Group Theory

Lecture Notes by Lorenz Halbeisen

http://user.math.uzh.ch/halbeisen/4students/gt.html

0. Introduction

A theory of groups first began to take form at the end of the eighteenth century. It developed slowly and attracted very little notice during the first decades of the nineteenth century. Then, in a few years around 1830, the theory of groups took a giant leap forward and made a major contribution to the general development of mathematics in the work of Galois and Abel on the solvability of algebraic equations.

Since then, the concepts underlying the theory of groups have been elaborated and extended into many branches of mathematics. There have been applications to such diverse fields as number theory, crystallography, and the theory of knots.

This module is mainly concerned with finite groups, especially the groups of rigid motions of the five Platonic solids, which are tetrahedron, cube, octahedron, dodecahedron, and icosahedron. But our first task is to clarify what is meant by a group.

Let us consider two different sets, each with a binary operation: The first set is $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of integers, and the binary operation on $\mathbb{Z}$ is addition.

The second set is the set of non-zero rational numbers $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, where $\mathbb{Q} := \big\{n/m : n \in \mathbb{Z} \wedge m \in \mathbb{Z} \setminus \{0\}\big\}$, and the binary operation on $\mathbb{Q}^*$ is multiplication.

Thus, we have two so-called *structures*, which we denote by $(\mathbb{Z}, +)$ and $(\mathbb{Q}^*, \cdot\,)$ respectively.

In $\mathbb{Z}$, there is an element x such that for each $y \in \mathbb{Z}$ we have $x + y = y + x = y$, namely $x = 0$. Such an element we call a **neutral element**. Hence, we get:

Observation 1. $(\mathbb{Z}, +)$ has a neutral element.

Similarly, in $\mathbb{Q}^*$, there is an element x such that for each $y \in \mathbb{Q}^*$ we have $x \cdot y = y \cdot x = y$, namely $x = 1$. Hence, we get:

Observation 2. $(\mathbb{Q}^*, \cdot\,)$ has a neutral element.

Are there some neutral elements in $(\mathbb{Z}, +)$ other than 0, or are there some neutral elements in $(\mathbb{Q}^*, \cdot\,)$ other than 1?

No, of course, you would say, but why not? Let us prove it for the structure $(\mathbb{Z}, +)$: Assume that $z \in \mathbb{Z}$ is a neutral element. So, for any $y \in \mathbb{Z}$ we have $z+y = y+z = y$. In particular we get $z+0 = 0+z = 0$, but since 0 is neutral, we also have $z+0 = 0+z = z$, hence, $z = 0$. This proves the following:

Observation 3. $(\mathbb{Z}, +)$ has exactly one neutral element, namely 0.

Similarly, one can prove the following (see Hw1.Q1a):

Observation 4. $(\mathbb{Q}^*, \cdot\,)$ has exactly one neutral element, namely 1.

For every $x \in \mathbb{Z}$ there is a $y \in \mathbb{Z}$ such that $x + y = y + x = 0$, in fact, $y = -x$. Such a y is called an **inverse** of x.

Observation 5. In $(\mathbb{Z}, +)$, each element has an inverse.

Notice that this is not true in $(\mathbb{N}, +)$, where $\mathbb{N} = \{0, 1, 2, \ldots\}$. Why?

Similarly, for every $q \in \mathbb{Q}^*$ there is a $p \in \mathbb{Q}^*$ such that $q \cdot p = p \cdot q = 1$, in fact, $q = 1/p$. Hence, we get:

Observation 6. In $(\mathbb{Q}^*, \cdot)$, each element has an inverse.

Notice that this is not true in $(\mathbb{Q}, \cdot)$. Why?

Is there more than one inverse element to some $x \in \mathbb{Z}$, or is there more than one inverse element to some $q \in \mathbb{Q}^*$?

No, of course, you would say again, but why not? Let us prove it for the structure $(\mathbb{Z}, +)$: Assume that there are $y_1, y_2 \in \mathbb{Z}$ such that $x + y_1 = y_1 + x = 0$ and $x + y_2 = y_2 + x = 0$. Therefore we have

$$\begin{aligned}
y_2 + x &= 0 && \text{add } y_1 \text{ on both sides from the right} \\
y_2 + \underbrace{x + y_1}_{=0} &= \underbrace{0 + y_1}_{=y_1} && \\
\underbrace{y_2 + 0}_{=y_2} &= y_1 && \text{and we finally get} \\
y_2 &= y_1
\end{aligned}$$

This proves the following:

Observation 7. In $(\mathbb{Z}, +)$, each element has exactly one inverse.

In a similar way, one can prove the following (see Hw1.Q1b):

Observation 8. In $(\mathbb{Q}^*, \cdot)$, each element has exactly one inverse.

As we have seen so far, $(\mathbb{Z}, +)$ and $(\mathbb{Q}^*, \cdot)$ are very similar: Both structures have a unique neutral element and in both structures there are inverse elements. In fact, such structures, *i.e.*, sets with a binary operation satisfying certain axioms, are called *groups*.

In this module we will investigate different types of (mainly finite) groups. In other words, we will set up the axioms for groups and look what we get out of them. It will be seen that the input (just three axioms) is small, but the output (dozens of theorems and propositions) is quite extensive.

1. The Axioms

A **binary operation** on a set is a correspondence that assigns to each ordered pair of elements of the set a uniquely determined element of the set. For example addition is a binary operation on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\{0\}$, and multiplication is a binary operation on $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{N}$, $\mathbb{Z}$, $\{-1, 1\}$, and $\{0, 1\}$; on the other hand, addition is neither a binary operation on $\{-1, 1\}$ nor on $\{0, 1\}$. Why?

A set G together with some binary operation, say "$\circ$" is a **group**, if the following axioms are satisfied:

(A0) For any $a, b, c \in G$ we have:

$$a \circ (b \circ c) = (a \circ b) \circ c\,.$$

This says that the operation "$\circ$" is **associative**.

(A1) There is an element $e \in G$ such that for all $a \in G$ we have:

$$e \circ a = a \circ e = a\,.$$

The element e is called a **neutral element** of $(G, \circ)$.

(A2) If e is a neutral element of $(G, \circ)$, then for each $a \in G$ there is an $\bar{a} \in G$ such that

$$a \circ \bar{a} = \bar{a} \circ a = e\,.$$

The element $\bar{a}$ is called an **inverse** of a.

Any binary operation on some set which satisfies (A0) is called associative. It is a consequence of (A0) that we can omit brackets. In particular, whenever "$\circ$" is a binary associative operation on some set S, then for any $a, b, c, d \in S$ we have (see Hw1.Q2):

$$(a \circ b) \circ (c \circ d) = \big(a \circ (b \circ c)\big) \circ d\,.$$

On the other hand, a binary operation is not necessarily associative (see Hw1.Q3).

A binary operation "$\circ$" on some set S is called **commutative** if for all $x, y \in S$ we have

$$x \circ y = y \circ x\,.$$

Definition. A group $(G, \circ)$ is called **abelian**, if the binary operation "$\circ$" is commutative.

For example $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \cdot)$, $\big(\{0\}, +\big)$ and $\big(\{-1, 1\}, \cdot\big)$ are abelian groups. On the other hand, as we will see later, not every group is abelian.

Let us now show that the neutral element of a group is unique and that each element has exactly one inverse.

Proposition 1.1. Let $(G, \circ)$ be a group, then there is exactly one neutral element and each element of G has exactly one inverse.

Proof. Let $e, \tilde{e} \in G$ be neutral elements of $(G, \circ)$. Thus, for every $x \in G$ we have $x \circ \tilde{e} = e \circ x = x$, and therefore,

$$e \underset{\substack{\uparrow \\ \tilde{e} \text{ neutral}}}{=} e \circ \tilde{e} \underset{\substack{\uparrow \\ e \text{ neutral}}}{=} \tilde{e}\,,$$

and hence, there is exactly one neutral element.

Let $a \in G$ be arbitrary and let $x, \tilde{x} \in G$ be such that $a \circ x = \tilde{x} \circ a = e$, where $e \in G$ is the unique neutral element of $(G, \circ)$. Now,

$$\tilde{x} \underset{\substack{\uparrow \\ e \text{ neutral}}}{=} \tilde{x} \circ e = \tilde{x} \circ (a \circ x) \underset{\substack{\uparrow \\ \text{“}\circ\text{” is associative}}}{=} (\tilde{x} \circ a) \circ x = e \circ x \underset{\substack{\uparrow \\ e \text{ neutral}}}{=} x\,,$$

and hence, a has exactly one inverse, and since $a \in G$ was arbitrary, this completes the proof. ⊣

Notation. For an “abstract” group we often write just G and instead of $(G, \circ)$, and for $a, b \in G$ we often write just ab instead of $a \circ b$. In other words, if the binary operation is not specified, we handle it like multiplication, and consequently, we usually denote the inverse of $a \in G$ by a^{-1}.

We can weaken the axioms (A1) and (A2) a little bit:

Proposition 1.2. G is a group if the following axioms hold:

(A0) The binary operation is associative.

(A1*) There is an element $e \in G$ such that for all $a \in G$ we have:

$$ea = a\,.$$

The element e is called a **left-neutral element** of G.

(A2*) If e is a left-neutral element of G, then for each $a \in G$ there is an $\bar{a} \in G$ such that

$$\bar{a}a = e\,.$$

The element $\bar{a}$ is called **left-inverse** of a.

Proof. We have to prove that e is also a right-neutral element of G and that $\bar{a}$ is also a right-inverse of a.

Let $a \in G$ be arbitrary and let $\bar{\bar{a}}$ be a left-inverse of $\bar{a}$, where $\bar{a}$ is a left-inverse of a. Now we have:

$$a\bar{a} \underset{\substack{\uparrow \\ e \text{ left-neutral}}}{=} e(a\bar{a}) = (\bar{\bar{a}}\bar{a})(a\bar{a}) \underset{\substack{\uparrow \\ \text{by associativity}}}{=} \bar{\bar{a}}\overbrace{(\bar{a}a)}^{e}\bar{a} = \bar{\bar{a}}\overbrace{(e\bar{a})}^{\bar{a}} = \bar{\bar{a}}\bar{a} = e\,.$$

Thus, $a\bar{a} = \bar{a}a = e$, which shows that each left-inverse of some $a \in G$ is also a right-inverse, hence an inverse of a.

Further, we have:

$$ae = a(\bar{a}a) \underset{\substack{\uparrow \\ \text{by associativity}}}{=} \overbrace{(a\bar{a})}^{e}a = ea \underset{\substack{\uparrow \\ e \text{ left-neutral}}}{=} a\,.$$

Thus, since $a \in G$ was arbitrary, e is also a right-neutral element, hence, a neutral element of G. $\dashv$

In (A1*) and (A2*) we can replace "left-neutral" and "left-inverse" by "right-neutral" and "right-inverse" respectively (see Hw2.Q9), but we cannot mix left and right:

Proposition 1.3. If a set S with an associative operation has a left-neutral element and each element of S has a right-inverse, then S is not necessarily a group.

Proof. Let $S = \{0, 1\}$ and for $x, y \in S$ define $x * y := y$. Now, the binary operation "$*$" is associative and 0 is a left-neutral element of $(S, *)$, 0 is the right-inverse of 0 as well as of 1, so, each element of S has a right-inverse. On the other hand, there is no $x \in S$ such that $x * 1 = 0$, or in other words, 1 has no left-inverse. Hence, $(S, *)$ is not a group. $\dashv$

Of course, in Proposition 1.3, we can swap "left" and "right" (see Hw2.Q10). However, the situation is different, if the left-neutral element is unique:

Proposition 1.4. If a set G with an associative operation has a unique left-neutral element and each element of G has a right-inverse, then G is a group.

Proof. Let e be the unique left-neutral element of G. Let

$$E(G) = \{a \in G : aa = a\}.$$

First we show that $E(G) = \{e\}$. Take any $a \in E(G)$ and $b \in G$, then

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

Therefore, since b was arbitrary, a is a left-neutral element, and since the left-neutral element is unique, we have $a = e$.

Consider $Ge = \{ge : g \in G\}$, and let us show that Ge is a group. By definition of Ge, any $x \in Ge$ is of the form $x = ge$ (for some $g \in G$). Now, $xe = (ge)e = g(ee) = ge = x$, and therefore, e (or more precisely ee) is a right-neutral element of Ge. Further, let g^{-1} be a right-inverse element of g, then $g^{-1}e \in Ge$ is a right-inverse of $x = ge$. Indeed,

$$x(g^{-1}e) = (ge)(g^{-1}e) = g(eg^{-1})e = (gg^{-1})e = ee = e.$$

So, Ge has a right-neutral element and each element of Ge has a right inverse, which implies (by the "right-version" of Proposition 1.2) that Ge is a group.

In order to show that G is a group, by Proposition 1.2 it is enough to show that each element in G has a left-inverse.

Let g be any element of G, and let $x \in Ge$ be such that $x(ge) = (ge)x = e$ (such an x exists since Ge is a group). We claim that $xg \in E(G)$:

$$\begin{aligned} (xg)(xg) &= (xg)e(xg) && (\text{since } x \in Ge,\ ex = x) \\ &= xeg \\ &= xg && (\text{since } x \in Ge,\ xe = x). \end{aligned}$$

Thus, $xg \in E(G) = \{e\}$, or in other words, $xg = e$. Since $g \in G$ was arbitrary, each element of G has a left-inverse, which implies (by Proposition 1.2) that G is a group. $\dashv$

Definition. The **order** of a group $(G, \circ)$, denoted by $|G|$, is the cardinality (or size) of the underlying set G.

If G has finitely many elements, then $|G| = n$ for some positive integer n (why there is no group with 0 elements?) and if G is infinite, then we set $|G| = \infty$.

To state the next result we have first to give some definitions.

Definition. A set S with a binary operation is **left cancellative** if whenever $x, y, z \in S$ and $xy = xz$, one has $y = z$. The notion **right cancellative** is defined similarly. Further, S is **cancellative** if S is left cancellative as well as right cancellative.

If the binary operation on S is commutative and S is left cancellative, then S is also right cancellative. On the other hand, if S is cancellative, then the binary operation on S is not necessarily commutative, as we will see later.

However, it is easy to see that every group is cancellative. Moreover, for finite sets, axioms (A1) and (A2) can be replaced by just one axiom:

Proposition 1.5. Let G be a finite set with an associative operation. If G is cancellative, then G is a group.

Proof. Let $a \in G$ be arbitrary. Consider the set $aG = \{ax : x \in G\}$. It is easy to see that $|aG| \leq |G|$. On the other hand, if $|aG| < |G|$, then would find two distinct $x, y \in G$ such that $ax = ay$, and since G is left cancellative, this would imply that $x = y$, a contradiction. So, $|aG| = |G|$, which implies that $aG = G$.

Now, there must be an element $e \in G$ such that $ae = a$. Further, we have $ae = (ae)e = a(ee)$, which implies, since G is left cancellative, that $e = ee$. Let now $b \in G$ be arbitrary. We get $be = b(ee) = (be)e$, and since G is right cancellative, $be = b$, and hence, e is a right-neutral element of G.

Let $b \in G$ be arbitrary. Again, we have $bG = G$, which implies that there is a $\bar{b} \in G$ such that $b\bar{b} = e$, thus, the element $b \in G$ has a right-inverse, and since $b \in G$ was arbitrary, every element of G has a right-inverse. By Proposition 1.2 (replacing "left" by "right"), this proves that G is a group. $\dashv$

Notice that in the proof of Proposition 1.5 we used that G is both, left and right cancellative and that G is finite. In fact, we cannot do better:

Proposition 1.6.

(a) A finite set S with an associative operation which is right cancellative is not necessarily a group.

(b) An infinite set S with an associative operation which is cancellative is not necessarily a group.

Proof. (a) Let $S = \{0, 1\}$ and for $x, y \in S$ define $x * y := x$. Then the operation "$*$" is associative and S is right cancellative (since $y * x = z * x$ implies $y = z$). But S is obviously not a group (see also the proof of Proposition 1.3).

(b) Consider $(\mathbb{N}, +)$, where $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ denotes the set of natural numbers. The operation "+" is associative and $\mathbb{N}$ is cancellative (since $x + y = x + z \Leftrightarrow y = z \Leftrightarrow y + x = z + x$). But $(\mathbb{N}, +)$ is not a group, since for example 1 does not have an inverse. $\dashv$

2. Examples of Groups

2.1. **Some infinite abelian groups.** It is easy to see that the following are infinite abelian groups:

$$(\mathbb{Z},+),\ (\mathbb{Q},+),\ (\mathbb{R},+),\ (\mathbb{C},+),$$

where $\mathbb{R}$ is the set of real numbers and $\mathbb{C}$ is the set of complex numbers,

$$(\mathbb{Q}^*,\,\cdot\,),\ (\mathbb{R}^*,\,\cdot\,),\ (\mathbb{C}^*,\,\cdot\,),$$

where the star means "without 0",

$$(\mathbb{Q}^+,\,\cdot\,),\ (\mathbb{R}^+,\,\cdot\,),$$

where the plus-sign means "just positive numbers", and

$$(\mathbb{U},\,\cdot\,),$$

where $\mathbb{U} = \{z \in C : |z| = 1\}$.

Let $2^{\mathbb{Z}} := \{2^x : x \in \mathbb{Z}\} = \{1, 2, \frac{1}{2}, 4, \frac{1}{4}, 8, \frac{1}{8}, \ldots\}$, then $(2^{\mathbb{Z}},\,\cdot\,)$ is a group:

(0) Multiplication is associative (and even commutative): For all $x, y, z \in \mathbb{Z}$ we have

$$2^x \cdot \big(2^y \cdot 2^z\big) = 2^{x+(y+z)} = 2^{(x+y)+z} = \big(2^x \cdot 2^y\big) \cdot 2^z\,.$$

(1) $2^0 = 1$ is the neutral element: For all $x \in \mathbb{Z}$ we have

$$2^0 \cdot 2^x = 2^x \cdot 2^0 = 2^{x+0} = 2^x\,.$$

(2) Every element in $2^{\mathbb{Z}}$ has an inverse: For all $x \in \mathbb{Z}$ we have

$$2^{-x} \cdot 2^x = 2^x \cdot 2^{-x} = 2^{x+(-x)} = 2^0\,.$$

The groups $(2^{\mathbb{Z}},\,\cdot\,)$ and $(\mathbb{Z},+)$ are essentially the same groups. To see this, let

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & 2^{\mathbb{Z}} \\ & x & \mapsto & 2^x \end{array}$$

It is easy to see that φ is a bijection (*i.e.*, a one-to-one mapping which is onto) between $\mathbb{Z}$ and $2^{\mathbb{Z}}$. Further, $\varphi(x+y) = 2^{x+y} = 2^x \cdot 2^y = \varphi(x) \cdot \varphi(y)$, and $\varphi(0) = 2^0 = 1$. So, the image under φ of $x + y$ is the same as the product of the images of x and y, and the image of the neutral element of the group $(\mathbb{Z},+)$ is the neutral element of the group $(2^{\mathbb{Z}},\,\cdot\,)$. Thus, the only difference between $(2^{\mathbb{Z}},\,\cdot\,)$ and $(\mathbb{Z},+)$ is that the elements as well as the operations have different names. This leads to the following:

Definition. Let $(G_1,\,\circ\,)$ and $(G_2,\,\bullet\,)$ be two groups. If there exists a bijection φ between G_1 and G_2 such that for all $x, y \in G_1$ we have

$$\varphi(x \circ y) = \varphi(x) \bullet \varphi(y)\,,$$

then the groups $(G_1,\,\circ\,)$ and $(G_2,\,\bullet\,)$ are called **isomorphic**, denoted by $G_1 \cong G_2$, and the mapping φ is called an **isomorphism**.

In other words, two groups are isomorphic if they are essentially the same groups (up to renaming the elements and the operation). In particular, all groups with 1 element are isomorphic.

2.2. **Some infinite non-abelian groups.** Let $\mathrm{M}(n)$ be the set of all n by n matrices with real numbers as entries. Notice that $\big(\mathrm{M}(n), \cdot\big)$ is *not* a group, even though there exists a unique neutral element, namely the n by n **identity matrix**

$$I_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Let $\mathrm{GL}(n) := \big\{A \in \mathrm{M}(n) : \det(A) \neq 0\big\}$, then $\big(\mathrm{GL}(n), \cdot\big)$ is a group, the so-called **general linear group**. It is easy to see that $\mathrm{GL}(1)$ is isomorphic to $(\mathbb{R}^*, \cdot)$, but for $n > 1$, $\mathrm{GL}(n)$ is a non-abelian group, consider for example

$$\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ 6 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 3 & 8 \end{pmatrix}.$$

The so-called **special linear group** is $\mathrm{SL}(n) := \big\{A \in \mathrm{GL}(n) : \det(A) = 1\big\}$, where the operation is again matrix-multiplication. It is easy to see that $\mathrm{SL}(1)$ is isomorphic to $\big(\{1\}, \cdot\big)$, but for $n > 1$, $\mathrm{SL}(n)$ is non-abelian group.

The so-called **orthogonal group** is $\mathrm{O}(n) := \big\{A \in \mathrm{M}(n) : AA^t = I_n\big\}$. It is easy to see that $\mathrm{O}(1)$ is isomorphic to $\big(\{-1, 1\}, \cdot\big)$, but for $n > 1$, $\mathrm{O}(n)$ is a non-abelian group.

The so-called **special orthogonal group** is $\mathrm{SO}(n) := \big\{A \in \mathrm{O}(n) : \det(A) = 1\big\}$. It is easy to see that $\mathrm{SO}(1)$ is isomorphic to $\big(\{1\}, \cdot\big)$. Further, each $A \in \mathrm{SO}(2)$ is of the form

$$A = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

for some $\alpha \in \mathbb{R}$, and therefore, the matrices in $\mathrm{SO}(2)$ are just rotations and the group $\mathrm{SO}(2)$ is abelian. In fact, $\mathrm{SO}(2)$ is isomorphic to $(\mathbb{U}, \cdot)$. But for $n > 2$, $\mathrm{SO}(n)$ is a non-abelian group, consider for example the matrices

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

2.3. **Some finite abelian groups.** For a positive integer n, consider the set $C_n := \{a^0, a^1, \dots, a^{n-1}\}$. On C_n define a binary operation as follows:

$$a^\ell a^m = \begin{cases} a^{\ell+m} & \text{if } \ell + m < n, \\ a^{(\ell+m)-n} & \text{if } \ell + m \geq n. \end{cases}$$

For every positive integer n, C_n is an abelian group: First note that every $x \in \mathbb{Z}$ is of the form $x = sn + r$, where $s \in \mathbb{Z}$ and $r \in \{0, 1, \dots, n-1\}$, and we write $x \equiv r \pmod{n}$. In fact, $a^\ell a^m = a^r$, where $\ell + m \equiv r \pmod{n}$. Thus, $a^k\big(a^\ell a^m\big) = \big(a^k a^\ell\big)a^m = a^r$, where r is such that $k + \ell + m \equiv r \pmod{n}$, and $a^m a^\ell = a^\ell a^m$, which implies that the operation is associative and commutative.

The element a^0 is a neutral element, since $a^0 a^m = a^{0+m} = a^m$. Further, for all $s \in \mathbb{Z}$ we have $a^n = a^{sn} = a^0$, since $sn \equiv 0 \pmod{n}$. The inverse of $a^m \in C_n$ is a^{n-m}, since $a^m a^{n-m} = a^{m+(n-m)} = a^n = a^0$.

Definition. The group C_n is called the **cyclic group** of order n (since $|C_n| = n$).

2.4. **Some finite non-abelian groups.** Let X, Y and Z be three sets and let $f : X \to Y$ and $g : Y \to Z$ be two functions. The composition of f and g is a function from X to Z defined as follows:

$$(g \circ f)(x) := g\big(f(x)\big) .$$

Let $X = \{1, 2, \ldots, n\}$ be a finite set and let S_n be the set of all bijections $\sigma : X \to X$. The composition "$\circ$" of two bijections $\sigma, \tau : X \to X$ is again a bijection, and therefore, "$\circ$" is a binary operation on S_n.

The operation "$\circ$" is associative:
For every $x \in X$ and any $\sigma, \tau, \pi \in S_n$ we have

$$\begin{aligned}\big((\sigma \circ \tau) \circ \pi\big)(x) &= \big(\sigma \circ \tau\big)\big(\pi(x)\big) = \sigma\big(\tau\big(\pi(x)\big)\big)\\ \big(\sigma \circ (\tau \circ \pi)\big)(x) &= \sigma\big((\tau \circ \pi)(x)\big) = \sigma\big(\tau\big(\pi(x)\big)\big)\end{aligned}$$

The identity mapping is a bijection and a neutral element of S_n, and the inverse mapping of a bijection is also a bijection. So, S_n has a neutral element and each $\sigma \in S_n$ has an inverse, denoted by σ^{-1}, and therefore, S_n is a group.

Definition. The group S_n is called the **symmetric group** of degree n, or the **permutation group** of degree n.

Notice that $|S_n| = n!$, so, except for $n = 1$ and $n = 2$, the order of S_n is strictly greater than n. Let us consider S_n for small values of n.

S_1: $|S_1| = 1$, namely the identity mapping $\iota : 1 \mapsto 1$. Since every group with just one element is isomorphic to C_1, we have $S_1 \cong C_1$.

S_2: $|S_2| = 2$, namely the identity mapping ι and the permutation $\sigma : \begin{cases} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \end{cases}$. Since every group with just two elements is isomorphic to C_2, we have $S_2 \cong C_2$.

S_3: $|S_3| = 6$. Consider the permutations $\sigma : \begin{cases} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 3 \end{cases}$ and $\tau : \begin{cases} 1 & \mapsto & 1 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \end{cases}$.

Now,

$$\begin{aligned}(\sigma \circ \tau)(1) &= \sigma\big(\tau(1)\big) = \sigma(1) = 2 ,\\ (\tau \circ \sigma)(1) &= \tau\big(\sigma(1)\big) = \tau(2) = 3 ,\end{aligned}$$

thus, S_3 is a non-abelian group. In fact, for every $n \geq 3$, S_n is a non-abelian group.

Let us now consider a special class of groups, namely the group of rigid motions of a two or three-dimensional solid.

Definition. A **rigid motion** of a solid S is a bijection $\varphi : S \to S$ which has the following property: The solid S can be moved through 3-dimensional Euclidean space in such a way that it does not change its shape and when the movement stops, each point $p \in S$ is in position $\varphi(p)$.

Since rigid motions are special kinds of bijections, for every solid S, the set of all rigid motions of S together with composition (as operation) is a group. In this course we will investigate in depth the groups of rigid motions of the five Platonic solids, which are tetrahedron, cube, octahedron, dodecahedron, and icosahedron. But first, let us consider a simpler solid, namely a regular n-sided polygon.

DEFINITION. The group of rigid motions of a regular n-sided polygon (for $n \geq 3$) is called the **dihedral group** of degree n and is denoted by D_n.

Let us consider first D_3: D_3 has 6 elements, namely the identity ι, two non-trivial rotations say ρ_1 and ρ_2, and three reflections say σ_1, σ_2, and σ_3. If we label the vertices of the regular triangle with 1, 2, and 3, then every permutation of $\{1,2,3\}$ corresponds to an element of D_3, and since $|D_3| = 6 = |S_3|$, $D_3 \cong S_3$. In particular, D_3 is a non-abelian group. In fact, for every $n \geq 3$, D_n is a non-abelian group.

2.5. **Representing finite groups by multiplication tables.** Let $S = \{a, b, c, \ldots\}$ be a finite set with some binary operation "$\circ$". Then the following table is the so-called multiplication table of S:

$\circ$	a	b	c	$\cdots$
a	$a \circ a$	$a \circ b$	$a \circ c$	$\cdots$
b	$b \circ a$	$b \circ b$	$b \circ c$	$\cdots$
c	$c \circ a$	$c \circ b$	$\cdots$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

For example, the multiplication table of $C_4 = \{e, a, a^2, a^3\}$, where $e = a^0$, is as follows:

$\circ$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

A multiplication table of a group is often called its **Cayley table**. Note that not every multiplication table is a Cayley table (see Hw3.Q11).

2.6. **Products of groups.** Let $(G, *_G)$ and $(H, *_H)$ be any groups (not necessarily finite groups), then

$$G \times H := \big\{ \langle x, y \rangle : x \in G \text{ and } y \in H \big\} .$$

On the set $G \times H$ we define an operation "$\circ$" as follows:

$$\langle x_1, y_1 \rangle \circ \langle x_2, y_2 \rangle := \langle x_1 *_G x_2, y_1 *_H y_2 \rangle .$$

It is easy to verify that $(G \times H, \circ)$ is a group and that it is abelian if and only if G and H are both abelian (see Hw3.Q12).

Let us consider the abelian group $C_2 \times C_2$: By definition we have $|C_2 \times C_2| = |C_2| \cdot |C_2| = 4$. Let $C_2 = \{a^0, a^1\}$ and let $e = \langle a^0, a^0 \rangle$, $x = \langle a^0, a^1 \rangle$, $y = \langle a^1, a^0 \rangle$, and $z = \langle a^1, a^1 \rangle$. In this notation, $C_2 \times C_2$ has the following Cayley table:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

It is easy to see that $C_2 \times C_2$ is not isomorphic to C_4 and we will see later that these two groups are essentially the only groups of order 4. If p and q are positive integers such that $\gcd(p, q) = 1$, then $C_p \times C_q \cong C_{pq}$ (see Hw3.Q14.a), but in general, $C_p \times C_q$ is not isomorphic to C_{pq}, *e.g.*, let $p = q = 2$ (see also Hw3.Q14.b).

3. Subgroups

Definition. Let G be a group. A non-empty set $H \subseteq G$ is a **subgroup** of G if for all $x, y \in H$, $x\,y^{-1} \in H$.

Notation. If H is a subgroup of G, then we write $H \leqslant G$. If $H \neq G$ is a subgroup of G, then we write $H < G$ and call H a **proper subgroup** of G.

Proposition 3.1. If $H \leqslant G$, then H is a group.

Proof. We have to show that H satisfies (A0), (A1), and (A2):

(A1) Let $x \in H$, then by definition, $x\,x^{-1} = e \in H$, so, the neutral element $e \in H$.
(A2) Let $x \in H$, then by definition $e\,x^{-1} = x^{-1} \in H$.
(A0) Let $x, y \in H$, then also $y^{-1} \in H$, and by definition $x(y^{-1})^{-1} = xy \in H$.

$\dashv$

Definition. The subgroups $\{e\}$ and G are called the **trivial subgroups** of G.

Proposition 3.2. The intersection of arbitrarily many subgroups of a group G is again a subgroup of G.

Proof. Let Λ be any set and assume that for every $\lambda \in \Lambda$, $H_\lambda \leqslant G$. Let

$$H = \bigcap_{\lambda \in \Lambda} H_\lambda\,,$$

and take any $x, y \in H$. Then, for every $\lambda \in \Lambda$, $x, y \in H_\lambda$, and thus, for every $\lambda \in \Lambda$, $x\,y^{-1} \in H_\lambda$. Thus, $x\,y^{-1} \in H$, and since $x, y \in H$ were arbitrary, $H \leqslant G$. $\dashv$

Definition. Let G be a group with neutral element e and let $x \in G$. Then the least positive integer n such that $x^n = e$ is called the **order of** x, denoted by $\mathrm{ord}(x)$. If there is no such integer, then the order of x is "∞".

The order of an element x of a finite group G is well-defined: Because the set $\{x^1, x^2, x^3, \ldots\} \subseteq G$ is finite, there are $0 < n < m$ such that $x^n = x^m = x^n\,x^{m-n}$, which implies $e = x^{m-n}$, where $m - n$ is a positive integer.

Definition. For a group G and a set $X \subseteq G$, let

$$\big\langle X \big\rangle := \bigcap_{\substack{H \leqslant G \\ X \subseteq H}} H\,.$$

By Proposition 3.2, $\big\langle X \big\rangle$ is a subgroup of G and it is called the subgroup **generated by** X. If $X = \{x\}$, then we write just $\langle x \rangle$ instead of $\big\langle \{x\} \big\rangle$.

Fact 3.3. If G is a group and $x \in G$ of order n, then $\langle x \rangle$ is a cyclic group (*i.e.*, subgroup of G) of order n.

Proof. The group $\langle x \rangle$ consists of the elements $x^1, x^2, \ldots, x^n$, where $x^n = e$. On the other hand, $\{x^1, x^2, \ldots, x^n\}$ is a cyclic group of order n. $\dashv$

This leads to the following:

Corollary 3.4. Let G be a group. If $x \in G$ is of finite order, then $\mathrm{ord}(x) = |\langle x \rangle|$.

Theorem 3.5. Subgroups of cyclic groups are cyclic.

Proof. Let $C_n = \{a^0, a^1, \dots, a^{n-1}\}$ be a cyclic group of order n (for some positive integer n) and let $H \leqslant C_n$. If $H = \{a^0\}$, then we are done. So, let us assume that $a^m \in H$, where $m \in \{1, \dots, n-1\}$. Take the least such m. Evidently, we have $\langle a^m \rangle \leqslant H$. Now, let $h \in H$ be arbitrary. Since $h \in C_n$, there is a $k \in \{0, 1, \dots, n-1\}$ such that $h = a^k$. Write k in the form $k = \ell m + r$, where $\ell, r \in \mathbb{N}$ and $0 \leq r < m$. Now,

$$\underbrace{(a^m)^{-1} \cdots (a^m)^{-1}}_{\ell\text{-times}} = (a^m)^{-\ell} \in H\,,$$

and therefore, $h(a^m)^{-\ell} = a^k(a^m)^{-\ell} = a^r \in H$. Thus, by the choice of m, we must have $r = 0$, which implies that $h \in \langle a^m \rangle$. Since $h \in H$ was arbitrary, this implies $H \leqslant \langle a^m \rangle$ and completes the proof. ⊣

Definition. For $H \leqslant G$ and $x \in G$, let

$$xH := \{xh : h \in H\} \quad \text{and} \quad Hx := \{hx : h \in H\}\,.$$

The sets xH and Hx are called **left cosets** and **right cosets** of H in G (respectively).

In the sequel, left and right cosets will play an important role and we will use the following lemma quite often.

Lemma 3.6 (left-version). Let G be a group, $H \leqslant G$ and let $x, y \in G$ be arbitrary.
(a) $|xH| = |H|$, in other words, there exists a bijection between H and xH.
(b) $x \in xH$.
(c) $xH = H$ if and only if $x \in H$.
(d) $xH = yH$ if and only if $x^{-1}y \in H$.
(e) $xH = \{g \in G : gH = xH\}$.

Proof. (a) Define the function $\varphi_x : H \to xH$ by stipulating $\varphi_x(h) := xh$. We have to show that φ_x is a bijection. If $\varphi_x(h_1) = \varphi_x(h_2)$ for some $h_1, h_2 \in H$, *i.e.*, $xh_1 = xh_2$, then $xh_1h_2^{-1} = xh_2h_2^{-1} = xe = x$, which implies $h_1h_2^{-1} = e$, and consequently, $h_1 = h_2$. Thus, the mapping φ_x is injective (*i.e.*, one-to-one). On the other hand, every element in xH is of the form xh (for some $h \in H$), and since $xh = \varphi_x(h)$, the mapping φ_x is also surjective (*i.e.*, onto), thus, φ_x is a bijection between H and xH.

(b) Since $e \in H$, $xe = x \in xH$.

(c) If $xH = H$, then, since $e \in H$, $xe = x \in H$. For the other direction assume that $x \in H$: Because H is a group we have $xH \subseteq H$. Further, take any element $h \in H$. Since $x^{-1} \in H$ we have $x^{-1}h \in H$ and therefore $xH \ni x(x^{-1}h) = h$, which implies $xH \supseteq H$. Thus, we have $xH \subseteq H \subseteq xH$ which shows that $xH = H$.

(d) If $xH = yH$, then

$$\underbrace{x^{-1}xH}_{=H} = x^{-1}yH \overset{\text{by (c)}}{\Longrightarrow} x^{-1}y \in H\,.$$

If $x^{-1}y \in H$, then by (c) we have $x^{-1}yH = H$, and therefore, $\underbrace{xx^{-1}yH}_{yH} = xH$.

(e) If $g \in xH$, then $g = xh$ for some $h \in H$, and hence, $gH = xhH = xH$. Therefore, $xH \subseteq \{g \in G : gH = xH\}$. Conversely, if $xH = gH$ for some $g \in G$, then by (b), $g \in xH$, which implies $\{g \in G : gH = xH\} \subseteq xH$ and completes the proof. ⊣

Obviously, there exists also a right-version of Lemma 3.6, which is proved similarly. As a consequence of Lemma 3.6 (b), combining left-version and right-version, we get:

COROLLARY 3.7. Let $H \leqslant G$, then

$$\bigcup_{x \in G} xH = G = \bigcup_{x \in G} Hx \,.$$

The following lemma is a consequence of Lemma 3.6 (d):

LEMMA 3.8 (left-version). Let $H \leqslant G$, then for any $x, y \in G$ we have either $xH = yH$ or $xH \cap yH = \emptyset$.

Proof. Either $xH \cap yH = \emptyset$ (and we are done) or there exists a $z \in xH \cap yH$. If $z \in xH \cap yH$, then $z = xh_1 = yh_2$ (for some $h_1, h_2 \in H$), thus, $x^{-1}z \in H$ and $z^{-1}y \in H$. Since H is a group, we get $(x^{-1}z)(z^{-1}y) = x^{-1}y \in H$, which implies by Lemma 3.6 (d) that $xH = yH$. ⊣

Obviously, there exists also a right-version of Lemma 3.8, which is proved similarly.

DEFINITION. For a subgroup $H \leqslant G$ let

$$G/H := \{xH : x \in G\} \quad \text{and} \quad H\backslash G := \{Hx : x \in G\} \,.$$

DEFINITION. A **partition** of a set S is a collection of pairwise disjoint non-empty subsets of S such that the union of these subsets is S.

As a consequence of Lemma 3.6 (a), Corollary 3.7 and Lemma 3.8 (left-versions and right-versions) we get:

COROLLARY 3.9. Let $H \leqslant G$, then G/H as well as $H\backslash G$ is a partition of G, where each part has the same order as H.

DEFINITION. Let $H \leqslant G$, then $|G/H| = |H\backslash G|$ is called the **index** of H in G and is written $|G : H|$.

As a consequence of Corollary 3.9 we get:

COROLLARY 3.10. Let G be a group and let $H \leqslant G$. If $|G : H| = 2$, then for all $x \in G$ we have $xH = Hx$.

Proof. If $x \in H$, then $xH = Hx = H$ (since H is a group). Now, let $x \in G$ be not in H. By Corollary 3.9 we have $G = H \cup xH$ and $G = H \cup Hx$, where $H \cap xH = \emptyset = H \cap Hx$, which implies $xH = Hx$. ⊣

If $H \leqslant G$, then in general we do not have $xH = Hx$ (for all $x \in G$). For example, let C be the cube-group and let D_4 be the dihedral group of degree 4. It is easy to see that $D_4 \leqslant C$ and that the index of D_4 in C is 3. Now, holding a cube in your hand, it should not take too long to find a rotation $\rho \in C$ such that $\rho D_4 \neq D_4 \rho$.

THEOREM 3.11. Let G be a (finite) group and let $H \leqslant G$, then $|G| = |G : H| \cdot |H|$. In particular, for finite groups we get $|H|$ divides $|G|$.

Proof. Consider the partition G/H of G. This partition has $|G : H|$ parts and each part has size $|H|$ (by Lemma 3.6 (a)), and thus, $|G| = |G : H| \cdot |H|$. In particular, if $|G|$ is finite, $|H|$ divides $|G|$. ⊣

Corollary 3.12. If G is a finite group of order p, for some prime number p, then G is a cyclic group. In particular, G is abelian.

Proof. For every $x \in G$, $\langle x \rangle$ is a subgroup of G, hence, by Theorem 3.11, $|\langle x \rangle|$ divides $p = |G|$, which implies $|\langle x \rangle| = 1$ or $|\langle x \rangle| = p$. Now, $|\langle x \rangle| = 1$ iff $x = e$. So, if $x \neq e$, then $|\langle x \rangle| = p$, which implies $\langle x \rangle = G$. Hence, G is cyclic, and since cyclic groups are abelian, G is abelian. ⊣

Definition. A **transversal** for a partition is a set which contains exactly one element from each part of the partition. For $H \leqslant G$, a transversal for the partition G/H $(H\backslash G)$ is called a **left (right) transversal** for H in G.

For example, let $G = (\mathbb{C}^*, \cdot\,)$ and $H = (\mathbb{U}, \cdot\,)$, where $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$. First notice that the set $\mathbb{C}^*/\mathbb{U}$ consists of concentric circles. So, an obvious (left or right) transversal for $\mathbb{U}$ in $\mathbb{C}^*$ is $\mathbb{R}^+$, which is even a subgroup of $\mathbb{C}^*$. Another (left or right) transversal for $\mathbb{U}$ in $\mathbb{C}^*$ is $\mathbb{R}^- = \{x \in \mathbb{R} : x < 0\}$, which is not a subgroup of $\mathbb{C}^*$, but there are many other choices of transversals available.

If H is a subgroup of G and $x \in G$, then, as we have seen above, in general $xH \neq Hx$. This implies that a left transversal for H in G is not necessarily also a right transversal. However, by Lemma 3.6, it is straightforward to transform a left transversal into a right transversal:

Proposition 3.13. Let $H \leqslant G$ and let $\{a_0, a_1, \ldots\}$ be a left transversal for H in G, then $\{a_0^{-1}, a_1^{-1}, \ldots\}$ is a right transversal for H in G.

Proof. Let x and y be two distinct elements of $\{a_0, a_1, \ldots\}$. Since $\{a_0, a_1, \ldots\}$ is a left transversal for H in G, we have $xH \neq yH$, and by Lemma 3.6 (left and right version) we get:

$$\begin{aligned} x^{-1}y \notin H \iff (x^{-1}y)^{-1} \notin H \iff y^{-1}x \notin H \iff \\ \iff H \neq Hy^{-1}x \iff Hx^{-1} \neq Hy^{-1}\,. \end{aligned}$$

Hence, $xH \neq yH$ if and only if $Hx^{-1} \neq Hy^{-1}$, and since x and y were arbitrary, this shows that $\{a_0^{-1}, a_1^{-1}, \ldots\}$ is a right transversal for H in G. ⊣

4. The Groups $(\mathbb{Z}_m, +)$ and $(\mathbb{Z}_p^*, \cdot)$

For $m \in \mathbb{Z}$, let $m\mathbb{Z} = \{mx : x \in Z\}$, then, by Hw2.Q6.(d), $m\mathbb{Z} \leqslant (\mathbb{Z}, +)$. In the sequel we investigate the sets $\mathbb{Z}/m\mathbb{Z}$ for positive integers m.

The set $\mathbb{Z}/m\mathbb{Z}$ contains m pairwise disjoint "copies" of $m\mathbb{Z}$ and every set in $\mathbb{Z}/m\mathbb{Z}$ is of the form $x + m\mathbb{Z}$, for some $x \in \mathbb{Z}$. If $x + m\mathbb{Z} = y + m\mathbb{Z}$, then, by Lemma 3.6 (d), $x - y \in m\mathbb{Z}$, so, $x - y = km$ for some $k \in \mathbb{Z}$. Hence,

$$x + m\mathbb{Z} = y + m\mathbb{Z} \iff x = km + y \iff x \equiv y \pmod{m}.$$

Instead of $x \equiv y \pmod{m}$ we write just $x \equiv_m y$.
It is easy to see that $\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}$, and hence,

$$\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$$

is a transversal for $m\mathbb{Z}$ in $\mathbb{Z}$. In particular, for every $x + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ there is exactly one $a \in \mathbb{Z}_m$ such that $x + m\mathbb{Z} = a + m\mathbb{Z}$, namely the unique $a \in \mathbb{Z}_m$ such that $x \equiv_m a$. Let us define an operation "$+$" on $\mathbb{Z}/m\mathbb{Z}$ as follows:

$$\begin{array}{rccc} + : & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \\ & (x + m\mathbb{Z}\,,\, y + m\mathbb{Z}) & \mapsto & (x + y) + m\mathbb{Z} \end{array}$$

It remains to show that "$+$" is an operation on $\mathbb{Z}/m\mathbb{Z}$, or in other words, that "$+$" is well defined:

Fact 4.1. If $x + m\mathbb{Z} = x' + m\mathbb{Z}$ and $y + m\mathbb{Z} = y' + m\mathbb{Z}$, then $(x + m\mathbb{Z}) + (y + m\mathbb{Z}) = (x' + m\mathbb{Z}) + (y' + m\mathbb{Z})$.

Proof. If $x + m\mathbb{Z} = x' + m\mathbb{Z}$ and $y + m\mathbb{Z} = y' + m\mathbb{Z}$, then, by Lemma 3.6 (d), $x' - x \in m\mathbb{Z}$ and $y' - y \in m\mathbb{Z}$. Now, $(x + m\mathbb{Z}) + (y + m\mathbb{Z}) = (x + y) + m\mathbb{Z}$, and therefore, by Lemma 3.6 (c), $(x + y) + m\mathbb{Z} = (x + y) + \big((x' - x) + (y' - y) + m\mathbb{Z}\big) = (x' + y') + m\mathbb{Z} = (x' + m\mathbb{Z}) + (y' + m\mathbb{Z})$. Thus, $(x + m\mathbb{Z}) + (y + m\mathbb{Z}) = (x' + m\mathbb{Z}) + (y' + m\mathbb{Z})$, which shows that the operation "$+$" on $\mathbb{Z}/m\mathbb{Z}$ is well defined. ⊣

The following fact is straightforward:

Fact 4.2. $\big(\mathbb{Z}/m\mathbb{Z}, +\big)$ is an abelian group.

Since every element of $\mathbb{Z}/m\mathbb{Z}$ is of the form $a + m\mathbb{Z}$ for some $a \in \mathbb{Z}_m$, let us identify the set $\mathbb{Z}/m\mathbb{Z}$ with the set $\mathbb{Z}_m$. This identification induces an operation "$+$" on $\mathbb{Z}_m$:

$$\begin{array}{rccc} + : & \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m \\ & (a\,,\, b) & \mapsto & a + b =: c \end{array}$$

where $c \in \mathbb{Z}_m$ is such that $a + b \equiv_m c$. So, by Fact 4.2, $(\mathbb{Z}_m, +)$ is an abelian group.

Since every integer $x \in \mathbb{Z}$ belongs to exactly one coset of $\mathbb{Z}/m\mathbb{Z}$, each $x \in \mathbb{Z}$ corresponds to exactly one element of $\mathbb{Z}_m$, say to $(x)_m \in \mathbb{Z}_m$. Now, by Fact 4.1, if $(x)_m = (x')_m$ and $(y)_m = (y')_m$, which is the same as $x \equiv_m x'$ and $y \equiv_m y'$, then $(x + y)_m = (x' + y')_m$. Moreover, we get

$$(x)_m = (x')_m \text{ and } (y)_m = (y')_m \implies (x \cdot y)_m = (x' \cdot y')_m\,,$$

or in other words,

$$x \equiv_m x' \text{ and } y \equiv_m y' \implies x \cdot y \equiv_m x' \cdot y'\,.$$

Proposition 4.3. The group $(\mathbb{Z}_m, +)$ is a cyclic group of order m.

Proof. By definition, $|\mathbb{Z}_m| = m$. Now, since the order of 1 is m, we have $\langle 1\rangle = \mathbb{Z}_m$ which implies that $\mathbb{Z}_m$ is cyclic. $\dashv$

Multiplication is also an operation on $\mathbb{Z}_m$ and for all $a, b, c \in \mathbb{Z}_m$ we have $a\cdot(b+c) = (a \cdot b) + (a \cdot c)$, which is called the **distributive law**.

In the following, let $m \geq 2$ and let $\mathbb{Z}_m^* := \mathbb{Z}_m \setminus \{0\} = \{1, \dots, m-1\}$. Is $(\mathbb{Z}_m^*, \cdot\,)$ a group?

Lemma 4.4. $(\mathbb{Z}_m^*, \cdot\,)$ is a group if and only if multiplication is an operation on $\mathbb{Z}_m^*$.

Proof. ($\Leftarrow$) If multiplication is an operation on $\mathbb{Z}_m^*$, then it is obviously associative and even commutative. Let us assume that multiplication is an operation on $\mathbb{Z}_m^*$. Suppose $a \cdot b \equiv_m a \cdot c$ (for some $a, b, c \in \mathbb{Z}_m^*$), then $(a \cdot b) - (a \cdot c) \equiv_m 0$, and thus, by the distributive law, $a \cdot (b - c) \equiv_m 0$. Now, $0 \notin \mathbb{Z}_m^*$, and since we assumed that multiplication is an operation on $\mathbb{Z}_m^*$, we must have $(b - c) \equiv_m 0$, which implies $b \equiv_m c$, and since $b, c \in \mathbb{Z}_m$, we get $b = c$. Because multiplication is commutative, this shows that $(\mathbb{Z}_m^*, \cdot\,)$ is cancellative. So, by Proposition 1.5 (since $\mathbb{Z}_m^*$ is finite), $(\mathbb{Z}_m^*, \cdot\,)$ is a group.
($\Rightarrow$) This is obvious. $\dashv$

Theorem 4.5. $(\mathbb{Z}_p^*, \cdot\,)$ is a group if and only if p is a prime number.

Proof. ($\Rightarrow$) If p is not a prime number, then there are $n, m \in \mathbb{Z}_p^*$ such that $p = n \cdot m$. Thus, $n \cdot m = p \equiv_p 0 \notin \mathbb{Z}_p^*$, which implies that multiplication is not an operation on $\mathbb{Z}_p^*$. Hence, by Lemma 4.4, $(\mathbb{Z}_p^*, \cdot\,)$ is not a group.
($\Leftarrow$) Suppose p is prime and let $n, m \in \mathbb{Z}_p^*$. So, $1 \leq n, m < p$, which implies that p neither divides n nor m. Now, since p is prime, $p \nmid n \cdot m$, which is the same as saying $n \cdot m \not\equiv_m 0$. Hence, multiplication is an operation on $\mathbb{Z}_p^*$ and by Lemma 4.4, $(\mathbb{Z}_p^*, \cdot\,)$ is a group. $\dashv$

In fact, for every prime number p, $(\mathbb{Z}_p^*, \cdot\,)$ is even a cyclic group, or in other words, there is always an element in $(\mathbb{Z}_p^*, \cdot\,)$ of order $p - 1$ (we omit the proof).

Lemma 4.6. If p is prime, then for each $k \in \mathbb{Z}_p^*$ we have $k^{p-1} \equiv_p 1$.

Proof. We work in $(\mathbb{Z}_p^*, \cdot\,)$. Let $k \in \mathbb{Z}_p^*$, then $\langle k\rangle$ is a cyclic subgroup of $(\mathbb{Z}_p^*, \cdot\,)$, and since $|(\mathbb{Z}_p^*, \cdot\,)| = p - 1$, by Theorem 3.11 we get that $\mathrm{ord}(k) = |\langle k\rangle|$ divides $p - 1$. So, there is some positive integer ℓ such that $\ell \cdot \mathrm{ord}(k) = p - 1$. Now, in $\mathbb{Z}_p^*$ we have

$$k^{p-1} = k^{\ell\cdot\mathrm{ord}(k)} = \left(k^{\mathrm{ord}(k)}\right)^{\ell} = 1^{\ell} = 1\,,$$

which implies $k^{p-1} \equiv_p 1$. $\dashv$

Let us conclude this section with Fermat's little theorem:

Theorem 4.7. If p is prime and n is a positive integer such that $p \nmid n$, then

$$p \mid n^{p-1} - 1\,.$$

Proof. We work in $(\mathbb{Z}_p^*, \cdot\,)$. $|(\mathbb{Z}_p^*, \cdot\,)| = p - 1$ and by Lemma 4.6, for every $k \in \mathbb{Z}_p^*$ we have $k^{p-1} \equiv_p 1$. Now, if $k \equiv_p n$, then $k^{p-1} \equiv_p n^{p-1}$. In particular, if $n \not\equiv_p 0$ (or equivalently, if $p \nmid n$), then $n^{p-1} \equiv_p 1$. Hence, $n^{p-1} - 1 \equiv_p 0$, or in other words, $p \mid n^{p-1} - 1$. $\dashv$

5. Normal Subgroups

Before we define the notion of a normal subgroup, let us prove the following:

Fact 5.1. Let G be a group. If $H \leqslant G$ and $x \in G$, then

$$xHx^{-1} = \{xhx^{-1} : h \in H\}$$

is a subgroup of G.

Proof. Let xh_1x^{-1} and xh_2x^{-1} be in xHx^{-1}. Then $\left(xh_2x^{-1}\right)^{-1} = xh_2^{-1}x^{-1}$ and $\left(xh_1x^{-1}\right)\left(xh_2^{-1}x^{-1}\right) = x\left(h_1h_2^{-1}\right)x^{-1} \in xHx^{-1}$. So, by definition, $xHx^{-1} \leqslant G$. ⊣

This leads to the following definition.

Definition. Suppose that G is a group and that $N \leqslant G$, then N is called a **normal subgroup** of G if for all $x \in G$ we have

$$xNx^{-1} = N\,,$$

or equivalently, if for all $x \in G$, $xN = Nx$.

In particular, the trivial subgroups are normal and all subgroups of an abelian group are normal.

Notation. If $N \leqslant G$ ($N < G$) is a normal subgroup of G, then we write $N \trianglelefteq G$ ($N \triangleleft G$).

The following is just a consequence of Corollary 3.10:

Fact 5.2. If $H < G$ and $|G : H| = 2$, then $H \triangleleft G$.

Proof. By Corollary 3.10 we know that if $|G : H| = 2$, then for all $x \in G$ we have $xH = Hx$, and therefore $H \triangleleft G$. ⊣

Proposition 5.3. If $N \leqslant G$, then $N \trianglelefteq G$ if and only if for all $x \in G$ and all $n \in N$ we have

$$xnx^{-1} \in N\,.$$

Proof. If $N \trianglelefteq G$, then $xNx^{-1} = N$ (for all $x \in G$), thus, $xnx^{-1} \in N$ for all $x \in G$ and $n \in N$.
On the other hand, if $xnx^{-1} \in N$ for all $x \in G$ and $n \in N$, then $xNx^{-1} \subseteq N$ (for all $x \in G$). Further, replacing x by x^{-1} we get

$$N = x\underbrace{\left(x^{-1}Nx\right)}_{\subseteq N}x^{-1} \subseteq xNx^{-1}\,.$$

Hence, $xNx^{-1} = N$ (for all $x \in G$). ⊣

The following Fact is similar to Proposition 3.2:

Fact 5.4. If $K, H \trianglelefteq G$, then $(K \cap H) \trianglelefteq G$.

Proof. If $K, H \trianglelefteq G$, then, by Proposition 5.3, for all $x \in G$ and $n \in K \cap H$ we have $xnx^{-1} \in K$ (since $K \trianglelefteq G$) and $xnx^{-1} \in H$ (since $H \trianglelefteq G$), and therefore, $xnx^{-1} \in K \cap H$ (for all $x \in G$ and $n \in K \cap H$). ⊣

Notice that if $H \lhd K \lhd G$, then H is not necessarly a normal subgroup of G. To see this, let T be the tetrahedron-group, let ρ_1, ρ_2 and ρ_3 be the three elements of T of order 2, and let ι be the neutral element of T. Further, let $H = \{\iota, \rho_1\}$ and $K = \{\iota, \rho_1, \rho_2, \rho_3\}$. Since the group K is isomorphic to $C_2 \times C_2$, it is abelian and therefore we get $H \lhd K$. Further, for each $\tau \in T$ and $\rho \in K$, $\tau\rho\tau^{-1}$ has either order 1 or 2. Thus, $\tau\rho\tau^{-1} \in K$, which implies by Proposition 5.3 that $K \lhd T$. Finally, it is not hard to see that H is not a normal subgroup of T.

Let us now give some examples of normal subgroups:

(1) $T \lhd C$ (since $|C : T| = 2$).
(2) For $n \geq 3$, $C_n \lhd D_n$ (since $|D_n : C_n| = 2$).
(3) For $n \geq 1$, $\mathrm{SO}(n) \lhd \mathrm{O}(n)$ (since $|\mathrm{O}(n) : \mathrm{SO}(n)| = 2$).
(4) As we have seen above, T contains a normal subgroup which is isomorphic to $C_2 \times C_2$.
(5) For $n \geq 1$, $\mathrm{SL}(n) \lhd \mathrm{GL}(n)$: For all $B \in \mathrm{GL}(n)$ and $A \in \mathrm{SL}(n)$ we have $\det\left(BAB^{-1}\right) = \det(A) = 1$, thus, $BAB^{-1} \in \mathrm{SO}(n)$.

Definition. Suppose that G is a group. We define the **centre** $Z(G)$ of G by

$$Z(G) := \left\{a \in G : \forall x \in G(ax = xa)\right\}.$$

In other words, $Z(G)$ consists of those elements of G which commute with every element of G.

Fact 5.5. $Z(G) = G$ if and only if G is abelian.

Proof. If G is abelian, then for all $a \in G$ and for all $x \in G$ we have $ax = xa$, thus, $Z(G) = G$. On the other hand, $Z(G) = G$ implies that for all $a \in G$ and for all $x \in G$, $ax = xa$, thus, G is abelian. ⊣

Fact 5.6.

(a) $Z(G) \leqslant G$ (see Hw7.Q31.a).
(b) $Z(G) \trianglelefteq G$ (see Hw7.Q31.b).
(c) $Z(G)$ is abelian (see Hw7.Q31.c).
(d) If $H \leqslant Z(G)$, then $H \trianglelefteq G$ (see Hw7.Q31.d).

It is possible that the centre of a group is just the neutral element, *e.g.*, $Z(T) = \{\iota\}$.

Definition. Let G be a group and let H and K be subgroups of G. If $G = HK$, then we say that G is the **inner product** of H and K.

Proposition 5.7. Let G be a finite group and let $H, K \leqslant G$. Then

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

Proof. First notice that $HK = \bigcup_{h \in H} hK$ and that $(H \cap K) \leqslant H$.

Now, for $h_1, h_2 \in H$ we have

$$h_1 K = h_2 K \iff h_1 h_2^{-1} \in K,$$

and further we have

$$h_1(H \cap K) = h_2(H \cap K) \iff h_1 h_2^{-1} \in (H \cap K) \iff h_1 h_2^{-1} \in K.$$

Therefore,

$$|HK| = \Big|\bigcup_{h\in H} hK\Big| = \big|H : (H\cap K)\big| \cdot |K| = \frac{|H|}{|H\cap K|}\cdot |K| = \frac{|H|\cdot|K|}{|H\cap K|}\,.$$

⊣

Notice that if H and K are subgroups of a group G, then HK is not necessarly a subgroup of G (see Hw7.Q34). On the other hand, if at least one of these two subgroups is a normal subgroup, then HK is a subgroup of G:

THEOREM 5.8. If $K \leqslant G$ and $N \trianglelefteq G$, then $KN = NK \leqslant G$.

Proof. Let us first show that $KN = NK$: Let $k \in K$ and $n \in N$, and let $n_1 = knk^{-1}$ and $n_2 = k^{-1}nk$. Then, since $N \trianglelefteq G$, $n_1, n_2 \in N$, and further we have

$$kn = n_1k \;\; \textit{and} \;\; nk = kn_2\,,$$

which shows that $KN = NK$. To see that $KN \leqslant G$, pick two elements (k_1n_1) and (k_2n_2) of KN. We have to show that $(k_1n_1)(k_2n_2)^{-1} \in KN$:

$$(k_1n_1)(k_2n_2)^{-1} = k_1\underbrace{n_1n_2^{-1}}_{=n_3\in N}k_2^{-1} = \underbrace{k_1k_2^{-1}}_{=k\in K}\underbrace{k_2n_3k_2^{-1}}_{=n\in N} = kn \in KN\,.$$

⊣

Let us give an example for Theorem 5.8: Consider the cube-group C. Let a, b, and c be the three axes joining centres of opposite faces and let $\rho_a, \rho_b, \rho_c \in C$ be the rotations about the axes a, b, and c respectively through π and let $\delta \in C$ be the rotation about the axis a through $\pi/2$. Now, let $N = \langle\{\rho_a, \rho_b, \rho_c\}\rangle$ and let $K = \langle\delta\rangle$. It is easy to see that K and N are both subgroups of C of order 4. Notice that $K \cong C_4$ and that $N \cong C_2 \times C_2$, so, K and N are not isomorphic, but they are both abelian. Let us now show that N is a normal subgroup of C: For this, we consider the set of axes $\{a, b, c\}$. Now, every $x \in C$ corresponds to a permutation τ_x on $\{a, b, c\}$, and $n \in N$ if and only if $\tau_n(a) = a$, $\tau_n(b) = b$, and $\tau_n(c) = c$, or in other words, $n \in N$ iff n corresponds to the identity permutation on $\{a, b, c\}$. For any $x \in C$ and $n \in N$, the permutation $\tau_{xnx^{-1}} = \tau_x\tau_n\tau_{x^{-1}}$ is the identity permutation on $\{a, b, c\}$, and hence, $xnx^{-1} \in N$, which shows that $N \lhd C$. Thus, by Theorem 5.8, $KN \leqslant C$. Since $|K \cap N| = 2$, by Proposition 5.7 we have $|KN| = \frac{|K|\cdot|N|}{|K\cap N|} = 8$ and it is not hard to see that $KN \cong D_4$.

PROPOSITION 5.9. If K and H are subgroups of the finite group G, $|H \cap K| = 1$ and $|H| \cdot |K| = |G|$, then $HK = G = KH$.

Proof. Let us just prove that $HK = G$ (to show that $KH = G$ is similar). Since $HK = \{hk : h \in H \textit{ and } k \in K\} \subseteq G$, $HK = G$ if and only if $|HK| = |G|$, which implies that $h_1k_1 = h_2k_2$ if and only if $h_1 = h_2$ and $k_1 = k_2$. So, let us assume that $h_1k_1 = h_2k_2$, then $h_1^{-1}(h_1k_1)k_2^{-1} = h_1^{-1}(h_2k_2)k_2^{-1}$, and hence, $k_1k_2^{-1} = h_1^{-1}h_2 \in H \cap K$, but since $H \cap K = \{e\}$, this implies that $h_1 = h_2$ and $k_1 = k_2$. ⊣

The following proposition shows that if K and H are normal subgroups of G such that $|H \cap K| = 1$, then the elements of H commute with the elements of K and vice versa. Notice that this is stronger than just saying $KH = HK$.

Proposition 5.10. If K and H are normal subgroups of G and $|H \cap K| = 1$, then for all $h \in H$ and all $k \in K$, $hk = kh$.

Proof. Let $h \in H$ and $k \in K$. Consider the element $hkh^{-1}k^{-1}$: On the one hand we have

$$\underbrace{h\overbrace{kh^{-1}k^{-1}}^{\in H}}_{\in H} \in H\,,$$

and on the other hand we have

$$\underbrace{\overbrace{hkh^{-1}}^{\in K}k^{-1}}_{\in K} \in K\,.$$

Thus, $hkh^{-1}k^{-1} \in H \cap K$, and since $|H \cap K| = 1$, $hkh^{-1}k^{-1} = e$, which implies $kh = hkh^{-1}k^{-1}(kh) = hk$. ⊣

Proposition 5.11. If K and H are normal subgroups of G, then $KH \trianglelefteq G$.

Proof. For any $x \in G$, $xkhx^{-1} = \underbrace{(xkx^{-1})}_{\in K}\underbrace{(xhx^{-1})}_{\in H} \in KH$, thus, $xKHx^{-1} = KH$. ⊣

Definition. A group G is called **simple** if it does not contain any non-trivial normal subgroup.

In particular, any abelian group which has a non-trivial subgroup cannot be simple, but there are also simple abelian groups, *e.g.*, the cyclic groups C_p, where p is prime (see Hw7.Q35). An example of a simple group which is not abelian is the dodecahedron-group D (as we will see later). On the other hand, there are many non-abelian groups which are not simple groups:

(1) The cube-group C, because $T \lhd C$.
(2) D_n for $n \geq 3$, because $C_n \lhd D_n$.
(3) $\mathrm{O}(n)$ for $n \geq 2$, because $\mathrm{SO}(n) \lhd \mathrm{O}(n)$.
(4) The tetrahedron-group T, because T contains a normal subgroup which is isomorphic to $C_2 \times C_2$.
(5) $\mathrm{GL}(n)$ for $n \geq 2$, because $\mathrm{SL}(n) \lhd \mathrm{GL}(n)$.

6. The Homomorphism Theorems

In this section, we investigate maps between groups which preserve the group-operations.

Definition. Let G and H be groups and let $\varphi : G \to H$ be a mapping from G to H. Then φ is called a **homomorphism** if for all $x, y \in G$ we have:

$$\varphi(xy) = \varphi(x)\,\varphi(y)\,.$$

A homomorphism which is also bijective is called an **isomorphism**.

A homomorphism from G to itself is called an **endomorphism**.

An isomorphism from G to itself is called an **automorphism**, and the set of all automorphisms of a group G is denoted by $\mathrm{Aut}(G)$.

Before we show that $\mathrm{Aut}(G)$ is a group under compositions of maps, let us prove that a homomorphism preserves the group structure.

Proposition 6.1. If $\varphi : G \to H$ is a homomorphism, then $\varphi(e_G) = e_H$ and for all $x \in G$, $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Proof. Since φ is a homomorphism, for all $x, y \in G$ we have $\varphi(xy) = \varphi(x)\,\varphi(y)$. In particular, $\varphi(y) = \varphi(e_G y) = \varphi(e_G)\,\varphi(y)$, which implies $\varphi(e_G) = e_H$. Further, $\varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\,\varphi(x^{-1}) = e_H$, which implies $\varphi(x^{-1}) = \varphi(x)^{-1}$. ⊣

Corollary 6.2. If $\varphi : G \to H$ is a homomorphism, then the image of φ is a subgroup of H.

Proof. Let a and b be in the image of φ. We have to show that also ab^{-1} is in the image of φ. If a and b are in the image of φ, then there are $x, y \in G$ such that $\varphi(x) = a$ and $\varphi(y) = b$. Now, by Proposition 6.1 we get

$$ab^{-1} = \varphi(x)\,\varphi(y)^{-1} = \varphi(x)\,\varphi(y^{-1}) = \varphi(xy^{-1})\,.$$

⊣

Proposition 6.3. For any group G, the set $\mathrm{Aut}(G)$ is a group under compositions of maps.

Proof. Let $\varphi, \psi \in \mathrm{Aut}(G)$. First we have to show that $\varphi \circ \psi \in \mathrm{Aut}(G)$: Since φ and ψ are both bijections, $\varphi \circ \psi$ is a bijection too, and since φ and ψ are both homomorphisms, we have

$$(\varphi\circ\psi)(xy) = \varphi\big(\psi(xy)\big) = \varphi\big(\psi(x)\,\psi(y)\big) = \\ \varphi\big(\psi(x)\big)\,\varphi\big(\psi(y)\big) = (\varphi\circ\psi)(x)\,(\varphi\circ\psi)(y)\,.$$

Hence, $\varphi\circ\psi \in \mathrm{Aut}(G)$. Now, let us show that $\big(\mathrm{Aut}(G), \circ\big)$ is a group:

(A0) Let $\varphi_1, \varphi_2, \varphi_3 \in \mathrm{Aut}(G)$. Then for all $x \in G$ we have

$$\big(\varphi_1\circ(\varphi_2\circ\varphi_3)\big)(x) = \varphi_1\big(\varphi_2\circ\varphi_3)(x)\big) = \varphi_1\big(\varphi_2\big(\varphi_3(x)\big)\big) = \\ \big(\varphi_1\circ\varphi_2\big)\big(\varphi_3(x)\big) = \big((\varphi_1\circ\varphi_2)\circ\varphi_3\big)(x)\,,$$

which implies that $\varphi_1\circ(\varphi_2\circ\varphi_3) = (\varphi_1\circ\varphi_2)\circ\varphi_3$, thus, "$\circ$" is associative.

(A1) The identity mapping ι on G is of course a bijective homomorphism from G to itself, and in fact, ι is the neutral element of $\big(\mathrm{Aut}(G), \circ\big)$.

(A2) Let $\varphi \in \operatorname{Aut}(G)$, and let φ^{-1} be such that for every $x \in G$, $\varphi\big(\varphi^{-1}(x)\big) = x$. It is obvious that $\varphi \circ \varphi^{-1} = \iota$ and it remains to show that φ^{-1} is a homomorphism: Since φ is a homomorphism, for all $x, y \in G$ we have

$$\varphi^{-1}(xy) = \varphi^{-1}\big(\underbrace{\varphi(\varphi^{-1}(x))}_{=x}\,\underbrace{\varphi(\varphi^{-1}(y))}_{=y}\big) = \varphi^{-1}\big(\varphi\big(\varphi^{-1}(x)\,\varphi^{-1}(y)\big)\big) = \varphi^{-1}(x)\,\varphi^{-1}(y)\,,$$

which shows that $\varphi^{-1} \in \operatorname{Aut}(G)$. ⊣

Definition. If $\varphi : G \to H$ is a homomorphism, then $\big\{x \in G : \varphi(x) = e_H\big\}$ is called the **kernel** of φ and is denoted by $\ker(\varphi)$.

Theorem 6.4. Let $\varphi : G \to H$ be a homomorphism, then $\ker(\varphi) \trianglelefteq G$.

Proof. First we have to show that $\ker(\varphi) \leqslant G$: If $a, b \in \ker(\varphi)$, then

$$\varphi(ab^{-1}) = \varphi(a)\,\varphi(b^{-1}) = \varphi(a)\,\varphi(b)^{-1} = e_H\,e_H^{-1} = e_H\,,$$

thus, $ab^{-1} \in \ker(\varphi)$, which implies $\ker(\varphi) \leqslant G$.
Now we show that $\ker(G) \trianglelefteq G$: Let $x \in G$ and $a \in \ker(\varphi)$, then

$$\varphi(xax^{-1}) = \varphi(x)\,\varphi(a)\,\varphi(x)^{-1} = \varphi(x)\,e_H\,\varphi(x)^{-1} = \varphi(x)\,\varphi(x)^{-1} = e_H\,,$$

thus, $xax^{-1} \in \ker(\varphi)$, which implies $\ker(\varphi) \trianglelefteq G$. ⊣

Let us give some examples of homomorphisms:

(1) The mapping

$$\begin{aligned} \varphi : \quad (\mathbb{R}, +) &\to (\mathbb{R}^+, \cdot\,) \\ x &\mapsto e^x \end{aligned}$$

is an isomorphism, and $\varphi^{-1} = \ln$.

(2) Let n be a positive integer. Then

$$\begin{aligned} \varphi : \quad (\mathrm{O}(n), \cdot\,) &\to \big(\{1, -1\}, \cdot\,\big) \\ A &\mapsto \det(A) \end{aligned}$$

is a surjective homomorphism and $\ker(\varphi) = \mathrm{SO}(n)$. Further, for $n = 1$, φ is even an isomorphism.

(3) The mapping

$$\begin{aligned} \varphi : \quad \mathbb{R}^3 &\to \mathbb{R}^2 \\ (x, y, z) &\mapsto (x, z) \end{aligned}$$

is a surjective homomorphism and $\ker(\varphi) = \big\{(0, y, 0) : y \in \mathbb{R}\big\}$.

(4) Let $n \geq 3$ be an integer, let $C_n = \{a^0, \ldots, a^{n-1}\}$, and let $\rho \in D_n$ be the rotation through $2\pi/n$. Then $\varphi : C_n \to D_n$, defined by $\varphi(a^k) := \rho^k$ is an injective homomorphism from C_n into D_n. Thus, C_n is isomorphic to a subgroup of D_n.

(5) Let $n \geq 3$ be an integer. For any $x \in D_n$, let

$$\operatorname{sg}(x) = \begin{cases} 1 & \text{if } x \text{ is a rotation,} \\ -1 & \text{if } x \text{ is a reflection,} \end{cases}$$

then

$$\begin{array}{rccl} \varphi : & D_n & \to & \big(\{1,-1\},\,\cdot\,\big) \\ & x & \mapsto & \operatorname{sg}(x) \end{array}$$

is a surjective homomorphism.

(6) The mapping

$$\begin{array}{rccl} \varphi : & (\mathbb{Z}_{12},+) & \to & (\mathbb{Z}_{12},+) \\ & x & \mapsto & 4x \end{array}$$

is an endomorphism of $(\mathbb{Z}_{12},+)$, where $\ker(\varphi) = \{0,3,6,9\}$ and the image of φ is $\{0,4,8\}$.

(7) For every $r \in \mathbb{Q}^*$, the mapping

$$\begin{array}{rccl} \varphi : & (\mathbb{Q},+) & \to & (\mathbb{Q},+) \\ & q & \mapsto & rq \end{array}$$

is an automorphism of $(\mathbb{Q},+)$.

(8) Let $C_2 \times C_2 = \{e,a,b,c\}$, then every permutation of $\{a,b,c\}$ is a bijective homomorphism from $C_2 \times C_2$ to itself. Hence, $\operatorname{Aut}(C_2 \times C_2)$ is isomorphic to S_3 (or to D_3).

In order to define an operation on the set G/N, where $N \trianglelefteq G$, we need the following:

Fact 6.5. If $N \trianglelefteq G$, then for all $x,y \in G$, $(xN)\,(yN) = (xy)N$.

Proof. Since N is a normal subgroup of G, we have

$$(xN)\,(yN) = \big(x\underbrace{(yNy^{-1})}_{=N}\big)(yN) = (xy)(NN) = (xy)N\,.$$

$\dashv$

This leads to the following:

Proposition 6.6. If $N \trianglelefteq G$, then the set $G/N = \{xN : x \in G\}$ is a group under the operation $(xN)\,(yN) := (xy)N$.

Proof. First we have to show that the operation $(xN)\,(yN)$ is well-defined: If $(xN) = (\tilde{x}N)$ and $(yN) = (\tilde{y}N)$, then, by Lemma 3.6 (d), $x^{-1}\tilde{x}, y^{-1}\tilde{y} \in N$. Now, since N is a normal subgroup of G,

$$(xy)^{-1}(\tilde{x}\tilde{y}) = y^{-1}\,\underbrace{(x^{-1}\tilde{x})}_{\in N}\,\tilde{y} \,\in\, y^{-1}N\tilde{y} = \underbrace{y^{-1}N(y}_{=N}\,y^{-1})\tilde{y} = N(y^{-1}\tilde{y}) = N\,,$$

which implies $(xN)\,(yN) = (xy)N = (\tilde{x}\tilde{y})N = (\tilde{x}N)\,(\tilde{y}N)$.
Now, let us show that G/N is a group:
(A0) $(xN)\big((yN)\,(zN)\big) = \big(x(yz)\big)N = \big((xy)z\big)N = \big((xN)\,(yN)\big)(zN)$.
(A1) For all $x \in G$ we have

$$(eN)\,(xN) = (ex)N = xN\,,$$

therefore, $eN = N$ is the neutral element of G/N.
(A2) For all $x \in G$ we have

$$(xN)\,(x^{-1}N) = (xx^{-1})N = eN = N = (x^{-1}x)N = (x^{-1}N)\,(xN)\,,$$

therefore, $(xN)^{-1} = (x^{-1}N)$. $\dashv$

For example, let C be the cube-group and let N be the normal subgroup of C which is isomorphic to $C_2 \times C_2$. Then, by Proposition 6.6, C/N is a group, and in fact, C/N is isomorphic to S_3 (see Hw9.Q41).

Lemma 6.7. If $N \trianglelefteq G$, then

$$\begin{array}{rccc} \pi: & G & \to & G/N \\ & x & \mapsto & xN \end{array}$$

is a surjective homomorphism, called the natural homomorphism from G onto G/N, and $\ker(\pi) = N$.

Proof. For all $x, y \in G$ we have $\pi(xy) = (xy)N = (xN)\,(yN) = \pi(x)\,\pi(y)$, thus, π is a homomorphism. Further, let $xN \in G/N$, then $\pi(x) = xN$, which shows that π is surjective. Finally, by Lemma 3.6 (c), $\ker(\pi) = \{x \in G : xN = N\} = N$. $\dashv$

By Theorem 6.4 we know that if $\varphi : G \to H$ is a homomorphism, then $\ker(\varphi) \trianglelefteq G$. On the other hand, by Lemma 6.7, we get the following:

Corollary 6.8. If $N \trianglelefteq G$, then there exists a group H and a homomorphism $\varphi : G \to H$ such that $N = \ker(\varphi)$.

Proof. Let $H = G/N$ and let φ be the natural homomorphism from G onto H. $\dashv$

Theorem 6.9 (First Isomorphism Theorem). Let $\psi : G \to H$ be a surjective homomorphism, let $N = \ker(\psi) \trianglelefteq G$ and let $\pi : G \to G/N$ be the natural homomorphism from G onto G/N. Then there is a unique isomorphism $\varphi : G/N \to H$ such that $\psi = \varphi \circ \pi$. In other words, the following diagram "commutes":

$$\begin{tikzcd} G \arrow[r, "\psi"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Proof. Define $\varphi : G/N \to H$ by stipulating $\varphi(xN) := \psi(x)$ (for every $x \in G$). Then $\psi = \varphi \circ \pi$ and it remains to be shown that φ is well-defined, a bijective homomorphism and unique.

φ is well-defined: If $xN = yN$, then $x^{-1}y \in N$ (by Lemma 3.6 (d)). Thus, since $N = \ker(\psi)$, $\psi(x^{-1}y) = e_H$ and since ψ is a homomorphism we have $e_H = \psi(x^{-1}y) = \psi(x)^{-1}\,\psi(y)$, which implies $\psi(x) = \psi(y)$. Therefore, $\varphi(xN) = \psi(x) = \psi(y) = \varphi(yN)$.

φ is a homomorphism: Let $xN, yN \in G/N$, then

$$\varphi\big((xN)(yN)\big) = \varphi\big((xy)N\big) = \psi(xy) = \psi(x)\,\psi(y) = \varphi(xN)\,\varphi(yN)\,.$$

φ is injective:

$$\begin{aligned} \varphi(xN) = \varphi(yN) \iff \psi(x) = \psi(y) \iff \\ \iff e_H = \psi(x)^{-1}\,\psi(y) = \psi(x^{-1})\,\psi(y) = \psi(x^{-1}y) \iff \\ \iff x^{-1}y \in N \iff xN = yN\,. \end{aligned}$$

φ is surjective: Since ψ is surjective, for all $z \in H$ there is an $x \in G$ such that $\psi(x) = z$, thus, $\varphi(xN) = z$.

φ is unique: Assume towards a contradiction that there exists an isomorphism $\tilde{\varphi} : G/N \to H$ different from φ such that $\tilde{\varphi} \circ \pi = \psi$. Then there is a coset $xN \in G/N$ such that $\tilde{\varphi}(xN) \neq \varphi(xN)$, which implies

$$\psi(x) = (\tilde{\varphi} \circ \pi)(x) = \tilde{\varphi}\big(\pi(x)\big) = \tilde{\varphi}(xN) \neq \varphi(xN) = \varphi\big(\pi(x)\big) = (\varphi \circ \pi)(x) = \psi(x)\,,$$

a contradiction. ⊣

For example, let m be a positive integer and let $C_m = \{a^0, \ldots, a^{m-1}\}$ be the cyclic group of order m. Further, let $\psi : \mathbb{Z} \to C_m$, where $\psi(k) := a^k$. Then ψ is a surjective homomorphism from $\mathbb{Z}$ to C_m and $\ker(\psi) = m\mathbb{Z}$. Thus, by Theorem 6.9, $\mathbb{Z}/m\mathbb{Z}$ and C_m are isomorphic and the isomorphism $\varphi : \mathbb{Z}/m\mathbb{Z} \to C_m$ is defined by $\varphi(k + m\mathbb{Z}) := a^k$.

Let us consider some other applications of Theorem 6.9:

(1) Let n be a positive integer. Then

$$\begin{aligned} \psi :\ (\mathrm{O}(n), \cdot\,) &\to \big(\{1, -1\}, \cdot\,\big) \\ A &\mapsto \det(A) \end{aligned}$$

is a surjective homomorphism with $\ker(\psi) = \mathrm{SO}(n)$, and thus, $\mathrm{O}(n)/\,\mathrm{SO}(n)$ and $\{1, -1\}$ are isomorphic (where $\{1, -1\} \cong C_2$).

(2) Let n be a positive integer and let $\mathrm{GL}(n)^+ = \{A \in \mathrm{GL}(n) : \det(A) > 0\}$. Then

$$\begin{aligned} \psi :\ (\mathrm{GL}(n)^+, \cdot\,) &\to (\mathbb{R}^+, \cdot\,) \\ A &\mapsto \det(A) \end{aligned}$$

is a surjective homomorphism with $\ker(\psi) = \mathrm{SL}(n)$, and thus, $\mathrm{GL}(n)^+/\,\mathrm{SL}(n)$ and $\mathbb{R}^+$ are isomorphic.

(3) The mapping

$$\begin{array}{rrcl} \psi: & (\mathbb{C}^*, \cdot\,) & \to & (\mathbb{R}^+, \cdot\,) \\ & z & \mapsto & |z| \end{array}$$

is a surjective homomorphism with $\ker(\psi) = \mathbb{U} = \{z \in \mathbb{C} : |z|\}$, and thus, $\mathbb{C}^*/\mathbb{U}$ and $\mathbb{R}^+$ are isomorphic.

(4) The mapping

$$\begin{array}{rrcl} \psi: & \mathbb{R}^3 & \to & \mathbb{R}^2 \\ & (x, y, z) & \mapsto & (x, z) \end{array}$$

is a surjective homomorphism with $\ker(\psi) = \big\{(0, y, 0) : y \in \mathbb{R}\big\} \cong \mathbb{R}$, and thus, $\mathbb{R}^3/\mathbb{R}$ and $\mathbb{R}^2$ are isomorphic.

(5) The mapping

$$\begin{array}{rrcl} \psi: & (\mathbb{Z}_{12}, +) & \to & (\mathbb{Z}_3, +) \\ & x & \mapsto & x \ (\mathrm{mod}\ 3) \end{array}$$

is a surjective homomorphism with $\ker(\psi) = \{0, 3, 6, 9\} = 3\mathbb{Z}_{12}$, and thus, $\mathbb{Z}_{12}/3\mathbb{Z}_{12}$ and $\mathbb{Z}_3$ are isomorphic.

THEOREM 6.10 (Second Isomorphism Theorem). Let $N \trianglelefteq G$ and $K \leqslant G$. Then

(1) $KN = NK \leqslant G$.
(2) $N \trianglelefteq KN$.
(3) $(N \cap K) \trianglelefteq K$.
(4) The mapping

$$\begin{array}{rrcl} \varphi: & K/(N \cap K) & \to & KN/N \\ & x(N \cap K) & \mapsto & xN \end{array}$$

is an isomorphism.

Proof. (1) This is Theorem 5.8.

(2) Since $KN \leqslant G$ and $N \subseteq KN$, $N \leqslant KN$. Hence, since $N \trianglelefteq G$, $N \trianglelefteq KN$.

(3) Let $x \in K$ and $a \in N \cap K$. Then xax^{-1} belongs to K, since $x, a \in K$, but also to N, since $N \trianglelefteq G$, thus, $xax^{-1} \in N \cap K$.

(4) Let $\psi : K \to KN/N$ be defined by stipulating $\psi(k) := kN$. Then ψ is a surjective homomorphism and $\ker(\psi) = \{k \in K : k \in N\} = N \cap K$.
Consider the following diagram:

$$\begin{tikzcd} K \arrow[r, "\psi"] \arrow[d, "\pi"'] & KN/N \\ K/(N \cap K) \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Since ψ is a surjective homomorphism, by Theorem 6.9, φ is an isomorphism. $\dashv$

For example, let m and n be two positive integers. Then $m\mathbb{Z}$ and $n\mathbb{Z}$ are normal subgroups of $\mathbb{Z}$, and by Theorem 6.10, $m\mathbb{Z}/(m\mathbb{Z}\cap n\mathbb{Z})$ and $(m\mathbb{Z}+n\mathbb{Z})/n\mathbb{Z}$ are isomorphic. In particular, for $m = 6$ and $n = 9$ we have $m\mathbb{Z} \cap n\mathbb{Z} = 18\mathbb{Z}$ and $m\mathbb{Z} + n\mathbb{Z} = 3\mathbb{Z}$. Thus, $6\mathbb{Z}/18\mathbb{Z}$ and $3\mathbb{Z}/9\mathbb{Z}$ are isomorphic, in fact, both groups are isomorphic to C_3.

THEOREM 6.11 (Third Isomorphism Theorem). Let $K \trianglelefteq G$, $N \trianglelefteq G$, and $N \trianglelefteq K$. Then $K/N \trianglelefteq G/N$ and

$$\begin{aligned} \varphi : \ G/K \ &\to \ {G/N}\Big/{K/N} \\ xK \ &\mapsto \ (xN)(K/N) \end{aligned}$$

is an isomorphism.

Proof. First we show that $K/N \trianglelefteq G/N$. So, for any $x \in G$ and $k \in K$, we must have $(xN)(kN)(xN)^{-1} \in K/N$:

$$(xN)(kN)(xN)^{-1} = xNkNx^{-1}N = xNkx^{-1}\underbrace{xNx^{-1}}_{=N}N =$$

$$= xNkx^{-1}N = \underbrace{xNx^{-1}}_{=N}\underbrace{xkx^{-1}}_{=:k'\in K}N = Nk'N = k'NN = k'N \in K/N\,.$$

Let

$$\begin{aligned} \psi : \ G \ &\to \ {G/N}\Big/{K/N} \\ x \ &\mapsto \ (xN)(K/N) \end{aligned}$$

Then ψ is a surjective homomorphism and $\ker(\psi) = \{x \in G : xN \in K/N\} = K$. Consider the following diagram:

$$\begin{tikzcd} G \arrow[r, "\psi"] \arrow[d, "\pi"'] & {G/N}\Big/{K/N} \\ G/K \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Since ψ is a surjective homomorphism, by Theorem 6.9, φ is an isomorphism. $\dashv$

For example, let m and n be two positive integers such that $m \mid n$. Then $m\mathbb{Z}$ and $n\mathbb{Z}$ are normal subgroups of $\mathbb{Z}$, $n\mathbb{Z} \trianglelefteq m\mathbb{Z}$, and by Theorem 6.11,

$$\mathbb{Z}/m\mathbb{Z} \ \cong \ {\mathbb{Z}/n\mathbb{Z}}\Big/{m\mathbb{Z}/n\mathbb{Z}}\,.$$

In particular, for $m = 6$ and $n = 18$,

$$\mathbb{Z}_6 \ \cong \ {\mathbb{Z}_{18}}\Big/{6\mathbb{Z}/18\mathbb{Z}}\,,$$

and in fact, both groups are isomorphic to C_6.

7. Permutation Groups

Recall that the set of all permutations of $\{1, \ldots, n\}$ under composition is a group of oder $n!$, denoted by S_n, which is called the **symmetric group** or **permutation group** of degree n. Permutations are usually denoted by Greek letters like π, ρ, and σ.

The following theorem indicates that permutation groups and their subgroups play a key-role in the investigation of finite groups.

Theorem 7.1. If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Proof. Let $G = \{a_1, \ldots, a_n\}$ and let

$$\begin{array}{rccc} \varphi: & G & \to & S_n \\ & x & \mapsto & \pi_x \end{array}$$

where for $i \in \{1, \ldots, n\}$, $\pi_x(i)$ is such that $xa_i = a_{\pi_x(i)}$.

φ is well-defined: We have to show that for all $x \in G$, $\varphi(x) \in S_n$. Let $x \in G$, then for all $i, j \in \{1, \ldots, n\}$ we have

$$\pi_x(i) = \pi_x(j) \iff xa_i = xa_j \iff a_i = a_j \iff i = j \, .$$

Thus, for each $x \in G$, $\varphi(x) = \pi_x$ is an injective mapping from $\{1, \ldots, n\}$ into $\{1, \ldots, n\}$, which implies – since $\{1, \ldots, n\}$ is a finite set – that $\varphi(x)$ is a permutation of $\{1, \ldots, n\}$, or equivalently, $\varphi(x) \in S_n$.

φ is injective: If $\varphi(x) = \varphi(y)$, then for each $i \in \{1, \ldots, n\}$ we have $\pi_x(i) = \pi_y(i)$, thus

$$xa_i = a_{\pi_x(i)} = a_{\pi_y(i)} = ya_i \, ,$$

which implies $x = y$.

φ is a homomorphism: We have to show that $\varphi(xy) = \varphi(x)\,\varphi(y)$. For $x, y \in G$ and for any $i \in \{1, \ldots, n\}$ we have

$$a_{\pi_{xy}(i)} = (xy)a_i = x(ya_i) = xa_{\pi_y(i)} = a_{\pi_x(\pi_y(i))} \, .$$

Thus, $\pi_{xy}(i) = \pi_x\big(\pi_y(i)\big)$ (for all $i \in \{1, \ldots, n\}$), and hence, $\varphi(xy) = \varphi(x)\,\varphi(y)$.

By Corollary 6.2 and since φ is injective, G is isomorphic to a subgroup of S_n, namely to the image of φ. ⊣

It is common to write a permutation $\pi \in S_n$ in *two-row* notation, in which the top row of the $2 \times n$ matrix contains the integers $1, \ldots, n$ and the effect of π on the integer i is written under i:

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(i) & \ldots & \pi(n) \end{pmatrix}$$

In particular, the identity permutation is

$$\begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ 1 & 2 & \ldots & i & \ldots & n \end{pmatrix}$$

and is denoted by ι. For any permutation π and any integer k we set $\pi^0 := \iota$ and $\pi^{k+1} := \pi(\pi^k)$.

A more compact notation is the so-called *cycle notation*, which avoids repeating the same first row in each permutation. The theoretical basis for this notation is in the following result.

PROPOSITION 7.2. Let $\pi \in S_n$, $i \in \{1,\dots,n\}$, and let k be the smallest positive integer for which $\pi^k(i)$ is in the set $\bigl\{i, \pi(i), \pi^2(i), \dots, \pi^{k-1}(i)\bigr\}$. Then $\pi^k(i) = i$.

Proof. If $\pi^k(i) = \pi^r(i)$ for some non-negative $r < k-1$, then, for $k' = k-r$ we have $k \geq k' > 0$ and $\pi^{k'} = \iota$, which implies $\pi^{k'}(i) = i \in \bigl\{i, \pi(i), \dots, \pi^{k-1}(i)\bigr\}$, and therefore, by our assumption, $k' = k$. ⊣

DEFINITION. A permutation $\rho \in S_n$ is a ***k*-cycle** if there exists a positive integer k and an integer $i \in \{1,\dots,n\}$ such that

(1) k is the smallest positive integer such that $\rho^k(i) = i$, and
(2) ρ fixes each $j \in \{1,\dots,n\} \setminus \{i, \rho(i), \dots, \rho^{k-1}(i)\}$.

The k-cycle ρ is usually denoted $\bigl(i, \rho(i), \dots, \rho^{k-1}(i)\bigr)$.

For example the five non-identity elements of S_3 are all cycles, and may be written as

$$(1,2,3),\ (3,2,1),\ (1,2),\ (1,3),\ \textit{and}\ (2,3)\,.$$

Notice that for example $(1,2,3) = (2,3,1) = (3,1,2)$ and that not every permutation is a cycle, *e.g.*,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

is not a cycle.

DEFINITION. Two permutations ρ and σ are **disjoint** if each number moved by ρ is fixed by σ, or equivalently, each number moved by σ is fixed by ρ.

It is quite easy to see that disjoint permutations commute.

FACT 7.3. Let σ and ρ be disjoint permutations, then $\sigma\rho = \rho\sigma$, and in general, for all positive integers k, $(\sigma\rho)^k = \sigma^k\rho^k$.

Proof. Since σ and ρ are disjoint permutations, each number moved by σ is fixed by ρ and vice versa. So, the set of numbers moved by σ is disjoint from the set of numbers moved by ρ, and therefore it does not matter which permutation we carry out first. Consequently we get $(\sigma\rho)^k = \sigma^k\rho^k$ (for all positive integers k). ⊣

The next result shows that cycles are the "atoms" of permutations.

PROPOSITION 7.4. Every permutation $\pi \in S_n$ may be written as a product of disjoint cycles.

Proof. Let $\pi \in S_n$. By Proposition 7.2 and since the set $\{1,\dots,n\}$ is finite, for every $i \in \{1,\dots,n\}$ there is a positive integer k_i such that $\pi^{k_i}(i) = i$ and $\rho_i = \bigl(i, \pi(i), \dots, \pi^{k_i-1}(i)\bigr)$ is a k_i-cycle. We proceed by induction. Let $i_1 := 1$ and for $j \geq 1$ with $\sum_{\ell=1}^{j} k_{i_\ell} < n$ let i_{j+1} be the least number of the non-empty set

$$\bigl\{1,\dots,n\bigr\} \setminus \bigcup \bigl\{\pi^k(i_\ell) : k \in \mathbb{Z} \textit{ and } 1 \leq \ell \leq j\bigr\}\,.$$

Further, let m be the least positive integer such that $\sum_{\ell=1}^{m} k_{i_\ell} = n$, then, by construction, $\pi = \rho_{i_1}\,\rho_{i_2}\,\dots\,\rho_{i_m}$ and the ρ's are disjoint cycles. ⊣

Definition. A decomposition of a permutation π into disjoint cycles is called a **cycle decomposition** of π.

For example the cycle decomposition of the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 5 & 3 & 4 & 1 & 7 & 9 & 8 \end{pmatrix}$$

is $(1,6)(2)(3,5,4)(7)(8,9)$. It is usual to omit cycles of length 1, those integers fixed by π, and so π is abbreviated to $(1,6)(3,5,4)(8,9)$.

Proposition 7.5. If ρ is a k-cycle, then $\operatorname{ord}(\rho) = k$, and consequently, if π is a product of disjoint cycles of length $k_1, \ldots, k_r$, then $\operatorname{ord}(\pi) = \operatorname{lcm}(k_1, \ldots, k_r)$, where $\operatorname{lcm}(k_1, \ldots, k_r)$ is the lowest common multiple of the integers $k_1, \ldots, k_r$.

Proof. Let ρ be an arbitrary k-cycle, then there exists an $i \in \{1, \ldots, n\}$ such that $\rho = \big(i, \rho(i), \ldots, \rho^{k-1}(i)\big)$ where $\rho^k(i) = i$. Hence, for every non-negative $\ell < k$ we have $\rho^k\big(\rho^\ell(i)\big) = \rho^\ell\big(\rho^k(i)\big) = \rho^\ell(i)$, which shows that $\rho^k = \iota$, thus $\operatorname{ord}(\rho) \geq k$. On the other hand, by definition of k, $\rho^\ell \neq \iota$ for any positive $\ell < k$, thus, $\operatorname{ord}(\rho) = k$.

Let π be a product of disjoint cycles $\rho_1, \ldots, \rho_r$ of length $k_1, \ldots, k_r$ and let $\operatorname{ord}(\pi) = k$. By Fact 7.3 we have $\iota = \pi^k = \rho_1^k \ldots \rho_r^k$ which implies that for every $1 \leq j \leq r$, k_j divides k, thus, $\operatorname{ord}(\pi) \geq \operatorname{lcm}(k_1, \ldots, k_r)$. On the other hand, it is easy to see that for $k = \operatorname{lcm}(k_1, \ldots, k_r)$, $\pi^k = \iota$, thus, $\operatorname{ord}(\pi) = k$. ⊣

For example, the order of $(1,2,3,4)(5,6,7)(8,9)$ is equal to $\operatorname{lcm}(4,3,2) = 12$. However, the permutation $(1,2,3,4)(2,6,7)(3,9)$ is not a product of disjoint cycles (and so need not have order 12). In fact,

$$(1,2,3,4)(2,6,7)(3,9) = (1,2,6,7,3,9,4)\,,$$

and therefore has order 7.

The following result shows that for any permutations π and ρ, π has the same cycle structure as $\rho\pi\rho^{-1}$.

Proposition 7.6. Let π and ρ be permutations in S_n. The cycle decomposition of the permutation $\rho\pi\rho^{-1}$ is obtained from that of π by replacing each integer i in the cycle decomposition of π with the integer $\rho(i)$.

Proof. Consider the effect that $\rho\pi\rho^{-1}$ has on the integer $\rho(i)$:

$$\rho\pi\rho^{-1}\big(\rho(i)\big) = \rho\big(\pi(i)\big)\,,$$

or in other words, $\rho\pi\rho^{-1}$ maps $\rho(i)$ to $\rho\big(\pi(i)\big)$. Hence, in the cycle decomposition of $\rho\pi\rho^{-1}$, the number $\rho(i)$ stands to the left of $\rho\big(\pi(i)\big)$, so

$$\rho\pi\rho^{-1} = \ldots\ \big(\ \ldots\ \rho(i), \rho\big(\pi(i)\big)\ \ldots\ \big)\ \ldots\,,$$

whereas in the cycle decomposition of π, i stands to the left of $\pi(i)$, so

$$\pi = \ldots\ \big(\ \ldots\ i, \pi(i)\ \ldots\ \big)\ \ldots\,,$$

which completes the proof. ⊣

Definition. A **transposition** is a cycle of length 2, and an **elementary transposition** is a transposition of the form $(i, i+1)$.

Lemma 7.7. Every k-cycle can be written as a product of $k-1$ transpositions and every transposition can be written as product of an odd number of elementary transpositions.

Proof. It is easily verified that

$$(i_1, i_2, \ldots, i_k) = (i_1, i_2)(i_2, i_3) \ldots (i_{k-1}, i_k)\,,$$

thus, every k-cycle can be written as a product of $k-1$ transpositions. Further, let j be a positive integer and let $(i, i+j)$ be a transposition. If $j = 1$, then $(i, i+1)$ is an elementary transposition and we are done. Otherwise, it is easy to see that

$$(i, i+j) = \underbrace{(i, i+1) \ldots (i+j-1, i+j)}_{j \text{ elementary transpositions}} \underbrace{(i+j-2, i+j-1) \ldots (i, i+1)}_{j-1 \text{ elementary transpositions}},$$

thus, $(i, i+j)$ is the product of $2j-1$ elementary transpositions and $2j-1$ is always odd. ⊣

Proposition 7.8.

(1) Each permutation can be written as a product of (elementary) transpositions.
(2) S_n is generated by the transpositions $(1, 2)$, $(1, 3), \ldots, (1, n)$.
(3) S_n is generated by the two permutations $(1, 2)$ and $(1, 2, \ldots, n)$.

Proof. (1) follows from Proposition 7.4 and Lemma 7.7.

(2) By (1), it is enough to show that every transposition (i, j), where $i < j$, belongs to $\big\langle \big\{(1, 2),\, (1, 3), \ldots, (1, n)\big\} \big\rangle$. Now, if $i = 1$, then we are done. Otherwise, it is easy to see that $(i, j) = (1, i)(1, j)(1, i)$.

(3) See Hw10.Q47. ⊣

The factorisation of a cycle into transpositions is not unique. Moreover, it is not even true that the number of transpositions in any factorisation of a given cycle is always the same, for example $(1, 3) = (2, 3)(1, 2)(2, 3)$. However, we will see that the numbers of transpositions in any two decompositions of a given permutation are either both even or both odd.

Definition. For any positive integer n, let Δ_n be the polynomial in n variables $x_1, \ldots, x_n$ defined by

$$\Delta_n(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} \big(x_i - x_j\big)\,,$$

and for any permutation $\pi \in S_n$ let $\pi \cdot \Delta_n$ be the polynomial

$$\prod_{1 \leq i < j \leq n} \big(x_{\pi(i)} - x_{\pi(j)}\big)\,.$$

The following properties are easily checked.

FACT 7.9.

(a) $\iota \cdot \Delta_n = \Delta_n$.
(b) $(\pi\rho) \cdot \Delta_n = \pi \cdot (\rho \cdot \Delta_n)$.
(c) For any real number λ, $\pi \cdot (\lambda\Delta_n) = \lambda(\pi \cdot \Delta_n)$.

DEFINITION. For any $\pi \in S_n$, the polynomial Δ_n is either equal to $\pi \cdot \Delta_n$, in which case we say that the permutation π is **even**, or $\Delta_n = -\pi \cdot \Delta_n$, in which case we say that π is **odd**. We write $\operatorname{sgn}(\pi) = 1$ if π is even and $\operatorname{sgn}(\pi) = -1$ if π is odd, so that $\pi \cdot \Delta_n = \operatorname{sgn}(\pi)\, \Delta_n$.

THEOREM 7.10. The map $\operatorname{sgn} : S_n \to C_2$ is a homomorphism.

Proof. We must show that $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$:

$$\begin{aligned}
\operatorname{sgn}(\pi\rho)\,\Delta_n &= (\pi\rho) \cdot \Delta_n && \text{by definition}\\
&= \pi \cdot (\rho \cdot \Delta_n) && \text{by Fact 7.9 (b)}\\
&= \pi \cdot \big(\operatorname{sgn}(\rho)\Delta_n\big) && \text{by definition}\\
&= \operatorname{sgn}(\rho)(\pi \cdot \Delta_n) && \text{by Fact 7.9 (c)}\\
&= \operatorname{sgn}(\rho)\operatorname{sgn}(\pi)\Delta_n && \text{by definition}
\end{aligned}$$

Thus, $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\rho)\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$, as required. ⊣

COROLLARY 7.11. For any permutation $\pi \in S_n$, $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$, and for any $\pi, \rho \in S_n$,

$$\operatorname{sgn}(\rho\pi\rho^{-1}) = \operatorname{sgn}(\pi)\,.$$

Proof. By Fact 7.9 and from the definition we have $\operatorname{sgn}(\iota) = 1$. Thus, by Theorem 7.10, we have

$$1 = \operatorname{sgn}(\iota) = \operatorname{sgn}(\pi\pi^{-1}) = \operatorname{sgn}(\pi)\operatorname{sgn}(\pi^{-1})\,,$$

which implis $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$.

Further, since

$$\operatorname{sgn}(\pi)\operatorname{sgn}(\rho) = \operatorname{sgn}(\rho)\operatorname{sgn}(\pi)\,,$$

by Theorem 7.10 it follows that

$$\operatorname{sgn}(\rho\pi\rho^{-1}) = \operatorname{sgn}(\rho)\operatorname{sgn}(\pi)\operatorname{sgn}(\rho^{-1}) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)\operatorname{sgn}(\rho^{-1}) = \operatorname{sgn}(\pi)\,.$$

⊣

COROLLARY 7.12. All transpositions are odd, and a k-cycle is odd if and only if k is even.

Proof. Firstly notice that by the definition of sgn, every elementary transposition $(i, i+1)$ is odd. Indeed, we change the sign of just one factor of the polynomial Δ_n, namely of the factor $\big(x_i - x_{i+1}\big)$. Now, by Lemma 7.7, every transposition can be written as product of an odd number of elementary transpositions, and therefore, by Theorem 7.10, all transpositions are odd.

Again by Lemma 7.7, every k-cycle can be written as a product of $k-1$ transpositions, and therefore, by Theorem 7.10, a k-cycle is odd if and only if k is even. ⊣

As an immediate consequence of Corollary 7.12 we get

Corollary 7.13. A permutation is even (odd) if and only if it can be written as a product of an even (odd) number of transpositions. In particular, ι is even.

By the way, if $A = (a_{i,j})$ is an $n \times n$ matrix, then

$$\det(A) := \sum_{\pi \in S_n} \Big(\operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)} \Big) .$$

Definition. The kernel of the homomorphism $\operatorname{sgn} : S_n \to C_2$ is the **alternating group** A_n. Or in other words,

$$A_n = \{ \pi \in S_n : \ \pi \text{ is even} \} .$$

For example, $A_3 = \big\{ \iota, (1,2,3), (3,2,1) \big\}$, and therefore, $A_3 \cong C_3$. But for $n \geq 4$, A_n is a non-abelian group of order $n!/2$. In particular, as we will see later, A_4 is isomorphic to the tetrahedron-group T and A_5 is isomorphic to the dodecahedron-group D, whereas the cube-group C is isomorphic to S_4.

By the First Isomorphism Theorem and the fact that for $n \geq 2$ the map sgn is surjective, for every $n \geq 2$, $A_n \trianglelefteq S_n$ and $|S_n : A_n| = 2$. This implies that for every $n \geq 3$, S_n is not simple. It is easy to see that A_3 is the only non-trivial normal subgroup of S_3 and that A_3 is simple (since it is isomorphic to C_3). On the other hand, the group S_4 has a normal subgroup of order 4 (*cf.* Hw10.Q50 (c)) which is also a normal subgroup of A_4, thus, A_4 is not the only non-trivial normal subgroup of S_4 and A_4 is not simple. But one can show that for every $n \geq 5$, A_n is simple and it is the only non-trivial normal subgroup of S_n (we omit the proof).

We have seen that S_n is generated by its transpositions and that all transpositions are odd. Thus, no transposition belongs to A_n. To find simple generators for A_n, we have to consider even permutations. The simplest even permutations, beside the identity, are 3-cycles, and indeed:

Proposition 7.14. The alternating group A_n is generated by its 3-cycles.

Proof. Let π be an element of A_n. By Corollary 7.13, π can be written as a product of an even number of transpositions. So, it is enough to show that any product of two different transpositions can be written as a product of 3-cycles. Let us consider the product $(i,j)(r,s)$:

If the four integers i, j, r, s are distinct, then

$$(i,j)(r,s) = (i,r,j)(i,r,s) .$$

Otherwise, we may assume without loss of generality that $i = r$, in which case

$$(i,j)(i,s) = (i,s,j) .$$

⊣

Let us now consider the centres of S_n and A_n. Since $S_1 = A_1 \cong A_2 \cong C_1$, $Z(S_1) = Z(A_1) \cong Z(A_2) = \{\iota\}$. Further, $S_2 \cong C_2$ and $A_3 \cong C_3$, which implies that S_2 and A_3 are abelian, and therefore, $Z(S_2) = S_2$ and $Z(A_3) = A_3$. In general, we get the following:

THEOREM 7.15.

(a) For any $n \geq 3$, $Z(S_n) = \{\iota\}$.
(b) For any $n \geq 4$, $Z(A_n) = \{\iota\}$.

Proof. (a) Let $\sigma \in S_n$ be any permutation except the identity: Since $\sigma \neq \iota$, there is an $i \in \{1, \ldots, n\}$ such that $\sigma(i) = j \neq i$. Pick any $k \in \{1, \ldots, n\}$ distinct from i and j. Now, $\sigma\,(i,k)\,\sigma^{-1} = \big(j, \sigma(k)\big) \neq (i,k)$, since $j \notin \{i,k\}$. Hence, $\sigma\,(i,k) \neq (i,k)\,\sigma$, which implies that $\sigma \notin Z(S_n)$.

(b) Let $\pi \in A_n$ be any permutation except the identity: Since $\pi \neq \iota$, there is an $i \in \{1, \ldots, n\}$ such that $\pi(i) = j \neq i$. Pick any distinct $k, \ell \in \{1, \ldots, n\}$, both distinct from i and j. Now, $\pi\,(i,k,\ell)\,\pi^{-1} = \big(j, \pi(k), \pi(\ell)\big) \neq (i,k,\ell)$, since $j \notin \{i,k,\ell\}$. Hence, $\pi\,(i,k,\ell) \neq (i,k,\ell)\,\pi$, which implies that $\pi \notin Z(A_n)$. ⊣

Finally, let us consider the automorphism group of S_n:

For any group G and for any $x \in G$, the mapping $\varphi_x : G \to G$ defined by $\varphi_x(a) := xax^{-1}$ is an automorphism of G (*cf.* Hw8.Q38). Such an automorphism is called an **inner automorphism** of G. Let $\mathrm{Inn}(G)$ denote the set of all inner automorphisms of G. Further, the mapping $\psi : G \to \mathrm{Aut}(G)$ defined by $\psi(x) := \varphi_x$ is a homomorphism from G to $\mathrm{Aut}(G)$, which implies that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$ and, by the First Isomorphism Theorem, that $G/Z(G) \cong \mathrm{Inn}(G)$ (*cf.* Hw10.Q46).

Let us turn back to the group S_n. As an immediate consequence of Theorem 7.15 we get the following:

PROPOSITION 7.16. For any $n \geq 3$, $\mathrm{Inn}(S_n) \cong S_n$.

In the following we will show that for any $n \geq 3$, where $n \neq 6$, every automorphism of S_n is an inner automorphism. Let us first consider what an automorphism is doing with transpositions.

LEMMA 7.17. Let $n \geq 3$, where $n \neq 6$, $\varphi \in \mathrm{Aut}(S_n)$ and (i,j) a transposition in S_n. Then $\varphi(i,j)$ is a transposition.

Proof. The transposition (i,j) has order 2, and therefore, $\varphi(i,j)$ has order 2 (see Hw9.Q44 (c)). Thus, $\varphi(i,j)$ must be the product of r disjoint transpositions where $2r \leq n$. There are $\binom{n}{2}$ transpositions in S_n, and there are

$$\underbrace{\binom{n}{2} \cdot \binom{n-2}{2} \cdot \ldots \cdot \binom{n-2(r-1)}{2}}_{r \text{ factors}} \cdot \frac{1}{r!}$$

products of r disjoint transpositions. Now, if $\varphi\big((i,j)\big)$ is a product of r disjoint transpositions, then for every transposition (k,ℓ), $\varphi\big((k,\ell)\big)$ is also a product of r disjoint transpositions. Indeed, by Proposition 7.6 there exists a permutation ρ such that $\rho\,(i,j)\,\rho^{-1} = (k,\ell)$, and since φ is an automorphism we get $\varphi\big(\rho\,(i,j)\,\rho^{-1}\big) = \varphi(\rho)\,\varphi\big((i,j)\big)\,\varphi(\rho)^{-1} = \varphi\big((k,\ell)\big)$, and therefore, by Proposition 7.6 again, $\varphi\big((i,j)\big)$ has the same cycle structure as $\varphi\big((k,\ell)\big)$. So, the number of transpositions in S_n must correspond to the number of products of r disjoint transpositions in S_n. In other words, we must have

$$\frac{n(n-1)}{2} = \frac{n(n-1)(n-2) \cdot \ldots \cdot (n-2r+1)}{2^r \cdot r!},$$

or equivalently,

$$2^{r-1} \cdot r! = (n-2)(n-3) \cdot \ldots \cdot (n-2r+1)\,. \tag{$*$}$$

Obviously, equation $(*)$ holds for $r = 1$. So, let us consider the other cases:

For $r = 2$ we get $4 = (n-2)(n-3)$, which is impossible.

For $r = 3$ we get $24 = (n-2)(n-3)(n-4)(n-5)$ which holds just for $n = 6$, but we excluded this case.

For $n \geq 4$ we get

$$\begin{aligned}(n-2)(n-3) \cdot \ldots \cdot (n-2r+1) &\underset{\substack{\uparrow \\ n \geq 2r}}{\geq} (2r-2)(2r-3) \cdot \ldots \cdot 1 = (2r-2)! = \\ &= \underbrace{(2r-2) \cdot \ldots \cdot (r+1)}_{r-2 \text{ factors, each } > 4} \cdot r! \geq 4^{r-2} \cdot r! = 2^{2(r-2)} \cdot r! > 2^{r-1} \cdot r!\,,\end{aligned}$$

which shows that also in this case the equation $(*)$ does not hold.

Thus, $r = 1$, or in other words, $\varphi\big((i,j)\big)$ is a transposition. ⊣

THEOREM 7.18. Let $n \geq 3$, where $n \neq 6$, then $\mathrm{Aut}(S_n) \cong S_n$.

Proof. By Proposition 7.16 it is enough to show that every automorphism of S_n is an inner automorphism. By Proposition 7.8 we know that S_n is generated by the transpositions $(1,2)$, $(1,3), \ldots, (1,n)$, so, it is enough to consider these transpositions. By Lemma 7.17 we know that for any $\varphi \in \mathrm{Aut}(S_n)$ and for any $i \in \{2, \ldots, n\}$, $\varphi\big((1,i)\big)$ is a transposition. Pick any two distinct numbers i, j from the set $\{2, 3, \ldots, n\}$ and let

$$\varphi\big((1,i)\big) = (k,\ell) \text{ and } \varphi\big((1,j)\big) = (p,q)\,.$$

Now, $(1,i)(1,j) = (1,j,i)$ and has order 3, and hence, $(k,\ell)(p,q)$ must also have order 3, which implies that two of the four element k, ℓ, p, q must be equal. Without loss of generality, let us assume that $p = k$. Then $\varphi\big((1,i)\big) = (k,\ell)$ and $\varphi\big((1,j)\big) = (k,q)$. If $n > 3$, then we can pick an number $h \in \{1, \ldots, n\} \setminus \{1, i, j\}$. Let $\varphi\big((1,h)\big) = (r,s)$, then $\{r,s\}$ has one element in common with $\{k,\ell\}$ and with $\{k,q\}$. If $r = \ell$ and $s = q$, then we would have

$$\begin{aligned}\varphi\big((1,j,i)\big) = \varphi\big((1,i)(1,j)\big) = (k,\ell)(k,q) = (k,q,\ell) = \\ = (q,\ell,k) = (k,q)(\ell,q) = \varphi\big((1,j)(1,h)\big) = \varphi\big((1,h,j)\big)\,,\end{aligned}$$

but this is a contradiction since φ is injective and $(1,j,i) \neq (1,h,j)$. So, we have either $r = k$ or $s = k$.

In general, for every $i \in \{2, \ldots, n\}$ there exists a unique $\pi(i) \in \{1, \ldots, n\} \setminus \{k\}$ such that

$$\varphi\big((1,i)\big) = \big(k, \pi(i)\big)\,.$$

Further, it is not hard to see that we stipulate $\pi(1) := k$, then π is a permutation of $\{1, \ldots, n\}$. Hence, by Proposition 7.6 we finally have

$$\varphi\big((1,i)\big) = \big(k, \pi(i)\big) = \big(\pi(1), \pi(i)\big) = \pi\,(1,i)\,\pi^{-1}\,,$$

which shows that every automorphism of S_n is an inner automorphism, which completes the proof. ⊣

What about $\operatorname{Aut}(S_6)$? One can show that there exists an automorphism $\varphi \in \operatorname{Aut}(S_6)$ such that $\varphi(i,j)$ is the product of 3 disjoint transpositions, and hence, by Proposition 7.6, $\varphi \notin \operatorname{Inn}(S_6)$. Moreover one can show that $|\operatorname{Aut}(S_6)| = 1440$, and since $\operatorname{Inn}(S_6) \cong S_6$ and $|S_6| = 720$, this implies that $|\operatorname{Aut}(S_6) : \operatorname{Inn}(S_6)| = 2$, and therefore $\operatorname{Inn}(S_6) \lhd \operatorname{Aut}(S_6)$ (we omit the proof).

8. The Sylow Theorems

In the sequel, G is always a finite group.

Definition. For $a \in G$, the set $C(a) := \{x \in G : xax^{-1} = a\}$ is called the **centralizer** of a in G.

Note that $x \in C(a)$ *iff* $xa = ax$, and that for any $a \in G$ we have $a \in C(a)$.

Fact 8.1. For any $a \in G$, $C(a) \leqslant G$.

Proof. We have to verify the axioms (A0), (A1) and (A2).

(A0) For $x, y \in C(a)$ we have

$$(xy)a = x(ya) \underset{\substack{\uparrow \\ y\in C(a)}}{=} x(ay) = (xa)y \underset{\substack{\uparrow \\ x\in C(a)}}{=} (ax)y = a(xy)\,,$$

hence, $xy \in C(a)$.

(A1) $ea = ae$, thus, $e \in C(a)$.

(A2) If $x \in C(a)$, then

$$x^{-1}a = x^{-1}a(xx^{-1}) = x^{-1}(ax)x^{-1} \underset{\substack{\uparrow \\ x\in C(a)}}{=} x^{-1}(xa)x^{-1} = (x^{-1}x)ax^{-1} = ax^{-1}\,,$$

hence, $x^{-1} \in C(a)$. ⊣

Definition. For $a \in G$, the set $\operatorname{orbit}(a) := \{xax^{-1} : x \in G\}$ is called the **orbit** of a.

Fact 8.2. For $a, a' \in G$ we either have $\operatorname{orbit}(a) = \operatorname{orbit}(a')$ or $\operatorname{orbit}(a) \cap \operatorname{orbit}(a') = \emptyset$. Further, $|\operatorname{orbit}(a)| = 1$ *iff* $a \in Z(G)$.

Proof. If $\operatorname{orbit}(a) \cap \operatorname{orbit}(a') \neq \emptyset$, then $xax^{-1} = ya'y^{-1}$ (for some $x, y \in G$). Thus, $a' = y^{-1}xax^{-1}y = y^{-1}xa(y^{-1}x)^{-1} \in \operatorname{orbit}(a)$ and $a = x^{-1}ya'y^{-1}x = x^{-1}ya'(x^{-1}y)^{-1} \in \operatorname{orbit}(a')$, which implies that $\operatorname{orbit}(a) = \operatorname{orbit}(a')$.

If $|\operatorname{orbit}(a)| = 1$, then for all $x \in G$ we have $xax^{-1} = a$, thus, for all $x \in G$ we have $xa = ax$, which implies $Z(G)$. On the other hand, if $a \in Z(G)$, then $xax^{-1} = a$ (for all $x \in G$), thus, $|\operatorname{orbit}(a)| = 1$. ⊣

Lemma 8.3. For every $a \in G$ we have

$$|\operatorname{orbit}(a)| = |G : C(a)|\,.$$

Proof. $|G : C(a)| = |G/C(a)| = \big|\{xC(a) : x \in G\}\big|$. Further, we have

$$xC(a) = yC(a) \iff x^{-1}y \in C(a) \iff (x^{-1}y)a(y^{-1}x = a \iff yay^{-1} = xax^{-1}\,,$$

which implies that $\big|\{xax^{-1} : x \in G\}\big| = \big|\{xC(a) : x \in G\}\big|$. ⊣

As a consequence of Fact 8.2 and Lemma 8.3 we get

Corollary 8.4. Let $a_1, \dots, a_n$ be representatives for the n orbits which have size larger than 1. Then

$$|G| = |Z(G)| + \sum_{i=1}^{n} |\operatorname{orbit}(a_i)| = |Z(G)| + \sum_{i=1}^{n} |G : C(a_i)|\,.$$

Proposition 8.5. If G is a group of order p^2, where p is prime, then G is abelian.

Proof. Assume that G is not abelian, then, by Corollary 8.4, we can choose some $a_1, \ldots, a_n \in G$ such that $|\operatorname{orbit}(a_i)| > 1$ (for all $a_i \in \{a_1, \ldots, a_n\}$) and $p^2 = |G| = |Z(G)| + \sum_{i=1}^{n} |G : C(a_i)|$. By Lemma 8.3, for each $a_i \in \{a_1, \ldots, a_n\}$ we get $1 < |\operatorname{orbit}(a_i)| = |G : C(a_i)|$, so, $p \mid |C(a_i)|$, and therefore $p \mid Z(G)$, which implies that $|Z(G)| \geq p$. If we assume that G is not abelian, then $Z(G) < G$, thus, $|Z(G)| = p$. Choose some $x \in G \setminus Z(G)$, then $Z(G) \leqslant C(x)$, and since $x \in C(x)$ we get $|C(x)| \geq p + 1$. Now, since $C(x) \leqslant G$, $|C(x)| \mid |G| = p^2$, and because $|C(x)| \geq p + 1$ we get $C(x) = G$, thus $x \in Z(G)$, which is absurd. Hence, we must have $Z(G) = G$, which shows that G is abelian. ⊣

Theorem 8.6 (Cauchy). Suppose that $p \mid |G|$ for some prime number p. Then there is an element $g \in G$ of order p.

Proof. The proof is by induction on $|G|$. If $|G| = 1$, then the result is vacuously true. Now, let us assume that $|G| > 1$ and that for every proper subgroup $H < G$ we have $p \nmid |H|$, (in other words, $p \mid |G : H|$), else we are home by induction. By Corollary 8.4 we get $p \mid |Z(G)|$, and by our assumption we get $G = Z(G)$ which implies that G is abelian. A proper subgroup $H < G$ is called maximal if $H \leqslant H' \leqslant G$ implies $H' = H$ or $H' = G$. If H, K are distinct maximal proper subgroups of G, then $HK \leqslant G$ (since G is abelian) and by maximality of H and K we get $HK = G$ (since $H, K \leqslant HK$). Now, $|G| = |HK| = \frac{|H| \cdot |K|}{|H \cap K|}$, but because $p \nmid |H|$ and $p \nmid |K|$, this implies $p \nmid |G|$, which is a contradiction. Therefore, G has a unique maximal proper subgroup, say M. Since M is the only maximal proper subgroup of G, all proper subgroups $H < G$ are subgroups of M. Choose $g \in G$ with $g \notin M$, then $\langle g \rangle = G$, (since otherwise, $\langle g \rangle \leqslant M$), and hence, G is cyclic. The order of g is $|G|$, and if we put $n = \frac{|G|}{p}$, then $\langle g^n \rangle$ is a subgroup of G of order p, which completes the proof. ⊣

Definition. Let $H \leqslant G$, then the set $N(H) := \{x \in G : xHx^{-1} = H\}$ is called the **normalizer** of H in G, and $\operatorname{orbit}(H) := \{xHx^{-1} : x \in G\}$ is called the **orbit** of H.

Fact 8.7. For every $H \leqslant G$, $N(H) \leqslant G$ and $|\operatorname{orbit}(H)| = |G : N(H)|$.

Proof. Just follow the proofs of Fact 8.1 and Lemma 8.3. ⊣

Fact 8.8. For every $H \leqslant G$, $H \trianglelefteq N(H)$.

Proof. By definition, for every $x \in N(H)$ we have $xHx^{-1} = H$, thus, $H \trianglelefteq N(H)$. ⊣

Lemma 8.9. Let G be such that $|G| = p^m n$, where p is prime, $m, n > 0$ and $p \nmid n$, and let $P, Q \leqslant G$ be such that $|P| = |Q| = p^m$. Then $Q \leqslant N(P)$ if and only if $Q = P$.

Proof. Of course, $Q = P$ implies $Q \leqslant N(P)$. On the other hand, if $Q \leqslant N(P)$, then, since $P \trianglelefteq N(P)$ (by Fact 8.8), $PQ \leqslant N(P) \leqslant G$. Thus,

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = \frac{p^m \cdot p^m}{|P \cap Q|}$$

must divide $|G| = p^m n$, which implies $|P \cap Q| = p^m$, hence, $Q = P$. ⊣

Definition. Let G be a finite group of order $p^m n$, where p is prime and does not divide n. Then any subgroup of G of order p^m is called a **Sylow p-subgroup** of G, and the set of all such subgroups of G is denoted $\mathrm{Syl}_p(G)$.

In order to state Sylow's Theorem, we need one more definition.

Definition. Two subgroups H_1 and H_2 of a group G are called conjugate in G if $H_1 = xH_2x^{-1}$ for some $x \in G$.

Theorem 8.10 (Sylow). Let G be a finite group of order $p^m n$, where p is prime and does not divide n.

(i) There is a Sylow p-subgroup P of G.
(ii) All elements of $\mathrm{Syl}_p(G)$ are conjugate in G.
(iii) $|\,\mathrm{Syl}_p(G)| \equiv 1 \mod p$.
(iv) $|\,\mathrm{Syl}_p(G)| \;\big|\; n$.

Proof. We prove (i) by induction on $|G|$. If $|G| = 1$, then the result is vacuously true, and therefore we may assume that $|G| > 1$. By Corollary 8.4 we have $|G| = |Z(G)| + \sum_{j=1}^{s} |G : C(x_j)|$, where the x_j are a collection of representatives for those orbits which are not singletons. Thus, each $C(x_j)$ is a proper subgroup of G. If $p \;\big|\; |G : C(x_j)|$ for every $1 \le j \le s$, then $p \;\big|\; |Z(G)| \neq 1$. Thanks to Cauchy's Theorem 8.6 we can choose $z \in Z(G)$ of order p, so, since $z \in Z(G)$, $\langle z\rangle \trianglelefteq G$. Let $\pi : G \to G/\langle z\rangle$ be the natural projection. By induction, there is a Sylow p-subgroup P_1 of $G/\langle z\rangle$. This group has order p^{m-1}, since $|G/\langle z\rangle| = p^{m-1}n$. The preimage of P_1 under π is $P \leqslant G$, where $P/\langle z\rangle$ has order $p^{m-1} = \frac{|P|}{p}$. Thus, $|P| = p^m$ and we have found a Sylow p-subgroup of G. The other possibility is that there is some x_j with $p \nmid |G : C(x_j)|$, so, $|G : C(x_j)| = p^m k$ with $k < n$ and $p \nmid k$. By induction, $C(x_j)$ has a Sylow p-subgroup P of order p^m, and since $P \leqslant G$, P is a Sylow p-subgroup of G.

For part (ii) and (iii), let P be a Sylow p-subgroup of G. Let $\Omega = \{xPx^{-1} : x \in G\}$ denote the set of all G-conjugates of P. Now, by Fact 8.7 we have $|\Omega| = |G : N(P)|$. Further, for $P_i \in \Omega$, let $\Omega_i = \{yP_iy^{-1} : y \in P\}$, then Ω is the disjoint union of some Ω_i's, so, $|\Omega| = \sum_i |\Omega_i|$. Again by Fact 8.7 we get $|\Omega_i| = |P : N(P_i) \cap P|$, which tells us that the orbits Ω_i have size divisible by p, unless $P \leqslant N(P_i)$, in which case $|\Omega_i| = 1$ and $P = P_i$ (by Lemma 8.9). Hence, of the orbits Ω_i there is exactly one of length 1 and all the others have size divisible by p, thus, $|\Omega| = \sum_i |\Omega_i| \equiv 1 \pmod p$. If we can show that $\Omega = \mathrm{Syl}_p(G)$, then we are done. So, assume towards a contradiction that $\Omega \neq \mathrm{Syl}_p(G)$, which means that there is a Sylow p-subgroup Q which is not a conjugate of P. Now, all Q-orbits $\Omega_i = \{yP_iy^{-1} : y \in Q\}$, where $P_i \in \Omega$ have size divisible by p, since otherwise, $Q \leqslant N(P_i)$ (for some i) and therefore $Q = P_i$ (by Lemma 8.9), which implies that Q is a conjugate of P. Since Ω is a disjoint union of sets − namely the Ω_i's − of size divisible by p we deduce that $|\Omega| \equiv 0 \pmod p$. However, we already know that $|\Omega| \equiv 1 \pmod p$ so this is absurd. Thus, $\Omega = \mathrm{Syl}_p(G)$, which implies that all Sylow p-subgroups of G are conjugate and $|\,\mathrm{Syl}_p(G)| \equiv 1 \pmod p$.

To verify (iv), let $P \in \mathrm{Syl}_p(G)$. Then, by (ii), $\mathrm{Syl}_p(G) = \{xPx^{-1} : x \in G\}$, and by Fact 8.7 we get $|\,\mathrm{Syl}_p(G)| = |G : N(P)|$. Since $P \leqslant N(P)$ it follows that $p^m \;\big|\; |N(P)|$, and so $|G : N(P)|$ must divide n. ⊣

As a consequence of Theorem 8.10 (ii) we get

Corollary 8.11. Let G be a finite group of order $p^m n$, where $n, m > 0$ and p is prime and does not divide n. Then $|\operatorname{Syl}_p(G)| = 1$ if and only if the unique Sylow p-subgroup is a normal subgroup of G. In particular, $|\operatorname{Syl}_p(G)| = 1$ implies that G is not simple.

9. The Groups T, C, and D

In the sequel, T denotes the *tetrahedron-group*, C denotes the *cube-group* and D denotes the *dodecahedron-group*. Further, O denotes the *octahedron-group* and I denotes the *icosahedron-group*.

We already know that $O \cong C$ and $I \cong D$, so, we do not have to consider O and I.

Theorem 9.1. $T \cong A_4$, $C \cong S_4$ and $D \cong A_5$.

Proof. $T \cong A_4$: Let $1, 2, 3, 4$ denote the four faces of the tetrahedron, then each $\tau \in T$ can be considered as a permutation of $\{1, 2, 3, 4\}$ and the corresponding map $\varphi : T \to S_4$ is an injective homomorphism. Thus, T is isomorphic to a subgroup of S_4 of order $|T| = 12$. Further, each cycle $(i_1, i_2, i_3) \in S_4$ of length 3 can be realized by a rotation $\tau \in T$ of order 3. Thus, since A_4 is generated by the cycles of length 3, A_4 is isomorphic to a subgroup of T. Now, because $|A_4| = |T|$, this implies $T \cong A_4$.

$C \cong S_4$: Let $1, 2, 3, 4$ denote the four long diagonals of the cube, then each $\gamma \in C$ can be considered as a permutation of $\{1, 2, 3, 4\}$. Further, it is easily verified that every elementary transposition of $\{1, 2, 3, 4\}$ corresponds to an element of C. Thus, since S_4 is generated by the elementary transpositions, S_4 is isomorphic to a subgroup of C of order $|S_4| = 24 = |C|$, and consequently we get $C \cong S_4$.

$D \cong A_5$: Let $1, 2, 3, 4, 5$ denote the five different cubes we can put into a dodecahedron in such a way that each edge of each cube lies on one face of the dodecahedron. Thus, each $\delta \in D$ can be considered as a permutation of $\{1, 2, 3, 4, 5\}$ and the corresponding map $\varphi : D \to S_5$ is a homomorphism. Now, since a dodecahedron has 20 vertices, the five cubes have $5 \cdot 8 = 40$ vertices and there are $\binom{5}{2} = 10$ pairs of cubes, every two cubes have exactly two vertices in common and these two vertices are opposite each other. Now, if $\delta \in D$ is a rotation about an axis joining 2 opposite vertices through $2\pi/3$, then $\varphi(\delta)$ is a 3-cycle. On the other hand, for every 3-cycle $\sigma \in S_5$, there is a $\delta \in D$ such that $\varphi(\delta) = \sigma$. Hence, since by Proposition 7.14 every alternating group is generated by its 3-cycles, A_5 is isomorphic to a subgroup of D, and since $|A_5| = |D|$, we get $D \cong A_5$. ⊣

The subgroups of *T*. By Sylow's Theorem, T has 1 or 4 Sylow 3-subgroups which have order 3, and it has 1 or 3 Sylow 2-subgroups which have order 4. Further, T must also have a subgroup of order 2 (since by Cauchy's Theorem, a group of order 4 has always a subgroup of order 2), but we already know that T does not have a subgroup of order 6.

In the following we give a complete list of all subgroups of $A_4 \cong T$:

Of course, A_4 has exactly one subgroup of order 1, namely $\{\iota\}$, where ι is the identity, and it has exactly one subgroup of order 12, namely A_4 itself.

The subgroups of order 2 are: $\{\iota, (1, 2)(3, 4)\}$, $\{\iota, (1, 3)(2, 4)\}$, $\{\iota, (1, 4)(2, 3)\}$, and none of them is a normal subgroup of A_4.

There is just one subgroup of order 4, namely $\{\iota, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$. Since a subgroup of order 4 is a Sylow 2-subgroup, by Corollary 8.11, $\{\iota, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ is a normal subgroup of A_4, and further, it is isomorphic to $C_2 \times C_2$.

The 4 subgroups of order 3 are: $\{\iota, (1, 2, 3), (3, 2, 1)\}$, $\{\iota, (1, 2, 4), (4, 2, 1)\}$, $\{\iota, (1, 3, 4),$

$(4,3,1)\}$ and $\{\iota,(2,3,4),(4,3,2)\}$. Since a subgroup of order 3 is a Sylow 3-subgroup, by Corollary 8.11, none of these subgroups of order 3 can be a normal subgroup of A_4.

COROLLARY 9.2. T is not simple.

Proof. Since T has a normal subgroup of order 4, T is not simple. ⊣

The subgroups of *C* of order 6, 8 and 12. The group C has 4 subgroups of order 3, namely rotations about a long diagonal through $2\pi/3$ and $-2\pi/3$. Each of these 4 Sylow 3-subgroups is isomorphic to C_3. Thus, C has 4 subgroups of order 6 (just turn the long diagonal), each of them is isomorphic to $D_3 \cong S_3$ and none of them is a normal subgroup of C. A subgroup of order 8 is a Sylow 2-subgroup, and since there are 3 subgroups of order 8, none of them is a normal subgroup. Further, each subgroup of order 8 is isomorphic to D_4. The group C has also a unique subgroup of order 12, which is isomorphic to T and since $|C : T| = 2$, this subgroup is a normal subgroup of C.

COROLLARY 9.3. C is not simple.

Proof. Since C has a normal subgroup of order 12, C is not simple. ⊣

The subgroups of *D*. A dodecahedron has 12 faces, 20 vertices and 30 edges. Remember that since $D \cong A_5$ and A_n is simple (for $n \geq 5$), D is simple, thus, D has no normal subgroups (except $\{\iota\}$ and D), in particular for $p = 2, 3, 5$, $|\operatorname{Syl}_p(D)| \neq 1$. In the following we give a complete list of all proper subgroups of D:

The subgroups of order 2 are the rotations about an axis joining midpoints of two opposite edges and since there are 30 edges, D has 15 subgroups of order 2.

A subgroup of order 3 is a Sylow 3-subgroup and therefore, $|\operatorname{Syl}_3(D)|$ is 4 or 10. Further, subgroups of order 3 are rotations about an axis joining opposite vertices and since there are 20 vertices, D has 10 subgroups of order 3.

A subgroup of order 4 is a Sylow 2-subgroup and therefore, $|\operatorname{Syl}_2(D)|$ is 3 or 5. Further, subgroups of order 4 are generated by rotations about three perpendicular axes joining midpoints of two opposite edges and since there are 30 edges, and each subgroup needs 6 edges, D has 5 subgroups of order 4 and each is isomorphic to $C_2 \times C_2$.

A subgroup of order 5 is a Sylow 5-subgroup and therefore, $|\operatorname{Syl}_5(D)|$ is 6. Indeed, subgroups of order 5 are rotations about an axis joining midpoints of opposite faces and since there are 12 faces, D has 6 subgroups of order 5.

It is not hard to see that D has 10 subgroups of order 6 and each is those subgroups is isomorphic to D_3.

Further, D has 6 subgroups of order 10 and each of those subgroups is isomorphic to D_5.

Finally we have 5 subgroups of order 12 and each of those subgroups is isomorphic to T.

Since D has no subgroups of order 15, 20 or 30, the 57 subgroups listed above are all proper subgroups of D.

THEOREM 9.4. D is simple.

Proof. Let us define an equivalence relation "$\sim$" on D as follows:

$$a \sim b \iff \exists x \in D(xax^{-1} = b)$$

First we have to check that "$\sim$" is an equivalence relation:

$a \sim a$: $\iota a \iota^{-1} = a$.

$a \sim b \to b \sim a$: If $xax^{-1} = b$, then $x^{-1}bx = a$.

$a \sim b$ *and* $b \sim c \to a \sim c$: If $xax^{-1} = b$ and $yby^{-1} = c$, then $(yx)a(yx)^{-1} = c$.

The equivalence relation "$\sim$" induces a partition of D into five pairwise disjoint parts, namely

$$\begin{aligned} P_\iota &= \{\iota\}, \\ P_{2\pi/3} &= \Big\{ \textit{rotations through } 2\pi/3 \textit{ about axes joining opposite vertices} \Big\}, \\ P_\pi &= \Big\{ \textit{rotations through } \pi \textit{ about axes joining midpoints of opposite edges} \Big\}, \\ P_{2\pi/5} &= \Big\{ \textit{rotations through } 2\pi/5 \textit{ about axes joining centres of opposite faces} \Big\}, \\ P_{4\pi/5} &= \Big\{ \textit{rotations through } 4\pi/5 \textit{ about axes joining centres of opposite faces} \Big\}. \end{aligned}$$

We have $|P_\iota| = 1$, $|P_{2\pi/3}| = 20$, $|P_{2\pi}| = 15$, $|P_{2\pi/5}| = |P_{4\pi/5}| = 12$. Notice that $|D| = 60 = |P_\iota| + |P_{2\pi/3}| + |P_{2\pi}| + |P_{2\pi/5}| + |P_{4\pi/5}|$, thus, each element of D belongs to exactly one part of the partition.

Assume that $N \trianglelefteq D$ and let $a \in N$. Firstly, since N is a normal subgroup of D, N must contain all elements which are equivalent to a, which implies that N must be a union of some of the five parts. Secondly, since $N \leqslant D$, $|N|$ must divide $|D| = 60$. Now, since $P_\iota \subseteq N$, this is just possible if $N = P_\iota$ or $N = P_\iota \cup P_{2\pi/3} \cup P_{2\pi} \cup P_{2\pi/5} \cup P_{4\pi/5} = D$. Thus, $N = \{\iota\}$ or $N = D$, and therefore, D is simple. $\dashv$