Sylow group of G.

Proof. Suppose $P \trianglelefteq G$ and $P' \leq G$ are p-Sylow groups of G. By Corollary 11.12 there is $x \in G$ such that $P' = xPx^{-1}$, and this $= P$ since P is normal.

On the other hand, if P is a p-Sylow group, then so is gPg^{-1} for any $g \in G$ (recall Lemma 11.10). Since we assume P is the unique p-Sylow group, we have $P = gPg^{-1}$ for all $g \in G$. □

Recall that the normaliser $N_G(H) = \{x \in G : xH = Hx\}$ of a subgroup $H \leq G$ is the largest subgroup of G in which H is normal. Hence $N_G(H)/H$ is a quotient group.

11.14. **Lemma.** Let P be a p-Sylow group of G. If $\overline{a} \in N_G(P)/P$ has order p^l for some $l \geq 0$, then $\overline{a}$ is the identity in $N_G(P)/P$ (i.e., $a \in P$).

Proof. The cyclic group $\langle\overline{a}\rangle$ has order p^l and hence is a p-group. By Theorem 8.10 (2) there is a subgroup H [namely $H = \pi^{-1}(\langle\overline{a}\rangle)$] such that $P \leq H \leq N_G(P)$ and $\langle\overline{a}\rangle = H/P$. Now $|H| = |H/P||P|$ and so $|H|$ is a power of p, hence H is a p-group. Definition 11.7 (2) implies $H = P$ and thus $\langle\overline{a}\rangle = P/P = \{\overline{e}\}$. □

11.15. **Lemma.** Let P be a p-Sylow group of G. If $a \in G$ with $\operatorname{ord} a$ a power of p, and $aPa^{-1} = P$, then $a \in P$.

Proof. Since $aP = Pa$ we have $a \in N_G(P)$. The image of a under the canonical epimorphism in $N_G(P)/P$ is also a power of p. The previous Lemma 11.14 implies $a \in P$. □

11.16. **The Third Sylow Theorem.** Let G be a finite group whose order is divisible by p. Then the number of p-Sylow groups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Denote by

$$\mathcal{X} = \{P_0, P_1, P_2, \ldots, P_r\} \tag{11.13}$$

the collection of p-Sylow groups P_i of G. By Corollary 11.12,

$$\mathcal{X} = \{gP_0g^{-1} : g \in G\}, \tag{11.14}$$

and by Theorem 10.17, $|\mathcal{X}| = |G : N_G(P_0)| = |G|/|N_G(P_0)|$. Hence $|\mathcal{X}|$ divides $|G|$.

To prove the second part of the statement, define the action

$$P \times \mathcal{X} \to \mathcal{X}, \qquad (h, X) \mapsto hXh^{-1}. \tag{11.15}$$

Equation (10.15) yields

$$|\mathcal{X}| = |\operatorname{Fix}_P(\mathcal{X})| + \sum_{\substack{X \in \mathcal{V} \\ |P:P_X|>1}} |P : P_X|. \tag{11.16}$$

Now

$$\operatorname{Fix}_P(\mathcal{X}) = \{X \in \mathcal{X} : hXh^{-1} = X \text{ for all } h \in P\}. \tag{11.17}$$

Since X is a p-Sylow group, Lemma 11.15 says that the condition $hXh^{-1} = X$ for all $h \in P$ implies $P \subseteq X$ and hence $P = X$ by Definition 11.7 (2). Therefore

$$\operatorname{Fix}_P(\mathcal{X}) = \{P\}, \qquad |\operatorname{Fix}_P(\mathcal{X})| = 1, \tag{11.18}$$

and (11.16) becomes

$$|\mathcal{X}| = 1 + \sum_{\substack{X \in \mathcal{V} \\ |P:P_X|>1}} |P : P_X|. \tag{11.19}$$

Since $|P : P_X| = |P|/|P_X|$ are of the form p^j for some $j \geq 0$, we conclude that the terms corresponding to $|P : P_X| > 1$ are divisible by p. □

12. Applications of Sylow's Theorems

12.1. We will know discuss some applications of Sylow's theorems to the classification of groups G of order p^r. The simplest case is $r = 1$. Then by Corollary 6.18 G is cyclic, and by Theorem 8.5 it is isomorphic to $(\mathbb{Z}_p, +)$.

In the case $r = 2$ we know from Theorem 10.19 that the center $Z(G)$ is non-trivial, i.e., $|Z(G)| > 1$ and hence $|Z(G)| = p$ or $|Z(G)| = p^2$. In the latter case $Z(G) = G$ and G is abelian. In the former case $G/Z(G)$ has order p and is thus cyclic (Corollary 6.18). This implies G is abelian (why?) and so $Z(G) = G$, which contradicts our assumption $|Z(G)| = p$. We conclude that every group of order p^2 is abelian. The following theorem gives a complete classification:

12.2. **Theorem.** For every prime p there are, up to isomorphism, precisely two non-isomorphic groups of order p^2; these are $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. By Theorem 5.11, $\mathbb{Z}_{p^2}$ has precisely one subgroup of order p, whereas $\mathbb{Z}_p \times \mathbb{Z}_p$ has at least two: $\mathbb{Z}_p \times \{0\}$ and $\{0\} \times \mathbb{Z}_p$. The two groups are therefore non-isomorphic.

Assume G has order p^2 and is not isomorphic to $\mathbb{Z}_{p^2}$. This means G is not cyclic. By Cauchy's Theorem 11.3 there is $a \in G$ with $\operatorname{ord} a = p$. For $b \notin \langle a \rangle$ we have $\operatorname{ord} b = p$ or $= p^2$; the latter is impossible since this would imply G is cyclic. So $\operatorname{ord} b = p$ and $|\langle b \rangle| = p$. Note that, since $b \notin \langle a \rangle$ and any group of prime order cannot have non-trivial subgroups, we have $\langle a \rangle \cap \langle b \rangle = \{e\}$. Clearly $|\langle a \rangle \langle b \rangle| = |\langle a \rangle||\langle b \rangle| = p^2 = |G|$ and thus $G = \langle a \rangle \langle b \rangle$. By the first observation in 12.1 G is abelian, hence $\langle a \rangle$ and $\langle b \rangle$ are normal subgroups, and so Theorem 8.5 and Theorem 9.12 show that $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. □

The case $r > 2$ is harder; we have the following general theorem, which allows a reduction to smaller r.

12.3. **Theorem.** Every group of order p^r, p prime, has a normal subgroup of order p^{r-1}.

Proof. Proof by induction. For $r = 1$ the statement is trivial. By Theorem 10.19, $Z(G)$ is non-trivial, i.e., $|Z(G)| = p^l$, for $l \geq 1$. The First Sylow Theorem guarantees the existence of a subgroup $N \leq Z(G)$ of order p, which (as a subgroup of the center) is normal. Then $|G/N| = |G|/|N| = p^{r-1}$. By assumption, the group G/N has a normal subgroup $\overline{K}$ of order p^{r-2}. By Theorem 8.10 (2) there is a subgroup K with $N \leq K \trianglelefteq G$, such that $\overline{K} = K/N$. Finally, $p^{r-2} = |\overline{K}| = |K|/|N| = |K|/p$ implies $|K| = p^{r-1}$. □

Iterated application of the above theorem proves:

12.4. **Corollary.** Let G be a finite group of order p^r, p prime. Then there are groups G_i $(i = 0, \ldots, r)$ of order p^i such that

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_{r-1} \trianglelefteq G_r = G. \tag{12.1}$$

12.5. **Theorem.** Let G be a finite group of order pq, with $p < q$ both prime. Then

(1) G contains precisely one q-Sylow group of order q.
(2) If $q \neq kp + 1$ for all $k \geq 0$, then G is cyclic.

Proof. (1) Corollary 11.9 shows that there is at least one q-Sylow group. Furthermore, any such group has of order q (cf. Theorem 11.8). Let s_q be the number of the q-Sylow groups of G. By the Third Sylow Theorem, s_q divides $|G|$, so $s_q \in \{1, p, q, pq\}$, and furthermore is of the form $s_q = kq + 1$, for some $k \geq 0$. The only consistent choice is $s_q = 1$, since $p = kq + 1$ implies $p > q$ (contradicting our assumption $p < q$), $q = kq + 1$ implies $q > q$, and $pq = kq + 1$ implies that q divides 1, which is false.

(2) The plan is to prove $G \simeq \mathbb{Z}_p \times \mathbb{Z}_q$, which, by Theorem 9.16 is equivalent to $G \simeq \mathbb{Z}_{pq}$, and thus establishes that G is cyclic. Let s_p be the number of the p-Sylow groups of G. Again, by the Third Sylow Theorem, s_p divides $|G|$, so $s_p \in \{1, p, q, pq\}$, and in addition is of the form $s_p = kp + 1$, for some $k \geq 0$. And again, $s_p = 1$ is the only possibility, since $s_p = p, pq$ are ruled out since p does not divide 1, and $s_p = q$ violates the assumption of (2). Hence we have precisely one subgroup H_p of order p and precisely one subgroup H_q of order q. By Corollary 6.19 $H_p \cap H_q = \{e\}$. Therefore Theorem 8.5 and Theorem 9.12 imply that $G \simeq \mathbb{Z}_p \times \mathbb{Z}_q$ (cf. the proof of Theorem 12.2). □

12.6. **Corollary.** There are precisely two (up to isomorphism) groups of order $2p$, p prime; these are $\mathbb{Z}_{2p}$ and the dihedral group D_p.

Proof. Let G be a group of order $2p$. The statement for $p = 2$ follows from Theorem 12.2. For $p > 2$ we now from the previous proof that $s_p = 1$ and $s_2 = 1$ or $s_2 = p$. We have seen that $s_2 = 1$ implies G is cyclic, i.e., $G \simeq \mathbb{Z}_{2p}$. If $s_2 = p$, then we have p-subgroups of order 2. Let P be the unique p-Sylow group of order p. P is then normal (Corollary 11.13) and cyclic, say $P = \langle a \rangle$. We have the coset decomposition $G = P \cup bP$ with $b \in G \setminus P$. There are three possibilities: $\operatorname{ord} b = 2, p, 2p$. If $\operatorname{ord} b = p$, then $|\langle b \rangle| = p$ which implies $\langle b \rangle = P$ by the uniqueness of P—a contradiction. If $\operatorname{ord} b = 2p$ then G is cyclic and there is precisely one 2-Sylow-group—a contradiction. Hence $\operatorname{ord} b = 2$. Since also $G = P \cup abP$, by the same reasoning $\operatorname{ord}(ab) = 2$. We conclude

$$G = \{e, a, a^2, \ldots, a^{p-1}, b, ba, ba^2, \ldots, ba^{p-1}\} \tag{12.2}$$

with $\operatorname{ord} a = p$, $\operatorname{ord} b = \operatorname{ord}(ab) = 2$, and so $G = D_p$ in this case. □

12.7. **Lemma.** If P is a p-Sylow group of the finite group G, then $N_G(N_G(P)) = N_G(P)$.

Proof. By Corollary 11.13, P is the unique p-Sylow group of $N_G(P)$. If $x \in N_G(N_G(P))$ then $xN_G(P)x^{-1} \subseteq N_G(P)$, and (because $P \subseteq N_G(P)$) we have $xPx^{-1} \subseteq N_G(P)$. Since also xPx^{-1} is p-Sylow, we have by uniqueness $xPx^{-1} = P$. So $x \in N_G(P)$ and so $N_G(N_G(P)) \subseteq N_G(P)$. Recall $N_G(P) \subseteq N_G(N_G(P))$ by definition. □

12.8. **Definition.** We say a group G satisfies the **normaliser condition** if $H < G$ implies $H < N_G(H)$.

12.9. **Lemma.** Assume the finite group G satisfies the normaliser condition. Then for every prime p dividing $|G|$ there is precisely one p-Sylow group of G.

Proof. Let P be a p-Sylow group of G. By the previous lemma $N_G(N_G(P)) = N_G(P)$, and so the normaliser condition rules $N_G(P) < G$ out, i.e., we have in fact $N_G(P) = G$. Hence $P \trianglelefteq G$, and Corollary 11.13 completes the proof. □

12.10. **Theorem.** Assume the finite group G satisfies the normaliser condition, and let $p_1, \dots, p_r$ be the primes dividing $|G|$. Then

$$G = G_{p_1} \cdots G_{p_r} \tag{12.3}$$

with the p-Sylow groups

$$G_p := \{x \in G : \text{ ord } x = p^k \text{ for some } k \geq 0\}. \tag{12.4}$$

Proof. $\langle x \rangle$ is a p-group, and so $\langle x \rangle \leq H_p$, where H_p is the unique p-Sylow group of G constructed in Lemma 12.9. Hence $G_p \leq H_p$. Trivially, $H_p \leq G_p$. Exercise 9.17 yields that

$$G_{p_1} \cdots G_{p_r} \simeq G_{p_1} \times \cdots \times G_{p_r}. \tag{12.5}$$

Since the outer direct product has the same order as G, it is isomorphic to G, and the proof is complete. □

12.11. **Exercise.** Let G be a group of order 12, and s_2 and s_3 the number of 2- resp. 3-Sylow groups in G.

(1) Which numbers are possible for s_2 and s_3? Justify your answer.
(2) Show that it is not possible to have $s_2 = 3$ and $s_3 = 4$ simultaneously.
(3) Show that, if $s_2 = s_3 = 1$, then G is abelian and there are two possible choices of G.

12.12. **Exercise.** Determine all groups of order 8 (up to isomorphism).

13. FINITELY GENERATED ABELIAN GROUPS

13.1. It is no surprise that the structure of abelian groups is easier to analyze than that of more general groups. It is traditional to use the symbol $+$ for the group composition "addition"), $)$ for the neutral element, $-g$ for the inverse of g, and call the direct product $\times$ of abelian groups the **direct sum**, denoted by $\oplus$.

13.2. A finitely generated abelian group $G = \langle g_1, \ldots, g_n \rangle$ then consists of all linear combinations of the form $m_1 g_1 + \ldots m_n g_n$ with $m_i \in \mathbb{Z}$. Note that a finitely generated abelian group is not necessarily finite; one example of an infinite, finitely generated abelian group is $\mathbb{Z}$.

13.3. The abelian group G is the direct sum of the subgroups $G_1, \ldots, G_n$, if and only if (1) every $g \in G$ can be written $g = g_1 + \ldots + g_n$ with $g_i \in G_i$ and (2) $g_1 + \ldots + g_n = 0$ implies $g_i = 0$ for all i.

13.4. The p-Sylow groups of a finite abelian group G are easily described: Let p be a prime dividing $|G|$. Then

$$G_p = \{x \in G : \ p^k x = 0 \text{ for some } k \geq 0\} \tag{13.1}$$

is the unique p-Sylow group of G, cf. Lemma 12.9 (note that every abelian group satisfies the normaliser condition). Theorem 12.10 furthermore shows:

13.5. **Corollary.** Every finite abelian group is the direct sum of its p-Sylow groups.

The following provides a complete description of all finitely generated abelian groups.

13.6. **Theorem.** An abelian group is finitely generated, if and only if it is the direct sum of finitely many cyclic groups. In this case

$$G \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{k_r}} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}, \tag{13.2}$$

with (not necessarily distinct) primes $p_1, \ldots, p_r$.

(The numbers $p_1^{k_1}, \ldots, p_r^{k_r}$ and the number of $\mathbb{Z}$ factors are in fact uniquely determined by G, but we will not prove this here.)

Proof. Assume G is the direct sum of finitely many cyclic groups. Then the generators of the cyclic groups form a finite generating set for G.

On the other hand, assume G is generated by n elements, $a_1, \ldots, a_n$, with n minimal (i.e., there is no generating set with less than n elements). We proceed by induction on n. If $n = 1$, then G is cyclic.

If in the case of general n, for any minimal set of generators $a_1, \ldots, a_n$ we have that $m_1 a_1 + \ldots + m_n a_n = 0$ implies $m_i a_i = 0$ for all i, then by 13.3

$$G = \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle. \tag{13.3}$$

Suppose this is not the case, i.e., there is a minimal set of generators such that $m_1a_1 + \ldots + m_na_n = 0$ has a solution with at least one $m_ia_i \neq 0$. What we will show is that G can still be written as a direct product of cyclic groups.

Assume without loss of generality that all $m_i \geq 0$ (replace a_i by $-a_i$ if necessary, $-a_i$ will still be a generator). Let $m > 0$ be the smallest non-zero coefficient that can appear for any choice of generators. Without loss of generality, we may assume $m = m_1$ (if necessary, relabel the a_i in different order).

Let us prove the following:

Claim 1. If $m_1'a_1 + \ldots + m_n'a_n = 0$ for some $m_i' \in \mathbb{Z}_{\geq 0}$, then m divides m_1'.

Claim 2. m divides m_i for all i.

Proof of Claim 1. Write $m_1' = hm + r$ with $0 \leq r < m$. Then

$$0 = \sum_{i=1}^{n} m_i'a_i - h\left(\sum_{i=1}^{n} m_ia_i\right) = ra_1 + \sum_{i=2}^{n}(m_i' - hm_i)a_i. \tag{13.4}$$

Because m is smallest possible positive coefficient and $r < m$, we find that $r = 0$. □

Proof of Claim 2. Write $m_2 = s_2m + r$ with $0 \leq r < m$. Then

$$0 = \sum_{i=1}^{n} m_ia_i = ma_1 + ms_2a_2 + ra_2 + \sum_{i=3}^{n} m_ia_i = ma_1' + ra_2 + \sum_{i=3}^{n} m_ia_i \tag{13.5}$$

with $a_1' = a_1 + s_2a_2$. Now $\{a_1', a_2, \ldots, a_n\}$ is a minimal generating set. As above, Because m is smallest possible positive coefficient and $r < m$, we find that $r = 0$. This proves the claim for m_2. The same argument of course also yields the claim for $m_3, m_4, \ldots, m_n$. □

Let $m_i = s_im_1$ and set

$$a_1^* := a_1 + s_2a_2 + \ldots + s_na_n. \tag{13.6}$$

Then

$$m_1a_1^* = m_1a_1 + m_1s_2a_2 + \ldots + m_1s_na_n = \sum_{i=1}^{n} m_ia_i = 0. \tag{13.7}$$

Let us now show

Claim 3.

$$G = \langle a_1^* \rangle \oplus \langle a_2, \ldots, a_n \rangle. \tag{13.8}$$

Proof. Note that $G = \langle a_1^*, a_2, \ldots, a_n \rangle$, and for $g \in \langle a_1^* \rangle \cap \langle a_2, \ldots, a_n \rangle$ we have

$$g = k_1a_1^* = k_2a_2 + \ldots + k_na_n, \tag{13.9}$$

i.e.,

$$k_1a_1^* - \left(k_2a_2 + \ldots + k_na_n\right) = 0. \tag{13.10}$$

Using (13.6),

$$k_1 a_1 + (k_1 s_1 - k_2) a_2 + \ldots\ldots + (k_1 s_n - k_n) a_n = 0. \tag{13.11}$$

Claim 1 now implies $k_1 = hm_1$ and so $g = k_1 a_1^* = hm_1 a_1^* = 0$ (since $m_1 a_1^* = 0$). So $g = 0$ and Claim 3 is proved. □

By the induction hypothesis, $\langle a_2, \ldots, a_n \rangle$ is the direct sum of finitely many cyclic groups. Claim 3 thus concludes the proof of the first part of the Theorem.

The isomorphism (13.2) follows from the facts that every cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ (for some $n \in \mathbb{N}$), and that $\mathbb{Z}_n$ can be written as a direct sum of groups of the form $\mathbb{Z}_{p^k}$ (Corollary 9.18). □

13.7. **Exercise.** Let G be a finitely generated abelian group. Prove that, if every $g \in G$ has finite order, then G is finite.

14. THE SYMMETRIC GROUP

14.1. **Definition.** Let X be a set and consider the set $S(X)$ of bijective maps $f : X \to X$, and denote by $\circ$ the usual composition of maps. Then $(S(X), \circ)$, or $S(X)$ for short, is called the **symmetric group** of X (often also the **group of permutations** of X).

14.2. **Exercise.** Prove that the symmetric group is indeed a group.

14.3. An important example is the symmetric group of $\mathbb{N}$, $S(\mathbb{N})$, and the group of permutations of n elements, $S_n := S(\{1, 2, \ldots, n\})$, which we view as a subgroup of S_{n+1} and of $S(\mathbb{N})$. It follows from elementary combinatorics that $|S_n| = n!$.

14.4. An element $f \in S_n$ is often represented as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}. \tag{14.1}$$

For the product $f \circ g$ we have

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ g(1) & g(2) & \cdots & g(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(g(1)) & f(g(2)) & \cdots & f(g(n)). \end{pmatrix} \tag{14.2}$$

For example ($n = 5$):

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}. \tag{14.3}$$

The inverse of f is calculated by swapping top and bottom rows,

$$\begin{pmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & \cdots & n \end{pmatrix} \tag{14.4}$$

and re-arranging the columns in such a way that the top row appears in the correct order. For example

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}. \tag{14.5}$$

14.5. **Example.** The Klein four group can be realized as the following subgroup of S_4:

$$V_4 = \left\{ e = \mathrm{id},\ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},\ b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},\ c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}. \tag{14.6}$$

14.6. It is convenient to reduce the notation by ignoring those elements that remain unchanged, e.g.,

$$\begin{pmatrix} 1 & 2 & 3 & 5 \\ 3 & 1 & 5 & 2 \end{pmatrix} := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}. \tag{14.7}$$

The above transformation corresponds to the substitutions

$$1 \mapsto 3 \mapsto 5 \mapsto 2 \mapsto 1, \qquad 4 \mapsto 4, \tag{14.8}$$

and is in fact completely characterized by the notation $(1,3,5,2)$ (or any cyclic permutation thereof). This motivates the following:

14.7. **Definition.** A permutation $f \in S_n$ is called **r-cycle**, if there is a (not necessarily ordered) subset

$$I = \{i_1, \dots, i_r\} \subseteq \{1, \dots, n\} \tag{14.9}$$

such that

$$f(i_k) = i_{k+1} \quad (1 \le k < r), \qquad f(i_r) = i_1, \qquad f(m) = (m) \quad (m \notin I). \tag{14.10}$$

We use the notation

$$f = (i_1, \dots, i_r). \tag{14.11}$$

A two-cycle is also called a **transposition**.

14.8. Note that the condition $f(i_r) = i_1$ is superfluous; it is implied by the other assumptions. The only one-cycle is the identity $\mathrm{id} = (i)$, for any $i \in \mathbb{N}$. It is customary to use (1). Here are a few calculation rules for the cycle notation:

14.9. **Theorem.**

(1) $(i_1, i_2, \dots, i_r) = (i_{m+1 \bmod r}, \dots, i_{m+r \bmod r})$ for all $m \in \mathbb{Z}$ (i.e., a cycle is invariant under cyclic permutations).
(2) $(i_1, \dots, i_r) = (i_1, \dots, i_j)(i_j, \dots, i_r)$ $(2 \le j \le r-1)$.
(3) $(i_1, \dots, i_r) = (i_1, i_2)(i_2, i_3) \cdots (i_{r-2}, i_{r-1})(i_{r-1}, i_r)$.
(4) $(i_1, \dots, i_r)^m = \begin{pmatrix} i_1 & \dots & i_r \\ i_{m+1 \bmod r} & \dots & i_{m+r \bmod r} \end{pmatrix}$.
(5) $\mathrm{ord}(i_1, \dots, i_r) = r$.
(6) $(i_1, \dots, i_r)^{-1} = (i_r, i_{r-1}, \dots, i_1)$.
(7) $f(i_1, \dots, i_r)f^{-1} = (f(i_1), \dots, f(i_r))$.

Proof. (1)–(6) are left as exercises. As to (7), since $g \mapsto fgf^{-1}$ is an automorphism, it is in view of (3) sufficient to prove the claim for transpositions. We have for the

permutation $f(i,j)f^{-1}$ of the element k

$$f(i,j)f^{-1}(k) = \begin{cases} k & \text{if } f^{-1}(k) \notin \{i,j\}, \\ f(i) & \text{if } f^{-1}(k) = j, \\ f(j) & \text{if } f^{-1}(k) = i. \end{cases} \tag{14.12}$$

Thus $f(i,j)f^{-1} = (f(i), f(j))$. □

14.10. **Theorem.** Let $n \in \mathbb{N}$, and set

$$f_l = \begin{cases} (l) & (l = n+1) \\ (l, n+1) & (1 \le l \le n). \end{cases} \tag{14.13}$$

Then we have the decomposition

$$S_{n+1} = \bigcup_{l=1}^{n+1} f_l S_n \tag{14.14}$$

into disjoint cosets $f_l S_n$.

Proof. Let $f \in S_{n+1}$. If $f(n+1) = n+1$ then $f \in S_n = f_{n+1}S_n$. If $f(n+1) = l$ for some $l \le n$, then $f_l f(n+1) = f_l(l) = n+1$, so $f_l f \in S_n$. Since $f_l = f_l^{-1}$ we have $f \in f_l S_n$. Hence (14.14) is proved. To show the cosets are disjoint, note that

$$\begin{aligned} f_k S_n = f_l S_n &\Leftrightarrow f_l^{-1} f_k S_n = S_n \\ &\Leftrightarrow f_l^{-1} f_k (n+1) = n+1 \\ &\Leftrightarrow f_k(n+1) = f_l(n+1) \\ &\Leftrightarrow k = l \end{aligned} \tag{14.15}$$

since $f_l(n+1) = l$ for $1 \le l \le n+1$. □

14.11. The above theorem implies that $|S_{n+1} : S_n| = n+1$. Thus, via Lagrange's Theorem, $|S_{n+1}| = (n+1)|S_n|$, and we recover (by induction on n) the classical combinatorial result $|S_n| = n!$.

14.12. **Corollary.** Every permutation $f \in S_n$ ($n \ge 2$) can be represented as a product of transpositions. (That is, S_n is generated by its transpositions.)

Proof by induction. For $n = 2$, S_2 is the group of $2! = 2$ elements $\{(1), (1,2)\}$, where $(1) = (1,2)(1,2)$. Hence $S_2 = \langle (1,2) \rangle$. If $f \in S_{n+1}$, then Theorem 14.10 says that $f = f_l g$ where f_l is a transposition (or the identity) and $g \in S_n$. By the induction hypothesis g is a product of transpositions, and therefore the same is true for f. □

14.13. Note that in fact $S_n = \langle (1,2), (1,3), \ldots, (1,n)\rangle$, since $(i,j) = (1,i)(1,j)(1,i)$:

$$\begin{array}{lll} 1 & i & j \\ i & 1 & j \\ i & j & 1 \\ 1 & j & i \end{array}$$

14.14. **Definition.** Two cycles $f = (i_1, \ldots, i_r)$ and $g = (j_1, \ldots, j_s)$ are called **disjoint**, if $\{i_1, \ldots, i_r\} \cap \{j_1, \ldots, j_s\} = \emptyset$.

14.15. **Theorem.** Disjoint cycles commute.

Proof. We have $fg(m) = m = gf(m)$ if $m \notin \{i_1, \ldots, i_r\} \cup \{j_1, \ldots, j_s\}$. Furthermore for $m \in \{i_1, \ldots, i_r\}$ (and thus by assumption $m \notin \{j_1, \ldots, j_s\}$) we have $fg(m) = f(m) = gf(m)$, since $f(m) \in \{i_1, \ldots, i_r\}$ and thus $f(m) \notin \{j_1, \ldots, j_s\}$. The analogous argument applies when $m \in \{j_1, \ldots, j_s\}$. □

14.16. **Theorem.** Every permutation $f \in S_n$ can be expressed as a unique product of disjoint cycles (up to ordering). [This product is called the **canonical factorisation** of f.]

Proof. Let $X = \{1, 2, \ldots, n\}$, and

$$X = \bigcup_x \langle f\rangle x = \bigcup_{i=1}^{t} X_i \tag{14.16}$$

the decomposition of X into disjoint orbits of the action of the cyclic subgroup $\langle f\rangle \leq S_n$. Define

$$f_i(j) := \begin{cases} f(j) & (j \in X_i) \\ j & (j \notin X_i). \end{cases} \tag{14.17}$$

If X_i comprises only one element, then $f_i = \mathrm{id}$. If, say, $X_1, \ldots, X_k$ are orbits with more than one element, then $f_1, \ldots, f_k$ are disjoint cycles, since $f_i(j_l) = f(j_l) = j_{l+1}$ for all $j_l \in \{j_1, \ldots, j_m\} = X_i$; this is a consequence of the fact that X_i is an orbit of the cyclic group $\langle f\rangle$. We therefore have $f = f_1 \cdots f_k$. Note that X_i is the only non-trivial orbit (i.e., it has more than one element) of the action of $\langle f_i\rangle$.

To show uniqueness, suppose $f = g_1 \ldots g_l$ is a different factorisation into disjoint cycles, and let Y_i be the non-trivial orbit of $\langle g_i\rangle$. Since the action of $\langle f\rangle$ and $\langle g_i\rangle$ on Y_i are the same, Y_i is also an orbit of $\langle f\rangle$. If $x \in X$ is not changed by at least one g_i, then $f(x) = x$. Hence $\langle f\rangle$ has no further non-trivial orbits than $Y_1, \ldots, Y_l$. But this implies $k = l$, $X_1 = Y_1$, $X_2 = Y_2$, etc. (after suitably relabeling the Y_i). Now $g_i|X_i = f|X_i = f_i|X_i$, and one the complement $g_i|X_i^c = \mathrm{id} = f_i|X_i^c$, and hence $f_i = g_i$. □

14.17. **Definition.** The **signature** $\epsilon(f)$ of a permutation $f \in S_n$ is defined as

$$\epsilon(f) = (-1)^s, \tag{14.18}$$

where s is the minimal number of transpositions $f_1, \dots, f_s$ such that $f = f_1 \cdots f_s$.

The following theorem shows that in fact formula (14.18) is valid even if $f = f_1 \cdots f_s$ is a not a minimal factorisation, and furthermore provides an explicit formula for $\epsilon(s)$.

14.18. **Theorem.** For $n \geq 2$, the map

$$\epsilon : S_n \to \{-1, 1\}, \qquad f \mapsto \epsilon(f), \tag{14.19}$$

is a homomorphism from S_n to the multiplicative group $\{-1, 1\}$. Furthermore

(1) $\epsilon(f) = (-1)^s$ if f is a product of s transpositions;
(2) $\epsilon(f) = \prod_{1 \leq i < j \leq n} \frac{f(i)-f(j)}{i-j}$.

Proof. Let us take (2) as the definition of ϵ and then show the remaining statements, including (14.18). For $f, g \in S_n$ we have

$$\begin{aligned}
\epsilon(fg) &= \prod_{1 \leq i < j \leq n} \frac{f(g(i)) - f(g(j))}{i-j} \\
&= \prod_{1 \leq i < j \leq n} \frac{f(g(i)) - f(g(j))}{g(i) - g(j)} \prod_{1 \leq i < j \leq n} \frac{g(i) - g(j)}{i-j} \\
&= \prod_{1 \leq g^{-1}(i) < g^{-1}(j) \leq n} \frac{f(i) - f(j)}{i-j} \prod_{1 \leq i < j \leq n} \frac{g(i) - g(j)}{i-j} \\
&= \prod_{1 \leq i < j \leq n} \frac{f(i) - f(j)}{i-j} \prod_{1 \leq i < j \leq n} \frac{g(i) - g(j)}{i-j} \\
&= \epsilon(f)\epsilon(g).
\end{aligned} \tag{14.20}$$

The equality before last follows from the fact that $\frac{f(i)-f(j)}{i-j}$ is invariant under the exchange of i and j.

To prove (1) (and thus in particular the original definition (14.18)) let (i, j) be a transposition. By Theorem 14.9 (7) $(i, j) = (g(1), g(2)) = g(1, 2)g^{-1}$ for any g such that $g(1) = i$, $g(2) = j$. Because of (14.20), $\epsilon((i, j)) = \epsilon(g)\epsilon((1, 2))\epsilon(g)^{-1} = \epsilon((1, 2))$. Finally

$$\begin{aligned}
\epsilon((1,2)) &= \prod_{1 < j \leq n} \frac{f(1) - f(j)}{1-j} \prod_{2 < j \leq n} \frac{f(2) - f(j)}{2-j} \prod_{3 \leq i < j \leq n} \frac{f(i) - f(j)}{i-j} \\
&= \frac{2-1}{1-2} \prod_{2 < j \leq n} \frac{2-j}{1-j} \prod_{2 < j \leq n} \frac{1-j}{2-j} \prod_{3 \leq i < j \leq n} \frac{i-j}{i-j} \\
&= -1.
\end{aligned} \tag{14.21}$$

Hence if $f = f_1 \cdots f_s$ with transpositions f_i, we have $\epsilon(f) = \epsilon(f_1) \cdots \epsilon(f_s) = (-1)^s$. $\square$

14.19. Note that the definition of ϵ is in fact independent of n. For $f \in S_{n-1} \leq S_n$ (so $f(n) = n$) we have

$$\begin{aligned} \epsilon(f) &= \prod_{1\leq i<j\leq n} \frac{f(i)-f(j)}{i-j} \\ &= \prod_{1\leq i<j\leq n-1} \frac{f(i)-f(j)}{i-j} \prod_{1\leq i<n} \frac{f(i)-f(n)}{i-n} \\ &= \prod_{1\leq i<j\leq n-1} \frac{f(i)-f(j)}{i-j}, \end{aligned} \tag{14.22}$$

since

$$\prod_{1\leq i<n} \frac{f(i)-f(n)}{i-n} = \prod_{1\leq i<n} \frac{f(i)-n}{i-n} = \frac{\prod_{i=1}^{n-1}(f(i)-n)}{\prod_{i=1}^{n-1}(i-n)} = \frac{\prod_{i=1}^{n-1}(i-n)}{\prod_{i=1}^{n-1}(i-n)} = 1. \tag{14.23}$$

By induction, we can apply this to $f \in S_2 \leq S_n$. In particular, for $f = (1,2)$

$$\epsilon(f) = \frac{f(1)-f(2)}{1-2} = \frac{2-1}{1-2} = -1, \tag{14.24}$$

which short-cuts the calculation (14.21).

14.20. **Corollary.** The number of transpositions that can appear in the factorisation of a given permutation f is always either even or odd.

Proof. $f = f_1 \cdots f_s = g_1 \cdots g_r$ implies $\epsilon(f) = (-1)^s = (-1)^r$. □

14.21. **Definition.** A permutation is called **even** if $\epsilon(f) = 1$, and **odd** if $\epsilon(f) = -1$.

14.22. **Example.**

(1) The identity is even since $(1) = (i,j)(j,i)$.
(2) All transpositions are odd.
(3) 3-cycles are even, since $(i,j,k) = (i,j)(j,k)$.
(4) Theorem 14.9 shows that an r-cycle is even or odd, if r is odd or even, respectively.

14.23. Consider the set of even permutations, $A_n \subseteq S_n$. For $n \geq 2$

$$f \in A_n \Leftrightarrow \epsilon(f) = 1 \Leftrightarrow f \in \ker \epsilon \tag{14.25}$$

and hence $A_n = \ker \epsilon$. So A_n is a normal subgroup of S_n, called the **alternating group** of degree n.

14.24. **Example.** $A_1 = A_2 = \{(1)\}$, $A_3 = \{(1), (1,2,3), (1,3,2)\}$.

14.25. **Theorem.** For $n \geq 2$, $|A_n| = \frac{1}{2}n!$.

Proof. The Homomorphism Theorem shows $S_n/A_n \simeq \{-1, 1\}$ and so $2 = |\{-1,1\}| = |S_n/A_n| = |S_n|/|A_n| = n!/2$. □

14.26. Since A_n is the group of even permutations, every element in A_n can be represented as an even product of transpositions (assume $n \geq 3$). Hence

$$A_n = \langle \{(i,j)(k,l) : 1 \leq i < j \leq n,\ 1 \leq k < l \leq n\}. \tag{14.26}$$

The following is more useful.

14.27. **Theorem.** For $n \geq 3$, A_n is generated by 3-cycles.

Proof. We have seen that 3-cycles are even and thus in A_n. Because of (14.26) is suffices to show that every product of two transpositions can be written as a product of 3-cycles. We distinguish three cases (recall $(i,j) = (j,i)$):

(1) i, j, k, l distinct: $(i,j)(k,l) = (i,j)(j,k)(j,k)(k,l) = (i,j,k)(j,k,l)$.
(2) $i \neq l$, $j = k$: $(i,j)(j,l) = (i,j,l)$.
(3) $i = l$, $j = k$: $(i,j)(j,i) = (1)$.

□

14.28. **Lemma.** If $n \geq 5$, then all 3-cycles are pairwise conjugate in A_n.

Proof. Since conjugacy is an equivalence relation, it is sufficient to show that any cycle (i,j,k) is conjugate to $(1,2,3)$. Since $n \geq 5$ there are integers $l, m \leq n$ so that i, j, k, l, m are distinct. Then one of

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \cdots & n \\ i & j & k & l & m & 6 & \cdots & n \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \cdots & n \\ i & j & k & m & l & 6 & \cdots & n \end{pmatrix} \tag{14.27}$$

is in A_n, since f and g differ by a transposition. By Theorem 14.9 (7)

$$f(1,2,3)f^{-1} = (i,j,k), \qquad g(1,2,3)g^{-1} = (i,j,k), \tag{14.28}$$

and so (i,j,k) is conjugate to $(1,2,3)$ in A_n. □

14.29. **Definition.** A group G is called simple if $G \neq \{e\}$ and $\{e\}$ and G are the only normal subgroups.

14.30. **Theorem.** (Jordan) A_n is simple if and only if $n \neq 1, 2, 4$.

Proof. The statement is obvious for $n = 1, 2, 3$.

A_4 is not simple since

$$\{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \tag{14.29}$$

forms a normal subgroup. (Exercise.) Assume $n \geq 5$ in the following.

Let $N \neq \{e\}$ be a normal subgroup of A_n. We will show below that N contains a 3-cycle g. Then, since N is assumed normal, $fgf^{-1} \in N$ for all $f \in A_n$. By Lemma 14.28, every 3-cycle can be represented in this way and hence N contains every 3-cycle. But this implies $N = A_n$ in view of Theorem 14.27.

To prove that N contains a 3-cycle g, let $a \in N$, and $a = a_1 \cdots a_t$ a canonical factorisation into disjoint cycles.

Case 1: Suppose the canonical factorisation contains one r-cycle with $r \geq 4$. Since a_i commute, we may assume that this is the first cycle $a_1 = (i_1, i_2, i_3, \ldots, i_r)$. Since N is normal, we have for $b = (i_1, i_2, i_3) \in A_n$ that the following element is in N:

$$\begin{aligned} N \ni a(ba^{-1}b^{-1}) &= (aba^{-1})b^{-1} \\ &= (a_1 b a_1^{-1})b^{-1} \\ &= [(i_1, i_2, i_3, \ldots, i_r)(i_1, i_2, i_3)(i_1, i_2, i_3, \ldots, i_r)^{-1}](i_3, i_2, i_1) \\ &= (i_2, i_3, i_4)(i_3, i_2, i_1) \quad \text{(Theorem 14.9 (7))} \\ &= (i_4, i_2, i_3)(i_3, i_2, i_1) \\ &= (i_4, i_2, i_1). \end{aligned} \tag{14.30}$$

This yields the desired 3-cycle.

Case 2: Suppose the canonical factorisation of a contains only transpositions and exactly one 3-cycle, i.e., $a = (i_1, i_2, i_3)(i_4, i_5)a_3 \cdots a_r$. For $b = (i_1, i_2, i_4) \in A_n$

$$\begin{aligned} N \ni a(ba^{-1}b^{-1}) &= \left[[(i_1, i_2, i_3)(i_4, i_5)](i_1, i_2, i_4)[(i_1, i_2, i_3)(i_4, i_5)]^{-1}\right](i_4, i_2, i_1) \\ &= (i_2, i_3, i_5)(i_4, i_2, i_1) \\ &= (i_3, i_5, i_2)(i_2, i_1, i_4) \\ &= (i_3, i_5, i_2, i_1, i_4) \end{aligned} \tag{14.31}$$

which is a 5-cycle, so we have reduced the problem to Case 1.

Case 3. Suppose the canonical factorisation of a contains more than one 3-cycle, i.e., $a = (i_1, i_2, i_3)(i_4, i_5, i_6)a_3 \cdots a_r$. For $b = (i_1, i_2, i_4) \in A_n$

(14.32)

$$\begin{aligned} N \ni a(ba^{-1}b^{-1}) &= \left[[(i_1, i_2, i_3)(i_4, i_5, i_6)](i_1, i_2, i_4)[(i_1, i_2, i_3)(i_4, i_5, i_6)]^{-1}\right](i_4, i_2, i_1) \\ &= (i_2, i_3, i_5)(i_4, i_2, i_1) \end{aligned}$$

and we conclude as in Case 2.

Case 4: Suppose the canonical factorisation of a contains only transpositions, $a = (i_1, i_2)(i_3, i_4)a_3 \cdots a_r$. Choose $i_5 \neq i_1, i_2, i_3, i_4$, and let $b = (i_1, i_3, i_5)$.

$$\begin{aligned} N \ni a(ba^{-1}b^{-1}) &= [a(i_1, i_3, i_5)a^{-1}](i_5, i_3, i_1) \\ &= (i_2, i_4, a(i_5))(i_5, i_3, i_1). \end{aligned} \tag{14.33}$$

If $a(i_5) = i_5$ then we obtain a 5-cycle and hence Case 1, if $a(i_5) \neq i_5$ it follows $(i_2, i_4, a(i_5)) = (a(i_1), a(i_3), a(i_5))$ and (i_5, i_3, i_1) are disjoint (since a is bijective), which yields Case 3. □

14.31. **Exercise.** Write

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 1 & 3 & 5 & 7 & 9 & 11 & 13 \end{pmatrix} \tag{14.34}$$

(1) as a product of disjoint cycles,

(2) as a product of transpositions.

14.32. **Exercise.** Calculate the conjugates $\pi\sigma\pi^{-1}$ for

(1) $\pi = (1,2)$, $\sigma = (2,3)(1,4)$;
(2) $\pi = (2,3)(3,4)$, $\sigma = (1,2,3)$;
(3) $\pi = (1,3)(2,4,1)$, $\sigma = (1,2,3,4,5)$;
(4) $\pi = (1,2,3)$, $\sigma = (1,2,3,4,5)$.

14.33. **Exercise.** Let $r \geq 1$. Show that in S_n all r-cycles are conjugate.

14.34. **Exercise.** Show that S_n is generated by $\{(1,2),(1,3),\ldots,(1,n)\}$.

15. THE JORDAN-HÖLDER THEOREM

15.1. **Definition.** A nested sequence of groups $\{G_i\}_{i\in\mathbb{N}}$

$$G = G_1 \geq G_2 \geq G_3 \geq \dots \tag{15.1}$$

is called a **descending chain** of G. The chain is **finite**, if there is i_0 such that $G_{i+1} = G_i$ for all $i \geq i_0$.

A descending chain is called a **normal chain**, if $G_{i+1} \trianglelefteq G_i$ for all $i \in \mathbb{N}$, and G_i/G_{i+i} are called the **factors** of the normal chain. (Note: G_i is not necessarily normal in G, which is why one often finds the notion of a subnormal chain in the literature.)

A normal chain is called a **cyclic chain** or **abelian chain**, if all factors are cyclic or abelian, respectively.

A finite normal chain

$$G = G_1 \geq G_2 \geq \dots \geq G_m = N \tag{15.2}$$

is called a **normal series** from G to N, if $N \trianglelefteq G$. (Again, the notion of subnormal series is often used in the literature instead.) If $N = \{e\}$ and $G_i \neq G_{i+1}$, the normal series is said to have **length** $m-1$.

Two normal series

$$G_1 \geq G_2 \geq \dots \geq G_m, \qquad H_1 \geq H_2 \geq \dots \geq H_n, \tag{15.3}$$

are called **equivalent** if $m = n$ and if there is a permutation $i \mapsto \pi(i)$ such that $G_i/G_{i+1} \simeq H_{\pi(i)}/H_{\pi(i)+1}$.

15.2. **Example.** $\mathbb{Z} > p\mathbb{Z} > p^2\mathbb{Z} > \dots$ is an infinite normal chain. Since $p^i\mathbb{Z}/p^{i+1}\mathbb{Z} \simeq \mathbb{Z}_p$ (Example 8.3) the chain is abelian.

15.3. **Theorem.** Let $N \trianglelefteq G$. A normal series from G to N is equivalent to a normal series of G/N to $E = \{e\}$.

Proof. Let $G = G_1 \geq G_2 \geq \dots \geq G_m = N$ be the normal series from G to N, then $N \trianglelefteq G_i$ $(1 \leq i \leq m)$. The second isomorphism theorem states that $G_{i+1}/N \trianglelefteq G_i/N$ and

$$(G_i/N)/(G_{i+1}/N) \simeq G_i/G_{i+1}. \tag{15.4}$$

Hence the normal series under consideration is equivalent to $G/N = G_1/N \geq G_2/N \geq G_3/N \geq \dots \geq G_m/N = E$. □

15.4. **Definition.** The normal series $G_1 \geq G_2 \geq \dots \geq G_m$ is called a **refinement** of the normal series $G_1 = H_1 \geq H_2 \geq \dots \geq H_k$ if

$$\{H_1, H_2, \dots, H_k\} \subseteq \{G_1, G_2, \dots, G_m\}. \tag{15.5}$$

15.5. **Third Isomorphism Theorem (Zassenhaus Lemma).** Let $A_1 \trianglelefteq A \leq G$, $B_1 \trianglelefteq B \leq G$. Then:

(1) $A_1(A \cap B_1) \trianglelefteq A_1(A \cap B)$.
(2) $B_1(A_1 \cap B) \trianglelefteq B_1(A \cap B)$.
(3) $A_1(A \cap B)/A_1(A \cap B_1) \simeq B_1(A \cap B)/B_1(A_1 \cap B)$.

Proof. Claim (3) follows directly from

$$A_1(A \cap B)/A_1(A \cap B_1) \simeq (A \cap B)/(A \cap B_1)(A_1 \cap B) \tag{15.6}$$

since the right hand side is invariant under $A \leftrightarrow B$, $A_1 \leftrightarrow B_1$.

To prove (1) and (15.6) set $H = A \cap B$, $K = A \cap B_1$, $L = A_1 \cap B$. Then (15.6) becomes

$$A_1H/A_1K \simeq H/KL. \tag{15.7}$$

We will construct an epimorphism

$$\varphi : A_1H/A_1 \to H/KL \tag{15.8}$$

with kernel $\ker \varphi = A_1K/A_1$. The homomorphism theorem then yields

$$(A_1H/A_1)/(A_1K/A_1) \simeq H/KL \tag{15.9}$$

and since the kernel A_1K/A_1 is normal, we have $KA_1 = A_1K$ is normal in A_1H (Theorem 8.10 (3)). This proves (1) and thus (2).

To construct φ, note that $H \leq A$ and $A_1 \trianglelefteq A$ implies $A_1H = HA_1$ and thus $A_1 \trianglelefteq A_1H \leq A$. The First Isomorphism Theorem shows that

$$\psi_1 : A_1H/A_1 \to H/A_1 \cap H = H/L, \qquad hA_1 \mapsto hL, \tag{15.10}$$

is an isomorphism. Since $K, L \trianglelefteq H$ we have $KL = LK \trianglelefteq H$. The Second Isomorphism Theorem (and its proof) shows

$$\psi_2 : H/L \to H/KL, \qquad hL \mapsto hKL, \tag{15.11}$$

is an epimorphism with $\ker \psi_2 = KL/L$. Set

$$\varphi = \psi_2 \circ \psi_1 : A_1H/A_1 \to H/KL. \tag{15.12}$$

This is precisely the epimorphism needed, since $hA_1 \in \ker \varphi$ if and only if $\psi_1(hA_1) = hL \in \ker \psi_2 = KL/L$. This is the case if and only if $h \in K$, i.e.,

$$\ker \varphi = \{hA_1 : h \in K\} = KA_1/A_1. \tag{15.13}$$

□

15.6. **Schreier's Theorem.** Any two normal series of a group G possess equivalent refinements.

Proof. Let

$$G = G_1 \geq G_2 \geq \ldots \geq G_m = E, \qquad G = H_1 \geq H_2 \geq \ldots \geq H_n = E \tag{15.14}$$

be two normal series of G. For $1 \leq i \leq m-1$ and $1 \leq j \leq n$ set

$$G_{i,j} := G_{i+1}(G_i \cap H_j). \tag{15.15}$$

Note that $G_{i,1} = G_i$, $G_{i,n} = G_{i+1}$. The Zassenhaus lemma (1) shows $G_{i,j+1} \trianglelefteq G_{i,j}$. We thus obtain a refinement of the normal series,

$$G = G_{1,1} \geq G_{1,2} \geq \ldots \geq G_{1,n} = G_{2,1} \geq G_{2,2} \geq \ldots \geq G_{m-1,n} = G_m = E \tag{15.16}$$

which has length $(m-1)(n-1)$.

For $1 \leq j \leq n-1$ and $1 \leq i \leq m$ we make the analogous construction for H_j,

$$H_{j,i} := H_{j+1}(G_i \cap H_j), \tag{15.17}$$

which leads to the refinement

$$G = H_{1,1} \geq H_{1,2} \geq \ldots \geq H_{1,m} = H_{2,1} \geq H_{2,2} \geq \ldots \geq H_{n-1,m} = H_n = E, \tag{15.18}$$

again of length $(m-1)(n-1)$. The Zassenhaus lemma, applied with $A = G_i$, $B = H_j$, $A_1 = G_{i+1}$, $B_1 = H_{j+1}$, proves the isomorphism $G_{i,j}/G_{i,j+1} \simeq H_{j,i}/H_{j,i+1}$. □

15.7. **Example.** $\mathbb{Z} > 2\mathbb{Z} > 10\mathbb{Z} > 30\mathbb{Z} > \{0\}$ and $\mathbb{Z} > 3\mathbb{Z} > 24\mathbb{Z} > \{0\}$ are normal series of $\mathbb{Z}$. The refinements gained from the procedure in the above proof are here (ignore repetitions)

$$\mathbb{Z} > 2\mathbb{Z} > 10\mathbb{Z} > 30\mathbb{Z} > 120\mathbb{Z} > \{0\} \qquad \text{(with factors } \mathbb{Z}_2, \mathbb{Z}_5, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}\text{)} \tag{15.19}$$

$$\mathbb{Z} > 3\mathbb{Z} > 6\mathbb{Z} > 24\mathbb{Z} > 120\mathbb{Z} > \{0\} \qquad \text{(with factors } \mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}\text{)}. \tag{15.20}$$

15.8. **Exercise.** As in Example 15.7, work out the equivalent refinements of the normal series

$$\mathbb{Z} > 15\mathbb{Z} > 60\mathbb{Z} > \{0\}, \qquad \mathbb{Z} > 12\mathbb{Z} > \{0\}, \tag{15.21}$$

and write down the corresponding factors.

15.9. **Definition.** $N \trianglelefteq G$ is called **maximal**, if $N \neq G$ and if $N \leq M \trianglelefteq G$ implies $M = N$ or $M = G$.

15.10. **Lemma.** $N \trianglelefteq G$ is maximal if and only if G/N is simple.

Proof. $N \neq G$ is equivalent to $G/N \neq E$. The rest of the statement follows from Theorem 8.10 (3). □

15.11. **Definition.** A normal series $G = G_1 \geq G_2 \geq \ldots \geq G_m = E$ is called a **composition series** of G, if $G_{i+1} \trianglelefteq G_i$ is maximal for all $1 \leq i < m$ (or, equivalently, if the quotients G_i/G_{i+1} are simple). The quotient groups (or factor groups) of a composition series are called **composition factors**.

15.12. Note that every finite group possesses a composition series, since the process of refining the series $G \geq \{e\}$ must terminate after finitely many steps. On the other hand, the infinite group $(\mathbb{Z}, +)$ is an example of a group that does not possess a composition series.

15.13. **Example.**

(1) Consider the inner direct product $G = N_1 N_2 \cdots N_k$ of simple normal subgroups N_i. Then $G = N_1 N_1 N_2 \cdots N_k > N_2 \cdots N_k > N_3 \cdots N_k > \ldots > N_k > E$ is a composition series with factors $N_1, N_2, \ldots, N_k$.

(2) $\mathbb{Z}_{24} > \mathbb{Z}_8 > \mathbb{Z}_4 > \mathbb{Z}_2 > \{0\}$, $\mathbb{Z}_{24} > \mathbb{Z}_{12} > \mathbb{Z}_4 > \mathbb{Z}_2 > \{0\}$, $\mathbb{Z}_{24} > \mathbb{Z}_{12} > \mathbb{Z}_6 > \mathbb{Z}_2 > \{0\}$ are composition series since its factors have prime order.

(3) $\mathbb{Z}_4 > \mathbb{Z}_2 > \{0\}$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 > \mathbb{Z}_2 > \{0\}$ have the same factors, $\mathbb{Z}_2$. This illustrates that non-isomorphic groups can have equivalent composition series.

15.14. **The Jordan-Hölder Theorem.** If a group possesses composition series, then any two composition series are equivalent.

Proof. Let

$$G = G_1 \geq G_2 \geq \ldots \geq G_m = E, \qquad G = H_1 \geq H_2 \geq \ldots \geq H_n = E \tag{15.22}$$

be two composition series of G. These are by definition without repetition. If we refine them via Schreier's Theorem to equivalent normal series, then we must introduce repetitions (since there are no normal subgroups inbetween G_i and G_{i+1}, and inbetween H_i and H_{i+1}). If we delete repetitions, the series remain equivalent—and we are back to our original composition series (15.22). □

15.15. **Exercise.** Show that every abelian group with a composition series is finite.

15.16. **Exercise.** Write down all possible composition series of $\mathbb{Z}_{24}$ with corresponding factors.

16. SOLUBLE GROUPS

16.1. In Section 13 we have given a complete classification of all finitely generated abelian groups. Soluble groups (to be defined below) may be viewed the simplest non-abelian generalization, and allow a similar analysis as for the abelian case. The following defines a measure of the "degree of commutativity" of a group:

16.2. **Definition.** Let G be a group. For $a, b \in G$ the product

$$[a, b] := aba^{-1}b^{-1} \tag{16.1}$$

is called the **commutator** of a and b. The group

$$K(G) := \langle\{[a, b] : a, b \in G\}\rangle \tag{16.2}$$

is called the **commutator group** of G.

16.3. Since $[a, b]^{-1} = [b, a]$, $K(G)$ comprises all finite products of commutators. Note however that a product of commutators is not necessarily a commutator! It is evident that $[a, b] = e$ if and only if a, b commute. Hence G is abelian if and only if $K(G) = \{e\}$, and the larger $K(G)$, the higher the degree of non-commutativity in G.

16.4. **Theorem.** $K(G) \trianglelefteq G$.

Proof. For every homomorphism φ of G we have

$$\varphi([a, b]) = \varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a^{-1})\varphi(b^{-1}) = [\varphi(a), \varphi(b)]. \tag{16.3}$$

Hence for the inner automorphism $\varphi_x : G \to G$, $g \mapsto xgx^{-1}$, we have $x[a, b]x^{-1} = \varphi_x([a, b]) = [\varphi_x(a), \varphi_x(b)] \in G$ for every $x \in G$. Thus if $h = [a_1, b_1] \cdots [a_r, b_r] \in K(G)$ is a product of commutators, then so is

$$xhx^{-1} = \varphi_x(h) = [\varphi_x(a_1), \varphi_x(b_1)] \cdots [\varphi_x(a_r), \varphi_x(b_r)]. \tag{16.4}$$

This proves $xhx^{-1} \in K(G)$ for all $h \in K(G)$, $x \in G$. □

16.5. **Theorem.** Let $N \trianglelefteq G$. Then G/N is abelian if and only if $K(G) \leq N$.

Proof. G/N is abelian if and only if $abN = aNbN = bNaN = baN$ for all $a, b \in G$. This is equivalent to $a^{-1}b^{-1}abN = N$ for all $a, b \in G$, i.e., $[a^{-1}, b^{-1}] \in N$ for all $a, b \in G$. But this is the same as saying $[a, b] \in N$ for all $a, b \in G$, i.e., $K(G) \subseteq N$ (since N is closed under multiplication). □

16.6. **Corollary.** $G/K(G)$ is abelian.

16.7. **Example.** $K(S_3) = A_3$, $K(A_3) = \{(1)\}$, $K(A_4) = V_4$, $K(V_4) = \{(1)\}$.

16.8. **Theorem.**

(1) $K(S_n) = A_n$ if $n \geq 2$.

(2) $K(A_n) = A_n$ if $n \geq 5$.

Proof. (1) S_2 is abelian and $A_2 = \{(1)\}$, so the case $n = 2$ is proved. Assume $n \geq 3$. We have for 3-cycles

(16.5)

$$(i,j,k) = (i,k,j)^2 = (i,k)(k,j)(i,k)(k,j) = (i,k)(k,j)(i,k)^{-1}(k,j)^{-1} = [(i,k),(k,j)]$$

and so all 3-cycles are in $K(S_n)$. Since the 3-cycles generate A_n (Theorem 14.27), we have $A_n \leq K(S_n)$. But since $S_n/A_n \simeq \{1,-1\}$ is abelian (cf. 14.23), and, by Theorem 16.5, this implies $K(S_n) \leq A_n$.

(2) This follows directly from Theorem 14.30. We give a more elementary proof:

If (i,j,k) is a 3-cycle as above, and $l,m \in \mathbb{N} \setminus \{i,j,k\}$ (these exist since $n \geq 5$) we have (as above)

$$(i,j,k) = (i,k,j)^2 = [(i,k),(k,j)] = [(i,k)(l,m),(l,m)(k,j)] \tag{16.6}$$

since (l,m) commutes with (i,k) and (k,j). This shows (again by Theorem 14.27) $A_n \leq K(A_n)$, and thus $A_n = K(A_n)$. □

16.9. **Definition.** The n**th commutator group** of G is defined inductively by

$$K_n(G) := K(K_{n-1}(G)), \qquad K_0(G) := G. \tag{16.7}$$

16.10. **Example.** $K_3(S_4) = K(K(K(S_4))) = K(K(A_4)) = K(V_4) = \{(1)\}$.

16.11. **Theorem.** Let G, G' be groups, and $H \leq G$, $N \trianglelefteq G$. Then, for all $n \geq 0$,

(1) $K_n(H) \leq K_n(G)$,

(2) $K_n(G/N) = K_n(G)N/N \simeq K_n(G)/(K_n(G) \cap N)$,

(3) $K_n(G \times G') = K_n(G) \times K_n(G')$.

Proof (by induction). (1) is evident.

(2) $n = 0$ is trivial, since $K_0(G) = G$.

$$\begin{aligned}
K_{n+1}(G/N) &= K\big(K_n(G/N)\big) && \text{(by definition)}\\
&= K\big(K_n(G)N/N)\big) && \text{(by induction hypothesis)}\\
&= \big\langle\{\bar{k}_1\bar{k}_2\bar{k}_1^{-1}\bar{k}_2^{-1} : \bar{k}_1, \bar{k}_2 \in K_n(G)N/N\}\big\rangle && \text{(by definition)}\\
&= \big\langle\{k_1Nk_2Nk_1^{-1}Nk_2^{-1}N : k_1, k_2 \in K_n(G)\}\big\rangle && (16.8)\\
&= \big\langle\{[k_1,k_2]N : k_1, k_2 \in K_n(G)\}\big\rangle && \text{(since } N \text{ is normal)}\\
&= \big\langle\{[k_1,k_2] : k_1, k_2 \in K_n(G)\}\big\rangle N/N\\
&= K_{n+1}(G)N/N && \text{(by definition).}
\end{aligned}$$

The isomorphism in (2) follows from the first isomorphism theorem.

(3) is left as an exercise. □

16.12. **Exercise.** Prove Theorem 16.11 (3).

16.13. **Definition.** A group G is called **soluble** if $K_m(G) = \{e\}$ for some $m \in \mathbb{N}$.

16.14. Note that every abelian group is soluble, since $K(G) = \{e\}$. Hence soluble groups may be viewed as a natural generalization of abelian groups. An example of a non-abelian group that is soluble is S_4; recall 16.10.

16.15. **Theorem.** If $n \geq 5$, then S_n is not soluble.

Proof. By Theorem 16.8, $K(S_n) = A_n$ and $K_m(S_n) = K_{m-1}(A_n) = A_n$ for all $m \geq 2$. So $K_m(S_n) \neq \{e\}$ for all $m \geq 0$. □

16.16. **Theorem.**

(1) Every subgroup of a soluble group is soluble.
(2) Every quotient group of a soluble group is soluble.
(3) Every finite direct product of soluble groups is soluble.

Proof. Note that $K_m(G) = \{e\}$ implies via Theorem 16.11 that $K_m(H) = \{e\}$ for every $H \leq G$ and $K_m(G/N) = \{e\}$ for every $N \trianglelefteq G$. □

16.17. **Theorem.** Let $N \trianglelefteq G$ such that N and G/N are soluble, then G is soluble.

Proof. Since G/N is soluble there is $m \in \mathbb{N}$ such that $K_m(G/N) = \{N\}$. From Theorem 16.11 (2), $K_m(G)N = N$, i.e., $K_m(G) \leq N$. Since N is soluble, $K_l(N) = \{e\}$ for some $l \in \mathbb{N}$. Now $K_{l+m}(G) = K_l(K_m(G)) \leq K_l(N)$ (by Theorem 16.11 (1)) $= \{e\}$. So $K_{l+m}(G) = \{e\}$ and G is soluble. □

16.18. If G is a soluble group with $K_m(G) = \{e\}$, then the series

$$G = K_0(G) \geq K_1(G) \geq \ldots \geq K_m(G) = \{e\} \tag{16.9}$$

is an abelian normal series, since $K_{i+1}(G) = K(K_i(G)) \trianglelefteq K_i(G)$ (Theorem 16.4) and $K_i(G)/K_{i+1}(G)$ are abelian groups (Corollary 16.6). We have in fact:

16.19. **Theorem.** A group is soluble, if and only if it possesses an abelian normal series.

Proof. We have already seen that the series of commutator groups (16.9) yields the required abelian normal series. For the inverse direction, we use induction on the length of the series.

Length 1: If $G = G_1 \geq G_2 = \{e\}$ is an abelian normal series, then $G \simeq G/\{e\} = G_1/G_2$ is abelian (by definition), so G is abelian and hence soluble.

Length $< n$: The induction hypothesis is that all groups with abelian normal series of length $< n$ are soluble. Let

$$G = G_1 \geq G_2 \geq \ldots \geq G_{n+1} = \{e\} \tag{16.10}$$

be an abelian normal series of length n. Then

$$G_2 \geq G_3 \geq \ldots \geq G_{n+1} = \{e\} \tag{16.11}$$

is an abelian normal series of length $n-1$, so by the induction hypothesis G_2 is soluble. We have assumed that the series (16.10) is abelian normal, so $G_2 \trianglelefteq G$ with G/G_2 abelian (and hence soluble). In view of Theorem 16.17, this means G is soluble. □

16.20. **Lemma.** Every refinement of an abelian normal series is an abelian normal series.

Proof. Let

$$G = G_1 \geq G_2 \geq \ldots \geq G_r = \{e\} \tag{16.12}$$

be an abelian normal series. Consider the (one-step) refinement

$$G = G_1 \geq G_2 \geq \ldots \geq G_i \geq H \geq G_{i+1} \geq \ldots \geq G_r = \{e\}. \tag{16.13}$$

Then H/G_{i+1} is abelian since it is a subgroup of the abelian group G_i/G_{i+1}. By the second isomorphism theorem G_i/H is isomorphic to $(G_i/G_{i+1})/(H/G_{i+1})$ which is abelian, and therefore G_i/H is abelian. A general refinement of (16.12) is obtained by iterating the above process finitely many times. □

16.21. **Theorem.** Let G be a group with composition series. G is soluble, if and only if the composition factors of G have prime order.

Proof. If G is soluble, then Theorem 16.19 guarantees the existence of an abelian normal series. We use Schreier's Theorem to show that the composition series and the abelian normal series can both be refined, so that they become equivalent normal series. These are abelian by Lemma 16.20. But since a refinement of a composition series is only achieved by repetition, the composition series itself is already abelian. Hence the composition factors are simple abelian groups, and are therefore cyclic and have prime order. □

16.22. **Corollary.** A soluble group G possesses a composition series, if and only if G is finite.

Proof. We have already noted in 15.12 that every finite group has a composition series. If on the other hand G possesses the composition series

$$G = G_1 \geq G_2 \geq \ldots \geq G_m = \{e\}, \tag{16.14}$$

then, by Theorem 16.21 we have $|G_i| = |G_i/G_{i+1}||G_{i+1}| = p_i|G_{i+1}|$ for some prime p_i $(1 \leq i < m)$. Hence $|G| = p_1|G_2| = p_1p_2|G_3| = \ldots = p_1p_2\cdots p_{m-1} < \infty$. □

16.23. **Theorem.** Every finite p-group (p prime) is soluble.

Proof. A finite p-group has order p^n for some $n \geq 0$. The case $n = 0$ is trivial. We proceed by induction on n. The induction hypothesis is that for any $m < n$, every finite group of order p^m is soluble. For $n \geq 1$, Theorem 10.19 says the center $Z(G)$ is nontrivial, i.e., $|Z(G)| = p^r$, $r \geq 1$. Since $|G/Z(G)| = p^{n-r}$ and $n - r < n$, the induction hypothesis shows $G/Z(G)$ is soluble. $Z(G)$ is abelian and thus also soluble. Therefore G is soluble (by Theorem 16.17). □

A famous theorem whose proof goes far beyond the scope of this course is:

16.24. **Feit-Thomson Theorem (1963).** Every finite group of odd order is soluble.

16.25. **Exercise.** Show that for any $m \in \mathbb{N}$

$$G_m := \{g \in G : g^m \in K(G)\} \tag{16.15}$$

is a subgroup of G.

16.26. **Exercise.** For $H, K \leq G$ define $[H, K] = \langle\{[h, k] : h \in H, k \in K\}\rangle$. Show that $N \leq G$ is normal if and only if $[G, N] \subseteq N$.

17. SOLUTIONS TO EXERCISES

Exercise 1.4.

(1) Note that if $a'a = e$ (as in the inverse axiom) then $(aa')(aa') = a(a'a)a' = aa'$, and by Lemma 1.3 $aa' = e$.
(2) We have $a = ea$ (identity axiom) $= aa'a$ (as shown in (1)) $= ae$ (inverse axiom).
(3) Suppose there are two identities, $e, \tilde{e}$. Then $ea = ae = a = \tilde{e}a = a\tilde{e}$ for all $a \in G$ (by the identity axiom and (2)). In particular for $a = e$: $e = \tilde{e}e$, and for $a = \tilde{e}$: $\tilde{e}e = \tilde{e}$. Hence $\tilde{e} = e$.
(4) Suppose there are two inverses $a', \tilde{a}'$ of a, i.e., $a'a = \tilde{a}'a = e$. This implies $a'aa' = \tilde{a}'aa' \Rightarrow a'e = \tilde{a}'e$ (by (3)) $\Rightarrow a' = \tilde{a}'$.
(5) By definition, $(a^{-1})^{-1}a^{-1} = e \Rightarrow (a^{-1})^{-1}a^{-1}a = ea \Rightarrow (a^{-1})^{-1}e = a \Rightarrow (a^{-1})^{-1} = a$.
(6) By definition, $(ab)^{-1}(ab) = e \Rightarrow (ab)^{-1}(ab)b^{-1} = eb^{-1} \Rightarrow (ab)^{-1}a = b^{-1} \Rightarrow (ab)^{-1}aa^{-1} = b^{-1}a^{-1} \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$.

Exercise 1.9. Associativity is a well known property of matrix multiplication. The rest follows from straightforward calculations.

Exercise 1.14. Tedious but straightforward.

Exercise 1.15. The symmetries of an n-gon are reflections $\sigma_0, \ldots, \sigma_{n-1}$ at the n diagonals (which are lines through the origin that meet the horizontal axis at angles $\pi m/n$, $m = 0, \ldots, n-1 \bmod n$) and rotations ρ_m by an angle $2\pi m/n$, $m = 0, \ldots, n-1 \bmod n$.

Existence of identity and inverse: $m = 0$ corresponds to the identity element. The inverse of a reflection is the reflection itself, $\sigma^{-1} = \sigma$, and the inverse of the rotation by $2\pi m/n$ is $-2\pi m/n$, i.e., $\rho_m^{-1} = \rho_{n-m}$.

Closure under multiplication: The product of two rotations $2\pi m/n$, $2\pi m'/n$ is evidently a rotation by $2\pi(m + m')/n$, i.e., $\rho_m\rho_{m'} = \rho_{m+m'}$. Any reflection σ_m can be written as $\sigma_m = \rho_{m/2}\sigma_0\rho_{m/2}^{-1}$. Note that for any rotation about the origin by and angle α, we have $\rho_\alpha\sigma_0 = \sigma_0\rho_\alpha^{-1}$. This an the previous relation yields $\sigma_m = \rho_m\sigma_0$, and $\sigma_m\sigma_{m'} = \rho_m\sigma_0\rho_{m'}\sigma_0 = \rho_{m-m'}\sigma_0\sigma_0 = \rho_{m-m'}$. Hence the product of two reflections is a rotation. Similarly $\rho_m\sigma_{m'} = \rho_{m+m'}\sigma_0 = \sigma m + m'$ and $\sigma_m\rho_{m'} = \rho_{m-m'}\sigma_0 = \sigma m - m'$, so the product of a reflection and rotation are a reflection.

Exercise 1.16. Assume K is a finite field with q elements. Let $M \in K^{n\times n}$ and consider the system of equations $Mx = 0$ with $x \in K$. We know from linear algebra that $x = 0$ is the unique solution of $Mx = 0$, if and only if $\det M \neq 0$. So if $\det M \neq 0$, the column vectors of M must be linearly independent over K, i.e., form a basis of the vector space K^n. In other words, the order of $GL(n, K)$ is the number of different

bases of K^n. To see how many there are, note that there are $q^n - 1$ choice of the first basis vector (anything but the zero vector), $q^n - q$ (anything but a multiple of the previously chosen vector), $q^n - q^2$ (anything but a linear combination of the previous two), ..., $q^n - q^{n-1}$ (anything but a linear combination of the previous $(n-1)$ choices). Hence the total is

$$\prod_{j=1}^{n}(q^n - q^{j-1}) = \prod_{j=1}^{n} q^{j-1} \prod_{j=1}^{n}(q^{n-j+1} - 1) = q^{n(n-1)/2} \prod_{j=1}^{n}(q^j - 1). \tag{17.1}$$

Exercise 2.3. This follows from a straightforward calculation.

Exercise 2.6. It is easy to see that $\varphi : \mathbb{Z} \to 2\mathbb{Z}, m \mapsto 2m$ defines a homomorphism (since $2(m+n) = 2m+2n$). The inverse map $\varphi : 2\mathbb{Z} \to \mathbb{Z}, m \mapsto m/2$ shows that φ is bijective.

Exercise 2.7.

(1) Clearly none of the maps is surjective, since both miss a good part of T. Since

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \Leftrightarrow \begin{pmatrix} 1 & t-u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Leftrightarrow t = u, \tag{17.2}$$

φ_1 is injective, and hence a monomorphism. The analogous argument shows φ_2 is a monomorphism.

(2) Since $\varphi_3(t) = \varphi_3(t+2\pi)$, the map is not injective. But since for every $x, y \in \mathbb{R}$ with $x^2 + y^2 = 1$ we find a $t \in \mathbb{R}$ such that $x = \cos(t)$, $y = \sin(t)$, the map is surjective. Hence φ_3 is an epimorphism.

Exercise 2.10. Straightforward application of the definitions.

Exercise 2.17. $\varphi_e(a) = eae^{-1} = a$, and so $a \sim a$. $a \sim b$ means there is a g: $\varphi_g(a) = gag^{-1} = b$; now $\varphi_{g^{-1}}(b) = g^{-1}bg = g^{-1}gag^{-1}g = a$, and so $a \sim b$ implies $b \sim a$. If $a \sim b$ and $b \sim c$, then there are g, h: $\varphi_g(a) = gag^{-1} = b$, $\varphi_h(b) = hbh^{-1} = c$; now $\varphi_{hg}(a) = hga(hg)^{-1} = hgag^{-1}h^{-1} = hbh^{-1} = c$, and so $a \sim c$.

Exercise 2.18. This follows from $\varphi_b(ab) = b(ab)b^{-1} = ba$.

Exercise 2.22. Recall that the elements of the Klein four group satisfy $a^2 = b^2 = c^2 = e$ (and hence every element equals its inverse), $ab = ba = c$, $bc = cb = a$, $ca = ac = b$. Besides the trivial automorphism $\varphi_0 = \mathrm{id}$ we find the following:

$$\varphi_1(a) = b, \qquad \varphi_1(b) = a, \qquad \varphi_1(c) = c; \tag{17.3}$$

$$\varphi_2(a) = a, \qquad \varphi_2(b) = c, \qquad \varphi_1(c) = b; \tag{17.4}$$

$$\varphi_3(a) = c, \qquad \varphi_3(b) = b, \qquad \varphi_3(c) = a; \tag{17.5}$$

$$\varphi_4(a) = b, \qquad \varphi_4(b) = c, \qquad \varphi_4(c) = a \tag{17.6}$$

since $\varphi_4(a)\varphi_4(b) = bc = a = \varphi_4(c) = \varphi_4(ab)$, etc.;

$$\varphi_5(a) = c, \qquad \varphi_5(b) = a, \qquad \varphi_5(c) = b. \tag{17.7}$$

Note that $\varphi_i^{-1} = \varphi_i$ $(i = 1, 2, 3)$ and $\varphi_4^{-1} = \varphi_5$. The automorphism group of the Klein four group has thus order 6.

Exercise 2.23. Clear—recall the relations between rotations and reflections discussed in Exercise 1.15.

Exercise 2.24.

(1) Clear.
(2) $\ker \varphi = \{m \in \mathbb{Z} : \zeta^m = 1\} = n\mathbb{Z}$.

Exercise 2.25.

(1) If $\operatorname{Aut} G = \{\mathrm{id}\}$ then $\varphi_g = \mathrm{id}$ for all $g \in G$, and hence $\varphi_g(a) = gag^{-1} = a$, i.e., $ag = ga$ for all $a, g \in G$. (Alternatively, note that $\operatorname{Aut} G = \{\mathrm{id}\}$ implies that $Z(G) := \ker \Phi = G$, which also says that G is abelian.)
(2) If $x \to x^2$ is a homomorphism, then $(ab)^2 = a^2b^2 \Rightarrow abab = aabb \Rightarrow ba = ab$.
(3) If $x \to x^{-1}$ is a homomorphism, then $(ab)^{-1} = a^{-1}b^{-1} \Rightarrow b^{-1}a^{-1} = a^{-1}b^{-1}$. Hence all inverses commute, and so all elements commute.

Exercise 3.13. We need to show $H_1 \cup H_2 = G$ implies $H_1 = G$ or $H_2 = G$. Assuming $H_1 \cup H_2 = G$ and furthermore $H_1 \neq H_1 \cap H_2 \neq H_2$ (i.e., H_1 is not contained in H_2 and vice versa), we have for all $h_1 \in H_1 \setminus H_2$, $h_2 \in H_2 \setminus H_1$ that $h_1h_2 \in H_1$ or $h_1h_2 \in H_2$ (since $G = H_1 \cup H_2$ is a group). In the first case we find $h_2 \in H_1$, which contradicts our assumption $h_2 \in H_2 \setminus H_1$. In the second case we find $h_1 \in H_2$, which contradicts our assumption $h_1 \in H_1 \setminus H_2$. We conclude that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$; but then $H_2 = G$ or $H_1 = G$, respectively.

Exercise 4.5. Suppose there is $K \leq G$ such that $G \setminus H \subseteq K$. For every $h \in H$, $g \notin H$ we have $gh \notin H$ since H is a group. This means $gh \in K$, and, since also $g \in K$ and K is a group, we have $h = g^{-1}gh \in K$. This holds for every $h \in H$ and so $H \subseteq K$. With this we have $G \subseteq K$ and hence $G = K$. The claim now follows from Definition 4.1.

Exercise 4.6.

(1) Since 0 is the neutral element of $\mathbb{R}$ and $\{0\} \leq \langle (0, \epsilon] \rangle$ by definition, we may assume $x \in \mathbb{R} \setminus \{0\}$. Choose $n \in \mathbb{Z}$ such that $x_0 := x/n \in (0, \epsilon]$ (this is always possible by the Archimedian principle). Hence $x = nx_0$ with $x_0 \in (0, \epsilon]$ and the claim is proved.
(2) The set $\mathcal{S} = \{\frac{1}{q} : q \in \mathbb{N}\}$ generates $\mathbb{Q}$, since every $x \in \mathbb{Q}$ can be expressed as $x = n\frac{1}{q}$ for $n \in \mathbb{Z}$, $q \in \mathbb{N}$.

Exercise 4.7. The relations given in the hint follow from direct computation. They imply that every $g \in \mathrm{SL}(2, \mathbb{R})$ can be represented as a product of the matrices $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The claim now follows from Theorem 4.3.

Exercise 5.12.

(1) For element of an abelian group $(ab)^r = a^r b^r$. Hence, if ord $a = m$ and ord$b = n$, then ord $ab \leq mn$. That is, every product of finite-order elements has finite order. Since the inverse of a group element has the same order the first claim is proved.

A counter example for the case of a non-abelian group is the following. Consider the group of maps $\mathbb{R} \to \mathbb{R}$ generated by the reflections $R_0 : x \mapsto -x$ (reflection at $x = 0$) and $R_1 : x \mapsto 1 - x$ (reflection at $x = 1/2$). We have $R_0^2 = \mathrm{id} = R_1^2$, i.e., both elements have order 2. However, $R_1 \circ R_0(x) = R_1(-x) = 1+x$, i.e., $T_1 = R_1 \circ R_0 : x \mapsto x + 1$ is a translation by 1. Clearly $T^n \neq \mathrm{id}$ for any $n \in \mathbb{Z} \setminus \{0\}$, and therefore T_1 has infinite order.

A second counter example is given by the following matrices: $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ satisfy the relations $S^2 = -e$ and $T^3 = -e$, and have therefore order 4 and 6, respectively. For the product, $TS = -\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, which has infinite order since $(TS)^n = (-1)^n \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq e$ for any $n \in \mathbb{Z} \setminus \{0\}$.

(2) We have $(ab)^2 = e$, and hence $ab = b^{-1}a^{-1}$. But since $a^2 = e$, $b^2 = e$, we have $a^{-1} = a$ and $b^{-1} = b$, so $ab = ba$ and the claim follows.

(3) Suppose a is the only element in G of order 2. Given $g \in G$, et $b = gag^{-1}$. Then $\neq e$ and $b^2 = gag^{-1}gag^{-1} = ga^2g^{-1} = e$. Hence b has order 2 and thus by assumption $a = b$. So $a = gag^{-1}$, i.e., $ag = ga$ for all $g \in G$.

Exercise 5.13.

(1) $\varphi(a)^s = \varphi(a^s)$ since φ is a homomorphism. Because it is an automorphism $\varphi(a^s) = e$ if and only if $a^s = e$. Since the order of an element g is either infinite or the smallest integer $s > 0$ such that $g^s = e$, the claim is proved.

(2) Apply (1) with the inner automorphism $\varphi = \varphi_b$.

(3) Let $a, c \in G$. Applying (2) with the choice $b = ca$ yields ord $ac =$ ord $aba^{-1} =$ ord $b =$ ord ca which proves the claim.

(4) We have $a^s = e$ if and only if $(a^{-1})^s = e$. Since the order of an element g is either infinite or the smallest integer $s > 0$ such that $g^s = e$, the claim is proved.

Exercise 5.14.

(1) Every $g \in G = \langle a \rangle$ is of the form $g = a^k$, $0 \leq k \leq n - 1$. Hence $\varphi(a) = a^k$ for some k in the above range. By Exercise 5.13 (1), ord $a^k =$ ord $a = n$, and

so Theorem 5.8 implies that $\gcd(k, n) = 1$. [Note that $\varphi(a) = a^k$ implies $\varphi(a^m) = \varphi(a)^m = (a^k)^m = (a^m)^k$ and thus $\varphi(g) = g^k$ for all $g \in G$.]

(2) By (2), every $\varphi \in \operatorname{Aut} G$ is of the form $\varphi(g) = g^k$, for some $k \in \{0, \dots, n-1\}$ with $\gcd(k, n) = 1$. On the other hand, for every such k the map $\varphi_k : g \mapsto g^k$ defines an automorphism: it is clearly a homomorphism since G is abelian, and bijective with the inverse $\varphi_k^{-1} = \varphi_{k'} : g \mapsto g^{k'}$, where k' is the inverse of k in $\mathbb{Z}_n^*$, i.e., $k'k = 1 \bmod n$. The preceding discussion shows that the map

$$\Phi : \mathbb{Z}_n^* \to \operatorname{Aut} G, \qquad k \mapsto \varphi_k. \tag{17.8}$$

is a bijection. To prove that it is a homomorphism (and thus an isomorphism), we need to show $\Phi(km) = \varphi_{km} = \varphi_k \circ \varphi_m = \Phi(k) \circ \Phi(m)$ for all $k, m \in \mathbb{Z}_n^*$; this however follows from $\varphi_{km}(g) = g^{km} = (g^m)^k = \varphi_k(\varphi_m(g)) = \varphi_k \circ \varphi_m(g)$.

Exercise 6.13. By Corollary 6.12, $s = \operatorname{ord} a$ divides $|G|$, i.e., $|G| \in s\mathbb{Z}$. Hence Corollary 5.7 implies $a^{|G|} = e$.

Exercise 6.26.

(1) We have $\mathbb{Z}_{15}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$ and hence $|\mathbb{Z}_{15}^*| = \varphi(15) = 8$. Furthermore $\langle\overline{7}\rangle = \{\overline{1}, \overline{4}, \overline{7}, \overline{13}\}$ since
   (a) $\overline{7}^2 = \overline{49} = \overline{4}$,
   (b) $\overline{7}^3 = \overline{4} \cdot \overline{7} = \overline{28} = \overline{13}$,
   (c) $\overline{7}^4 = \overline{13} \cdot \overline{7} = -\overline{2} \cdot \overline{7} = -\overline{14} = \overline{1}$.

   By Lagrange's Theorem, $|\mathbb{Z}_{15}^* : \langle\overline{7}\rangle| = 8/4 = 2$, and so we have two left cosets $\mathbb{Z}_{15}^* = \langle\overline{7}\rangle \cap \overline{2}\langle\overline{7}\rangle$. [Instead of $\overline{2}$ any element not in $\langle\overline{7}\rangle$ can be used.]

(2) $\overline{7}^{350} = \overline{7}^{352}\overline{7}^{-2} = \overline{7}^{-2}$ (since $352 = 8 \cdot 44$, apply Fermat's little theorem with $|G| = 8$) $= \overline{13}^2 = \overline{(-2)}^2 = \overline{4}$.

   $\overline{2}^{1000} = \overline{1}$ since $1000 = 8 \cdot 125$ and by Fermat's little theorem.

Exercise 7.4.

(1) Since H, K are normal in G, we have $HK = KH$ and hence HK is a subgroup of G (Theorem 3.11). To show HK is normal, note that for any $g \in G$: $gHKg^{-1} = gHg^{-1}gKg^{-1} \subseteq HK$, since by normality of H, K we have $gHg^{-1} \subseteq H$, $gKg^{-1} \subseteq K$.

(2) Set $N = \bigcap_{x \in G} xHx^{-1}$. This means that if $a \in N$ we have that $a \in xHx^{-1}$ for all $x \in G$. For any $g \in G$ we have $gag^{-1} \in yHy^{-1}$ with $y = gx \in G$, and hence $gag^{-1} \in yHy^{-1}$ for all $y \in G$. That is, $gag^{-1} \in N$, i.e., $gNg^{-1} \subseteq N$ and so N is normal.

Exercise 7.9.

(1) Suppose $a, b \in N_G(X)$, i.e., $aX = Xa$, $bX = Xb$. Then $Xa^{-1} = a^{-1}X$ and so $a^{-1} \in N_G(X)$. Furthermore, $abX = aXb = Xab$ and thus $ab \in N_G(X)$.

(2) If $H \trianglelefteq G$ then by definition $aHa^{-1} \subseteq H$ for all $a \in G$. Since this implies that $H \subseteq a^{-1}Ha$, we have in fact $H \subseteq aHa^{-1}$ for all $a \in G$ and hence $aH = Ha$ for all $a \in G$. Therefore $N_G(H) = G$.

If on the other hand $N_G(H) = G$, we have $xH = Hx$ for all $x \in G$ and hence $xHx^{-1} \subseteq H$ for all $x \in G$. Hence $H \trianglelefteq G$.

(3) We have for all $g \in N_G(H)$: $gHg^{-1} = (gH)g^{-1} = (Hg)g^{-1} = H$, and so $H \trianglelefteq N_G(H)$.

(4) Problem (2) says that $K \trianglelefteq H$ implies $N_H(K) = H$. The statement follows from the observation that $N_H(K) = \{h \in H : hK = Kh\} \subseteq N_G(K)$.

Exercise 8.8. The idea of proof is similar as in Lagrange's theorem. Consider the union

$$HK = \bigcup_{h \in H} hK. \tag{17.9}$$

Let us calculate the number of disjoint cosets hK, $h \in H$. $hK = K$ implies $h \in K$ and thus $h \in H \cap K$. $hK = h'K$ implies that $h'h^{-1} \in H \cap K$, i.e., $h' \in h(H \cap K)$. Hence each coset in $\{hK : h \in H\}$ corresponds exactly to a coset $h(H \cap K)$ with $h \in H$. Since $H \cap K$is a subgroup of H there are $|H : H \cap K| = |H|/|H \cap K|$ such cosets. So the union (17.9) is a disjoint union of $|H|/|H \cap K|$ sets, each with $|K|$ elements. This proves the claim.

Exercise 9.10.

(1) The normal subgroup property implies that $bab^{-1} \in N_i$ and $aba^{-1} \in N_j$. Hence for $i \neq j$ we have

$$abab^{-1}b^{-1} \in N_iN_i \cap N_jN_j = N_i \cap N_j \subseteq N_i \cap \prod_{j\neq i} N_j = \{e\}, \tag{17.10}$$

and so $abab^{-1}b^{-1} = e$, i.e., $ab = ba$.

(2) Because of Definition 9.6 (1) the decomposition $a = a_1 \cdots a_k$ with $a_i \in N_i$ exists. It remains to show uniqueness. First consider the special case $e = a_1 \cdots a_k$. Then, for every i, we have using (1)

$$a_i^{-1} = a_1 \cdots a_{i-1}a_{i+1} \cdots a_n \in N_i \cap \prod_{j\neq i} N_j = \{e\} \tag{17.11}$$

and hence $a_i = e$ for every i. As to the general case, suppose we have two decompositions $a = a_1 \cdots a_k$ and $a = b_1 \cdots b_k$, then, using again (1), we see that $(a_1b_1^{-1}) \cdots (a_kb_k^{-1}) = e$, which, in view of the special case considered before, implies that $a_ib_i^{-1} = e$, i.e., $a_i = b_i$.

Exercise 9.17. Theorem 8.5 shows that G is cyclic if and only if $G \simeq \mathbb{Z}_n$ with $n = p_1^{k_1} \dots p_r^{k_r}$. Using Theorem 9.16, we have $\mathbb{Z}_n = \mathbb{Z}_{p_1^{k_1}\cdots p_{r-1}^{k_{r-1}}} \times \mathbb{Z}_{p_r^{k_r}}$. Hence, by induction on r, $\mathbb{Z}_n = \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_r^{k_r}}$.

Exercise 9.22.

(1) (We have already proved this; cf. Corollary 6.19.) The group $L = H \cap K$ is a subgroup of both H and K. Hence, by Lagrange's Theorem, $|L|$ divides both $|H|$ and $|K|$. But since the latter a coprime, the only possibility is $|L| = 1$ and hence $L = \{e\}$. (Note: We have not used the fact that H, K are normal.)

(2) Since $H \trianglelefteq G$ we have $gH = Hg$ for all $g \in G$. Hence in particular (for $g \in K$) we have $HK = KH$, and hence $G' := HK$ is a group (by Theorem 3.11); note that this fact was already proved in Exercise 7.4. Part (1) of the present exercise shows that G' is an inner direct product of H and K, and so, by Theorem 9.9, $hk = kh$ for all $h \in H$, $k \in K$.

(3) We have shown in (2) that HK is an inner direct product. By Theorem 9.12 this inner direct product is isomorphic to the outer direct product $H \times K$.

Exercise 10.8.

(1) We have by definition of the stabiliser $G_{g\cdot x} = \{h \in G : h \cdot (g \cdot x) = g \cdot x\}$, which equals $\{h \in G : (g^{-1}hg) \cdot x = x\} = \{gkg^{-1} : k \in G,\ k \cdot x = x\} = g\{k \in G : k \cdot x = x\}g^{-1} = gG_x g^{-1}$, with $k = g^{-1}hg$.

(2) The statement ($G_x = G_y$ for all $y \in G \cdot x$) is, by item (1) of this exercise, equivalent to ($G_x = G_{g\cdot x} = gG_x g^{-1}$ for all $g \in G$), which in turn is equivalent to $G_x \trianglelefteq G$.

Exercise 10.12.

(1) This can be either checked by a direct computation (recommended), or by the observation that the action can be represented as $(M, \xi) \mapsto M\xi$, where $M\xi$ is the standard matrix product of a 2×2 with a 2×1 matrix. Axiom (1) for group actions follows then from the associativity of matrix multiplication, and axiom (2) from $E\xi = \xi$, where E is the identity matrix.

(2) We have $G \cdot 0 = \{0\}$, so the origin $0 \in \mathbb{R}^2$ is a fixed point and orbit of the G action. Furthermore, given a point $\begin{pmatrix} x \\ y \end{pmatrix} \neq 0$, there is a matrix $M \in G$ such that $\begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; this matrix is given by $M = \begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix}$ if $x \neq 0$ and $M = \begin{pmatrix} x & 1 \\ y & 0 \end{pmatrix}$ if $y \neq 0$. Hence $\mathbb{R}^2 \setminus \{0\} = G \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is the only other orbit of the G action, and 0 is the only fixed point.

Exercise 10.13.

(1) The orbits are $H \cdot \begin{pmatrix} r \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} r\cos\phi \\ r\sin\phi \end{pmatrix} : \phi \in [0, 2\pi) \right\}$ for $r \geq 0$, i.e., the origin $\{0\}$ ($r = 0$) and all circles of radius $r > 0$ centered at the origin. 0 is thus the only fixed point.

(2) The orbits are $H \cdot 0 = \{0\}$, and the rays $H \cdot \begin{pmatrix} \cos\phi \\ \sin\phi \end{pmatrix} = \left\{ \begin{pmatrix} a\cos\phi \\ a\sin\phi \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}$ for $\phi \in [0, 2\pi)$. 0 is therefore again the only fixed point.

(3) The orbits are $H \cdot 0 = \{0\}$, $H \cdot \begin{pmatrix} r \\ r \end{pmatrix} = \left\{ \begin{pmatrix} ra \\ ra^{-1} \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}$ for $r \in \mathbb{R} \setminus \{0\}$ (i.e., the branches of hyperbolas satisfying the equation $xy = r^2$, where r values with the same modulus but opposite sign correspond to different orbits) and $H \cdot \begin{pmatrix} r \\ -r \end{pmatrix} = \left\{ \begin{pmatrix} ra \\ -ra^{-1} \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}$ for $r \in \mathbb{R} \setminus \{0\}$ (the branches of hyperbolas satisfying the equation $xy = -r^2$). 0 is the only fixed point.

(4) The orbits are the one-element sets $H \cdot \begin{pmatrix} r \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} r \\ 0 \end{pmatrix} \right\}$ for $r \in \mathbb{R}$, and the straight lines $H \cdot \begin{pmatrix} 0 \\ r \end{pmatrix} = \left\{ \begin{pmatrix} x \\ r \end{pmatrix} : x \in \mathbb{R} \right\}$ for $r \in \mathbb{R} \setminus \{0\}$. Hence $\mathrm{Fix}_H(\mathbb{R}^2) = \left\{ \begin{pmatrix} r \\ 0 \end{pmatrix} : r \in \mathbb{R} \right\}$.

(5) We have $H = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$. The H action yields $\pi/2$ rotations in $\mathbb{R}^2$ about the origin. The orbits are $H \cdot 0 = \{0\}$, $H \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \left\{ \pm \begin{pmatrix} x \\ y \end{pmatrix}, \pm \begin{pmatrix} y \\ -x \end{pmatrix} \right\}$, which are disjoint for $x > 0, y \geq 0$, say. 0 is the only fixed point.

Exercise 10.22.

(1) We have $(gh)(aH) = g(haH)$ by the associativity of group composition, and $e(aH) = aH$ by the identity axiom.

(2) Let $x = aH$, $y = bH \in X = G/H$. Then $g = ba^{-1} \in G$ satisfies $g \cdot x = (ba^{-1})(aH) = bH = y$.

Exercise 12.11.

(1) By the Third Sylow Theorem s_2 divides 12 and is of the form $2k+1$ for some $k \geq 0$. Hence $s_2 \in \{1, 3\}$. Similarly, s_3 divides 12 and is of the form $3k+1$ for some $k \geq 0$. Hence $s_3 \in \{1, 4\}$.

(2) Suppose $s_3 = 4$, i.e., there are four distinct 3-Sylow groups P_1, P_2, P_3, P_4 of G, each with 3 elements. Then for $i \neq j$, $P_i \cap P_j < P_i$ and thus $|P_i \cap P_j| < 3$. Hence $|P_i \cap P_j| = 1$ (since 2 does not divide 3) and so $P_i \cap P_j = \{e\}$. Therefore G has 8 elements of order 3 (2 from each P_i), and the identity.

The set S of three remaining elements in G is the set of elements which order is not equal to 3. This follows from the fact that if $\operatorname{ord} g = 3$, then $\langle g \rangle$ is a 3-Sylow group and hence is equal to one of P_1, P_2, P_3, P_4. So G has only 8 elements of order 3. Thus

$$\bigcup_{i=1}^{4} P_i = \{g \in G : \operatorname{ord} g = 3\} \cup \{e\}$$

and hence

$$S := G \setminus \bigcup_{i=1}^{4} P_i = \{g \in G : g \neq e, \operatorname{ord} g \neq 3\}.$$

We note that every 2-Sylow group in G (which has order 12) has order 4. Since 4 and 3 are coprime, it is clear that every 2-Sylow group has a trivial intersection with any P_i and is therefore contained in $S \cup \{e\}$. But $|S \cup \{e\}| = 4$. This implies that $S \cup \{e\}$ is a 2-Sylow group (in particular a group). Moreover, any 2-Sylow group is equal to $S \cup \{e\}$. Hence, there can be only one 2-Sylow group.

(3) Since there is a unique 2-Sylow group P_2 and a unique 3-Sylow group P_3, by Corollary 11.13 both are normal in G. Now $P_2 \cap P_3 < P_3$ and so, by the same argument as in (2), $P_2 \cap P_3 = \{e\}$. Therefore, and since $|P_2| = 4$, $|P_3| = 3$, we have $|P_2P_3| = 12$ and thus $G = P_2P_3$. G is hence an inner direct product of P_2 and P_3. By 12.1 $P_3 \simeq \mathbb{Z}_3$, and by Theorem 12.2 $P_2 \simeq \mathbb{Z}_4$ or $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. We conclude

$$G \simeq \mathbb{Z}_3 \times \mathbb{Z}_4, \qquad \text{or} \qquad G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3. \tag{17.12}$$

Exercise 12.12. By Theorem 12.3, a group G of order $8 = 2^3$ has a normal subgroup N of order $4 = 2^2$. N can only be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$ (Theorem 12.2). That is, (Case 1) $N = \langle a_1 \rangle \langle a_2 \rangle$ with $a_1 a_2 = a_2 a_1$, $\operatorname{ord} a_1 = \operatorname{ord} a_2 = 2$, or (Case 2) $N = \langle a \rangle$ with $\operatorname{ord} a = 4$. Since $|G : N| = 2$ we have $G = N \cup bN$, with $b \in G \setminus N$.

Furthermore $|G : N| = 2$ implies $G/N \simeq \mathbb{Z}_2$, and hence $b^2 \in N$. There are now three possibilities: $\operatorname{ord} b = 2, 4, 8$.

- If $\operatorname{ord} b = 8$, then $G = \langle b \rangle \simeq \mathbb{Z}_8$.

- If ord $b = 4$, then $b^2 \neq e$ and so $\langle b \rangle \cap N$ is a non-trivial subgroup of G.

  For Case 1: Then $b^2 = a_1$ (or $b^2 = a_2$, which we ignore in the following since it will lead to an isomorphic group). The coset decomposition with respect to $\langle b \rangle$ yields

$$G = \{e, b, b^2, b^3, a_2, a_2b, a_2b^2, a_2b^3\}. \tag{17.13}$$

  If a_2 and b commute, we have $G = \langle b \rangle \langle a_2 \rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$. If they do not, $ba_2 \neq a_2b$. The cases $ba_2 = e, b, b^2, b^3$ are easily ruled out (the latter would for instance imply $a_2 = a_1$). Now $ba_2 = a_2b^2 = a_2a_1 = a_1a_2$ which implies $b = a_1$, a contradiction. $ba_2 = a_2b^3$ is thus the only possibility. This relation can be written $ba_2ba_2 = e$, i.e., $\mathrm{ord}(ba_2) = 2$. Hence we obtain the dihedral group $G = D_4$, cf. (12.2); recall also Exercise 1.15.

  For Case 2: Then $b^2 = a^2$, and the coset decomposition with respect to $N = \langle a \rangle$ yields

$$G = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\}. \tag{17.14}$$

  If G abelian then $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ as above. So we assume G is not abelian. Since $\langle a \rangle$ is normal, $bab^{-1} \in \langle a \rangle$. Then $bab^{-1} = a^2$ or $bab^{-1} = a^3$ are the only possibilities. The former becomes $bab^{-1} = b^2$, i.e., $a = b^2 = a^2$, a contradiction. The latter becomes $bab^{-1} = a^3 = b^2a$, i.e., $ab^{-1} = ba$. (The corresponding group is called Hamilton's quaternion group.)

- If ord $b = 2$, i.e., $b^2 = e$, then $\langle b \rangle \cap N = \{e\}$ (otherwise $b \in N$, contradicting the above).

  For Case 1:

$$G = \{e, a_1, a_2, a_1a_2, b, ba_1, ba_2, ba_1a_2\}. \tag{17.15}$$

  If $\mathrm{ord}(ba_1) = 4$ or 8, then G contains an element $\tilde{b} = ba_1 \notin N$ of order 4 or 8, respectively. We have already dealt with these cases above. Hence we may assume $\mathrm{ord}(ba_1) = 2$, that is, $ba_1ba_1 = e$, i.e., $a_1b = ba_1$. We infer similarly that $a_2b = ba_2$. Therefore $G = \langle b \rangle \langle a_1 \rangle \langle a_2 \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

  For Case 2:

$$G = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\}. \tag{17.16}$$

  As in Case 1, we may assume $\mathrm{ord}(ba) = 2$, hence $ba = a^{-1}b$. This implies $\mathrm{ord}(ba^3) = 2$, and

$$(ba)(ba^3) = a^2 = (ba^3)(ba). \tag{17.17}$$

  Then $H = \langle ba \rangle \langle ba^3 \rangle = \langle ba^3 \rangle \langle ba \rangle = \{e, ba, a^2, ba^3\}$ is a group by Theorem 3.11. [Note that although the element ba^2 has also order 2, neither $\langle ba \rangle \langle ba^2 \rangle$ nor $\langle ba^2 \rangle \langle ba^3 \rangle$ give us a group.]

It follows from (17.17) that H is abelian, and so we have $\langle ba \rangle \trianglelefteq H$ and $\langle ba^3 \rangle \trianglelefteq H$. Hence the group H is an inner direct product and isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. [This follows also from Theorem 9.11.] Since $aHa^{-1} \subseteq H$, $bHb^{-1} \subseteq H$ (check!), H is normal in G. Note that $a \notin H$. So with a assuming the role of b above, and H assuming the role of N above, the present case actually corresponds to the situation ord $b = 4$, Case 1.

In conclusion, the above shows that the only groups of order 8 are the cyclic groups $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, the dihedral group D_4 in (12.2), and Hamilton's quaternion group, which is generated by a, b subject to the relations $a^4 = e$, $b^2 = a^2$, $ab^{-1} = ba$.

Exercise 13.7. Since G is finitely generated, it is by Theorem 13.6 the direct product of finitely many cyclic groups $\langle a_1\rangle \times \cdots \times \langle a_r\rangle$. If G is infinite then at least one of these, say $\langle a_1\rangle$, must be infinite. This in turn implies that G contains an element of infinite order, namely $(a_1, e, e, \ldots, e)$, contradicting our assumption.

Exercise 14.2. It is well known that the composition of two bijective maps is bijective. The composition of maps is furthermore associative. The existence of the identity and inverse is evident.

Exercise 14.31.

(1) $\pi = (1,2,4,8)(3,6,12,9)(5,10)(7,14,13,11)$.
(2) Use Theorem 14.9 (3): $\pi = (1,2)(2,4)(4,8)(3,6)(6,12)(12,9)(5,10)(7,14)(14,13)(13,11)$.

Exercise 14.32. Use Theorem 14.9 (7), i.e., $\pi(i_1, \ldots, l_r)\pi^{-1} = (\pi(i_1), \ldots, \pi(i_r))$.

(1) $\pi(2,3)(1,4)\pi^{-1} = \pi(2,3)\pi^{-1}\pi(1,4)\pi^{-1} = (1,3)(2,4)$.
(2) $\pi = (2,3,4)$, so $\pi(1,2,3)\pi^{-1} = (1,3,4)$.
(3) $\pi(1,2,3,4,5)\pi^{-1} = (1,3)(2,4,1)(1,2,3,4,5)(2,4,1)^{-1}(1,3)^{-1} = (1,3)(2,4,3,1,5)(1,3)^{-1} = (2,4,1,3,5)$.
(4) $\pi(1,2,3,4,5)\pi^{-1} = (1,2,3)(1,2,3,4,5)(1,2,3)^{-1} = (2,3,1,4,5)$.

Exercise 14.33. For $f = \begin{pmatrix} 1 & 2 & \cdots & r \\ i_1 & i_2 & \cdots & i_r \end{pmatrix}$ we have by Theorem 14.9 (7): $f(1,2,\ldots,r)f^{-1} = (i_1, i_2, \ldots, i_r)$. Hence the r-cycle $(i_1, i_2, \ldots, i_r)$ is conjugate to $(1,2,\ldots,r)$, and so all r-cycles are conjugate.

Exercise 14.34. As shown in 14.13, any transposition can be written as $(i,j) = (1,i)(1,j)(1,i)$. Since S_n is generated by transpositions (Corollary 14.12), it is also generated by the transpositions $(1,i)$, $i = 2,\ldots,n$.

Exercise 15.8. Let $G_1 = H_1 = \mathbb{Z}$, $G_2 = 15\mathbb{Z}$, $G_3 = 60\mathbb{Z}$, $H_2 = 12\mathbb{Z}$, $G_4 = H_3 = \{0\}$. Then

$$
\begin{aligned}
G_{1,2} &= G_2(G_1 \cap H_2) = 15\mathbb{Z} + 12\mathbb{Z} = 3\mathbb{Z},\\
G_{1,3} &= G_2(G_1 \cap H_3) = 15\mathbb{Z} + \{0\} = 15\mathbb{Z},\\
G_{2,1} &= G_3(G_2 \cap H_1) = 60\mathbb{Z} + 15\mathbb{Z} = 15\mathbb{Z},\\
G_{2,3} &= G_3(G_2 \cap H_2) = 60\mathbb{Z} + (15\mathbb{Z} \cap 12\mathbb{Z}) = 60\mathbb{Z},\\
G_{3,1} &= G_4(G_3 \cap H_1) = 60\mathbb{Z},\\
G_{3,2} &= G_4(G_3 \cap H_2) = 60\mathbb{Z} \cap 12\mathbb{Z} = 60\mathbb{Z},\\
H_{1,2} &= H_2(G_2 \cap H_1) = 12\mathbb{Z} + 15\mathbb{Z} = 3\mathbb{Z},\\
H_{1,3} &= H_2(G_3 \cap H_1) = 12\mathbb{Z} + 60\mathbb{Z} = 12\mathbb{Z},\\
H_{1,4} &= H_2(G_4 \cap H_1) = 12\mathbb{Z},\\
H_{2,1} &= H_3(G_1 \cap H_2) = 12\mathbb{Z},\\
H_{2,3} &= H_3(G_3 \cap H_2) = 60\mathbb{Z} \cap 12\mathbb{Z} = 60\mathbb{Z},\\
H_{2,4} &= H_3(G_4 \cap H_2) = \{0\}.
\end{aligned}
\tag{17.18}
$$

We thus obtain the refinements (ignoring repetitions)

$$\mathbb{Z} > 3\mathbb{Z} > 15\mathbb{Z} > 60\mathbb{Z} > \{0\} \qquad \text{(with factors } \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_4, \mathbb{Z}) \tag{17.19}$$

$$\mathbb{Z} > 3\mathbb{Z} > 12\mathbb{Z} > 60\mathbb{Z} > \{0\} \qquad \text{(with factors } \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}). \tag{17.20}$$

Exercise 15.15. Let $G = G_1 \geq \ldots \geq G_r = \{e\}$ be the composition series of the abelian group G. Then G_i/G_{i+1} is simple and abelian. Because every subgroup of an abelian group is normal, being simple means in this case that G_i/G_{i+1} goes not contain any proper non-trivial subgroup. This is only possible if G_i/G_{i+1} is cyclic (if there was more than one generator we would have non-trivial subgroups) and finite (any infinite cyclic group is isomorphic to $\mathbb{Z}$ which has non-trivial subgroups). Therefore G_i/G_{i+1} is finite for all i. Now by Lagrange's Theorem $|G| = |G_1/G_2||G_2/G_3|\cdots|G_{r-2}/G_{r-1}||G_{r-1}/G_r|$, which is finite since every factor is. Hence G is finite.

Exercise 15.16. Recall that very subgroup of a cyclic group is cyclic. So the subgroups of $\mathbb{Z}_{24}$ are of the form $m\mathbb{Z}_{24} \simeq \mathbb{Z}_{24/m}$ for every integer m that divides 24. The factors of any normal series of $\mathbb{Z}_{24}$ are thus $\mathbb{Z}_{24/m}/\mathbb{Z}_{24/n} \simeq \mathbb{Z}_{n/m}$ where $m, n|24$ and $m|n$. $\mathbb{Z}_{n/m}$ is simple if and only if n/m is a prime. The following are therefore composition series

of $\mathbb{Z}_{24}$:

$$\begin{aligned}
&\mathbb{Z}_{24} > \mathbb{Z}_8 > \mathbb{Z}_4 > \mathbb{Z}_2 > \{0\} \text{ with factors } \mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2;\\
&\mathbb{Z}_{24} > \mathbb{Z}_{12} > \mathbb{Z}_4 > \mathbb{Z}_2 > \{0\} \text{ with factors } \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2;\\
&\mathbb{Z}_{24} > \mathbb{Z}_{12} > \mathbb{Z}_6 > \mathbb{Z}_2 > \{0\} \text{ with factors } \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2;\\
&\mathbb{Z}_{24} > \mathbb{Z}_{12} > \mathbb{Z}_6 > \mathbb{Z}_3 > \{0\} \text{ with factors } \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3.
\end{aligned} \tag{17.21}$$

The Jordan-Hölder Theorem implies (in view of the above factors) that these are in fact all composition series.

Exercise 16.12. For $(a, a'), (b, b') \in G \times G'$ we have

$$\begin{aligned}
[(a, a'), (b, b')] &= (a, a')(b, b')(a, a')^{-1}(b, b')^{-1}\\
&= (aba^{-1}b^{-1}, a'b'a'^{-1}b'^{-1})\\
&= ([a, b], [a', b']).
\end{aligned} \tag{17.22}$$

This proves that $K(G \times G') = K(G) \times K(G')$ and hence by induction $K_m(G \times G') = K_m(G) \times K_m(G')$.

Exercise 16.25. Let $N = K(G)$. Consider the map $\varphi : G \to G/N$, $a \mapsto a^m N$. Since G/N is abelian (by Corollary 16.6), we have $(ab)^m N = (aNbN)^m = (aN)^m (bN)^m = a^m b^m N$. Thus $\varphi(ab) = \varphi(a)\varphi(b)$ and hence φ is a homomorphism. The kernel of φ is

$$\ker \varphi = \{a \in G : a^m N = N\} = \{a \in G : a^m \in N\} = G_m, \tag{17.23}$$

which implies that G_m is a normal subgroup of G.

Exercise 16.26. If $N \trianglelefteq G$, then for $n \in N$, $g \in G$ we have $[g, n] = gng^{-1}n^{-1} = n'gg^{-1}n^{-1} = n'n^{-1}$ for some $n' \in N$, and so $[g, n] \in N$ for all $n \in N$, $g \in G$. This implies $[G, N] \subseteq N$.

To prove the reverse implication, assume $[G, N] \subseteq N$. Hence in particular $[g, n] = gng^{-1}n^{-1} \in N$ for all $n \in N$, $g \in G$. Thus $gng^{-1} \in N$ for all $n \in N$, $g \in G$, i.e., $gNg^{-1} \subseteq N$ for all $g \in G$.