Chapter I: Groups

1 Binary operations

Definition. Let X be a set. A **(binary) operation** on X is a map $X \times X \to X$.

Remark. Binary operations are written using infix notation such as $a * b, a + b, a \cdot b$ or just ab rather than by functional notation of the form $f(a, b)$.

Examples.

1. $X = \mathbb{R}, (a, b) \mapsto a + b, a - b, ab$
2. $X = \mathbb{N}, (a, b) \mapsto a^b, \gcd(a, b)$
3. $X = \mathrm{M}_n(\mathbb{R}), (A, B) \mapsto A + B, AB$
4. For a given set M, let X be the collection of subsets of M. Then $(A, B) \mapsto A \cup B, A \cap B, A \setminus B$ is a binary operation.
5. For a given set M, let X be the set of all maps from M to M. Then $(f, g) \mapsto f \circ g$ is a binary operation.

Definition. Let $*$ be a binary operation on X.

1. The operation $*$ is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in X$.
2. The operation $*$ is **commutative** if $a * b = b * a$ for all $a, b \in X$.

Examples.

1. $X = \mathbb{R}, a * b = a + b, ab$ are both associative and commutative
2. $X = \mathbb{R}, a * b = a - b$ is neither associative nor commutative
3. $X = \mathbb{N}, a * b = 2a + 2b$ is commutative but not associative
4. $X = \mathrm{M}_n(\mathbb{R}), A * B = AB$ is associative but not commutative

Exercise 1.1. *Prove that $(a * b) * c = c * (b * a)$ for any $a, b, c \in X$ if $*$ is an associative commutative operation on X.*

Theorem 1.1 (Generalized associativity)**.** *Let $*$ be an associative operation on a set X. Then for any $x_1, \ldots, x_n \in X$ all possible parenthesizations of the expression $x_1 * x_2 * \cdots * x_n$ are equal.*

Proof. The cases $n = 1, 2$ are tautological. The case $n = 3$ follows from the definition of associativity. Assume $n > 3$, and that the result holds for all $m < n$. We will show that any parenthesization of $A = x_1 * x_2 * \cdots * x_n$ is equal to the left-associated expression:

$$(\cdots((x_1 * x_2) * x_3) * \cdots) * x_n.$$

For any parenthesization, there is an outermost $*$, that is $A = B*C$, where $B = x_1*\cdots*x_m, C = x_{m+1}*\cdots*x_n$, both parenthesized in some unknown way, with $0 < m < n$. Applying the induction assumption,

$$B = (\cdots(x_1 * x_2) * \cdots) * x_m, \quad C = (\cdots(x_{m+1} * x_{m+2}) * \cdots) * x_n.$$

If $m = n-1$, we are already done. If not, $C = D*x_n$ for $D = (\cdots(x_{m+1}*x_{m+2})*\cdots)*x_{n-1}$ and $A = B*(D*x_n) = (B*D)*x_n$. By the induction assumption, $B*D = (\cdots(x_1*x_2)*\cdots)*x_{n-1}$ which completes the proof. □

Remark. Generalized associativity implies that for an associative operation parenthesis may be omitted.

Definition. Let $*$ be a binary operation on a set X. An element $e \in X$ is an **identity element** or **neutral element** with respect to $*$ if $e * x = x * e = x$ for any $x \in X$.

Examples.

1. $X = \mathbb{R}, a * b = a + b, e = 0$
2. $X = \mathbb{R}, a * b = ab, e = 1$
3. For a given set M, let X be the set of all maps from M to M and $f * g = f \circ g$. Then id_X is an identity element
4. $X = \mathbb{R}, a * b = a - b$ has no identity element

Lemma 1.2. *Let $*$ be a binary operation on a set X. If an identity for $*$ exists, it is unique.*

Proof. If $e, e' \in X$ are identity elements then $e = e * e' = e'$. □

Remark. The identity element is generally denoted by e.

Definition. Let $*$ be a binary operation on a set X with identity element e. An element $y \in X$ is an **inverse** (with respect to $*$) of $x \in X$ if $y * x = x * y = e$. An element is **invertible** if it has an inverse.

Remark. The identity element is always invertible.

Examples.

1. $X = \mathbb{R}, a * b = a + b$, any element is invertible
2. $X = \mathbb{R}, a * b = ab$, any element except 0 is invertible
3. $X = \mathbb{Z}, a * b = ab$, the only invertible elements are ± 1
4. For a given set M, let X be the set of all maps from M to M and $f * g = f \circ g$. Then f is invertible iff f is bijective

Lemma 1.3. *Let $*$ be an associative operation on X with identity element e. If an inverse of $x \in X$ exists, it is unique.*

Proof. Let y, y' be inverse elements of x whence $y * x = e$ and $x * y' = e$. Then by associativity

$$y' = e * y' = (y * x) * y' = y * (x * y') = y * e = y.$$

□

Remark. If the operation is denoted as an addition, the inverse of x is denoted $-x$. Otherwise, the inverse of x is generally denoted x^{-1}.

Proposition 1.4. *For an associative operation $*$ on X with identity element e*

1. *if $a \in X$ is invertible then a^{-1} is also invertible and $(a^{-1})^{-1} = a$*

2. *if $a, b \in X$ are invertible then $a * b$ is also invertible and $(a * b)^{-1} = b^{-1} * a^{-1}$.*

Proof. The identities $a^{-1} * a = a * a^{-1} = e$ imply that a is the inverse of a^{-1}. Also one has

$$(b^{-1} * a^{-1}) * (a * b) = (b^{-1} * (a^{-1} * a)) * b = (b^{-1} * e) * b = b^{-1} * b = e$$

and

$$(a * b) * (b^{-1} * a^{-1}) = (a * (b * b^{-1})) * a^{-1} = (a * e) * a^{-1} = a * a^{-1} = e.$$

□

Exercise 1.2. *Let $X = \mathbb{R}$ and $a * b = a + b + ab$.*
i) *Is the operation $*$ associative?*
ii) *Does the operation $*$ possess an identity element?*
iii) *Find all $x \in X$ which are not invertible.*

2 Residue classes

Definition. Let $m \in \mathbb{N}$. Integers a and b are **congruent** modulo m if $a - b$ is divisible by m. Notation: $a \equiv b \pmod{m}$, $a \equiv_m b$.

Example. $1 \equiv -2 \pmod 3, 1 \not\equiv 2 \pmod 3$

Proposition 2.1. *Let $m \in \mathbb{N}$.*

1. *$a \equiv a \pmod{m}$ for any $a \in \mathbb{Z}$*

2. *if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$ for any $a, b \in \mathbb{Z}$*

3. *if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ for any $a, b, c \in \mathbb{Z}$*

4. *if $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ and $a_1 b_1 \equiv a_2 b_2 \pmod{m}$ for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}$*

5. *every integer is congruent modulo m exactly to one of $0, 1, \ldots, m-1$.*

Proof. 1. $a - a = 0$ is divisible by m.

2. If $a - b$ is divisible by m, then $b - a = -(a - b)$ is divisible by m.

3. If $a - b$ and $b - c$ are divisible by m, then $a - c = (a - b) + (b - c)$ is divisible by m.

4. If $a_1 - a_2$ and $b_1 - b_2$ are divisible by m, then $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$ and $a_1 b_1 - a_2 b_2 = (a_1 - a_2) b_1 + a_2 (b_1 - b_2)$ are divisible by m.

5. Let $n \in \mathbb{Z}$. Let $n = mq + r$, where $0 \leq r \leq m - 1$ is the remainder; then $n - r$ is divisible by m and $n \equiv r \pmod{m}$. On the other hand, if $n \equiv r_1 \pmod{m}, n \equiv r_2 \pmod{m}$ and $0 \leq r_1, r_2 \leq m - 1$, then $r_1 \equiv r_2 \pmod{m}$, i.e., $m \mid r_1 - r_2$. This and the inequality $|r_1 - r_2| \leq m - 1$ imply $r_1 = r_2$.

□

Proposition 2.1 implies that $\equiv_m$ is an equivalence relation on $\mathbb{Z}$ and its quotient set $\mathbb{Z}/m\mathbb{Z}$ contains m elements.

Definition. The elements of $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ are called the **residue classes** modulo m.

Remark. $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$.

Introduce on $\mathbb{Z}/m\mathbb{Z}$ addition $+$ and multiplication $\cdot$. If $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$, we define

$$\overline{a} + \overline{b} = \overline{a + b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}.$$

It is necessary to verify that the results of these operation do not depend on the choice of representatives, i.e., the operations are well-defined.

Let a', b' be other representatives of the equivalence classes $\overline{a}, \overline{b}$, i.e. $\overline{a'} = \overline{a}$ and $\overline{b'} = \overline{b}$. Then $a' \equiv a \pmod{m}$, $b' \equiv b \pmod{m}$. It remains to check that $\overline{a + b} = \overline{a' + b'}$ and $\overline{ab} = \overline{a'b'}$, i.e., $a' + b' \equiv a + b \pmod{m}$ and $a'b' \equiv ab \pmod{m}$. These congruences follow from Proposition 2.1.

Remark. Why does one need to check the well-definedness of the operations? Let us define an operation $*$ on $\mathbb{Z}/2\mathbb{Z}$ by $\overline{a} * \overline{b} = \overline{[\frac{a+b}{2}]}$, where $[\alpha]$ denotes the integer part of $\alpha \in \mathbb{Q}$. Then $\overline{1} = \overline{[\frac{1+1}{2}]} = \overline{1} * \overline{1} = \overline{3} * \overline{1} = \overline{[\frac{3+1}{2}]} = \overline{2}$, which is obviously false. The operation $*$ is not well-defined.

Example. Addition and multiplication tables for $\mathbb{Z}/3\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Exercise 2.1. *Write the addition and multiplication tables for* $\mathbb{Z}/4\mathbb{Z}$

Proposition 2.2. *Let* $m \in \mathbb{N}$.

1. *Addition in $\mathbb{Z}/m\mathbb{Z}$ is commutative and associative*
2. *$\overline{0}$ is the identity element in $\mathbb{Z}/m\mathbb{Z}$ with respect to addition If $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ then $\overline{-a}$ is its additive inverse*

Proof. 1. For any $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$, one has

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}.$$

Similarly,

$$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b+c} = \overline{a + (b+c)} = \overline{(a+b)+c} = \overline{a+b} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}.$$

2. For any $\overline{x} \in \mathbb{Z}/m\mathbb{Z}$, one has $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$ and $\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}$.

□

Proposition 2.3. *Let $m \in \mathbb{N}$.*

1. *Multiplication in $\mathbb{Z}/m\mathbb{Z}$ is commutative and associative*
2. *$\overline{1}$ is the identity element in $\mathbb{Z}/m\mathbb{Z}$ with respect to multiplication*
3. *$\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ is invertible with respect to multiplication iff $\gcd(a, m) = 1$. In particular if p is prime, all non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ are invertible with respect to multiplication*

Proof. 1. For any $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$, one has

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}.$$

Similarly,

$$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}.$$

2. For any $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$, one has $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}$.

3. If $a \in \mathbb{Z}$ and $\gcd(a, m) = 1$ then $ab + mn = 1$ for some $b, n \in \mathbb{Z}$ by Bézout's identity. Then $\overline{a}\overline{b} = \overline{ab} = \overline{1 - mn} = \overline{1}$. Conversely, if $\overline{a}\overline{b} = \overline{1}$ for some $b \in \mathbb{Z}$ then $\overline{ab} = \overline{1}$ whence $ab = 1 + mn$ for some $n \in \mathbb{Z}$. This implies $\gcd(a, m) = 1$.

□

Example. $\overline{5}^{-1} = \overline{3}$ in $\mathbb{Z}/7\mathbb{Z}$ since $\overline{5} \cdot \overline{3} = \overline{15} = \overline{1}$.

Exercise 2.2. *Solve the below equations in $\mathbb{Z}/7\mathbb{Z}$*

i) $x^2 + \overline{2}x - \overline{1} = \overline{0}$
ii) $\overline{2}x^2 + \overline{3}x + \overline{2} = \overline{0}$

3 Permutations

Definition. A **permutation** of n elements is a bijection from the set $\{1, \ldots, n\}$ to itself. The **identity permutation** is the identity map of this set. The **product** of two permutations is their composition.

Let σ be a permutation of n elements. Then it is defined by the data $\sigma(1), \ldots, \sigma(n)$. It leads to two notations used to represent permutations, two-line and one-line notations, respectively:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \quad \text{and} \quad \Big(\sigma(1)\sigma(2)\cdots\sigma(n)\Big).$$

The identity permutation then is represented as $(12\ldots n)$.

The product of two permutations can be easily found when they are represented in two-line notation. Let

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Then

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

since $\pi \circ \rho(1) = \pi(4) = 3, \pi \circ \rho(2) = \pi(3) = 2, \pi \circ \rho(3) = \pi(1) = 1, \pi \circ \rho(4) = \pi(2) = 4$.

Every bijection has the inverse map, and its representation can be found by swapping the lines in two-line notation and arranging the firs line in ascending order:

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \quad \rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

Definition. Let σ be a permutation of n elements, $1 < k \leq n$ and there are k distinct numbers $1 \leq m_1, \ldots, m_k \leq n$ such that

i) $\sigma(m_i) = m_{i+1}$ for $1 \leq i \leq k-1$

ii) $\sigma(m_k) = m_1$

iii) $\sigma(t) = t$ for $t \neq m_1, \ldots, m_k$

Such permutations is called a **cyclic permutation** or a k-**cycle**. The set $\{m_1, \ldots, m_k\}$ is the **support** of σ.

Two cycles are **disjoint** if their supports do not intersect.

Proposition 3.1 (Cycle decomposition)**.** *1. Any non-identity permutation can be uniquely expressed as a product of disjoint cycles.*

2. Disjoint cycles commute.

Example. The below permutation is expressed as the product of a 2-cycle and a 3-cycle.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$$

4 Basic definitions and examples

Definition. A set G with binary operation $*$ is a **group** if:

I. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$ (**associativity**)

II. There exists $e \in G$ (an **identity element**) such that $a * e = e * a = a$ for any $a \in G$

III. For any $a \in G$ there is $a' \in G$ (an **inverse** of a) such that $a * a' = a' * a = e$

A group G is **commutative**, or **abelian** if $a * b = b * a$ for all $a, b \in G$. A group is **finite** if it has a finite number of elements. The **order** of a group is the number of its elements.

Examples.

1. If $k = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ then k with respect to addition is an abelian group (the **additive group** of k).

2. If $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ then $k^* = k \setminus \{0\}$ with respect to multiplication is an abelian group (the **multiplicative group** of k).

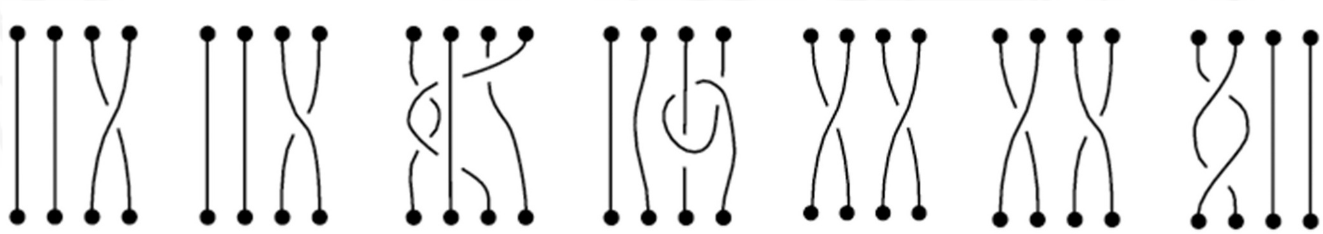
3. The set of all invertible matrices over $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with respect to multiplication $\mathrm{GL}_n(k)$ is a non-abelian group (the **general linear group**).

4. $T = \{z \in \mathbb{C} \mid |z| = 1\}$ with respect to multiplication is an abelian group

5. The set of all permutations of n elements with respect to multiplication S_n is a non-abelian group (the **symmetric group**)

6. The set of all isometries of a fixed regular n-gon with respect to composition D_n is a non-abelian group (the **dihedral group**). It consists of n rotations and n reflections and thus $|D_n| = 2n$.

7. The set of all braids one can make with n strands under concatenation is a non-abelian group. Its identity element is the untangled braid. If one starts with a set of straight strands whose ends are tied off, tangles it while leaving the ends tied, and then partitions it into two braids, one braid is the inverse of the other.



1 2 3 4 5 6 7

Braids 1 and 2 are different, braids 1 and 3 are considered as the same. Braid 4 is not considered a braid as the strands are required to move upside down. The concatenation of braids 5 and 6 yields braid 7.

8. The following are not groups:

   - The non-negative integers with respect to addition
   - $\mathbb{R}$ with respect to multiplication
   - $\mathbb{Z} \setminus \{0\}$ with respect to addition
   - The odd integers together with 0 with respect to addition

Lemma 4.1 (Cancellation property). *Let G be a group with binary operation $*$. If $g*h = g*h'$ for some $g, h, h' \in G$ then $h = h'$.*

Proof. One has $h = e*h = (g^{-1}*g)*h = g^{-1}*(g*h) = g^{-1}*(g*h') = (g^{-1}*g)*h' = e*h' = h'$. ☐

Let G, H be groups with operations $*, \star$ respectively. On the set $G \times H$, introduce an operation:

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 * g_2, h_1 \star h_2) \text{ for } g_1, g_2 \in G, h_1, h_2 \in H.$$

Proposition 4.2. *$G \times H$ with respect to the operation $\bullet$ is a group.*

Proof. I. For any $g_1, g_2, g_3 \in G, h_1, h_2, h_3 \in H$ one has $\Big((g_1, h_1) \bullet (g_2, h_2)\Big) \bullet (g_3, h_3) = (g_1 * g_2, h_1 \star h_2) \bullet (g_3, h_3) = ((g_1 * g_2) * g_3, (h_1 \star h_2) \star h_3) = (g_1 * (g_2 * g_3), h_1 \star (h_2 \star h_3)) = (g_1, h_1) \bullet (g_2 * g_3, h_2 \star h_3) = (g_1, h_1) \bullet \Big((g_2, h_2) \bullet (g_3, h_3)\Big)$ since both $*$ and $\star$ are associative

II. Let e_G, e_H be the identity elements of G, H, respectively. Then (e_G, e_H) is the identity elements of $G \times H$ since $(g, h) \bullet (e_G, e_H) = (g * e_G, h \star e_H) = (g, h)$ and $(e_G, e_H) \bullet (g, h) = (e_G * g, e_H \star h) = (g, h)$ for any $g \in G, h \in H$.

III. For any $g \in G, h \in H$ one has $(g, h) \bullet (g^{-1}, h^{-1}) = (g * g^{-1}, h \star h^{-1}) = (e_G, e_H)$ and $(g^{-1}, h^{-1}) \bullet (g, h) = (g^{-1} * g, h^{-1} \star h) = (e_G, e_H)$.

☐

Definition. $G \times H$ with above defined operation $\bullet$ is called the **direct product** of the groups G and H.

Exercise 4.1. *Let G be a group with operations $*$. Prove that G with respect to the operation $g_1 \bullet g_2 = g_2 * g_1$ is also a group.*

Exercise 4.2. *Show that the set of functions $f(t) = \frac{at+b}{ct+d}$ where $a, b, c, d \in \mathbb{R}, ad - bc \neq 0$ is a group with respect to composition.*

Exercise 4.3. *Which of the below subsets of $\mathbb{Z}/10\mathbb{Z}$ form groups with respect to multiplication?*

i) $\{\bar{1}, \bar{9}\}$

ii) $\{\overline{1}, \overline{7}\}$
iii) $\{\overline{1}, \overline{3}, \overline{7}\}$
iv) $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

Remark. In what follows the symbol $*$ will be often omitted in the notation of the group operation *(juxtaposition).*

Definition. Let G be a finite group consisting of the elements $e = g_1, g_2, g_3, \cdots, g_n$. The **Cayley table** of G has $g_i g_j$ at its (i, j)th position.

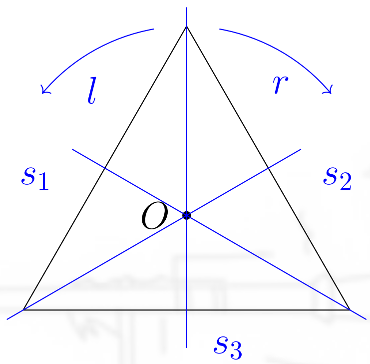
	e	g_2	g_3	$\cdots$	g_n
e	e	g_2	g_3	$\cdots$	g_n
g_2	g_2	g_2g_2	g_2g_3	$\cdots$	g_2g_n
g_3	g_3	g_3g_2	g_3g_3	$\cdots$	g_3g_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
g_n	g_n	g_ng_2	g_ng_3	$\cdots$	g_ng_n

Examples. 1. The Cayley table of the additive group of $\mathbb{Z}/m\mathbb{Z}$ is its addition table

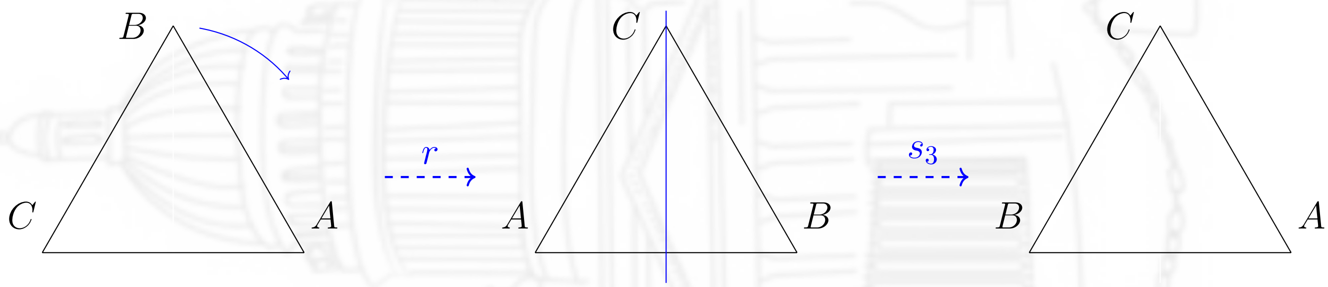
2. Let $S_3 = \{(123), (213), (132), (321), (231), (312)\}$.

	(123)	(213)	(132)	(321)	(231)	(312)
(123)	(123)	(213)	(132)	(321)	(231)	(312)
(213)	(213)	(123)	(231)	(312)	(132)	(321)
(132)	(132)	(312)	(123)	(231)	(321)	(213)
(321)	(321)	(231)	(312)	(123)	(213)	(132)
(231)	(231)	(321)	(213)	(132)	(312)	(123)
(312)	(312)	(132)	(321)	(213)	(123)	(231)

3. Consider a regular triangle with center O. Then $D_3 = \{e, r, l, s_1, s_2, s_3\}$ where e is the identity map, r is the clockwise rotation about O by $120°$, l is the counterclockwise rotation about O by $120°$, and s_1, s_2, s_3 are the reflections across the lines connecting the midpoints of each side to the opposite vertices.



Example of calculation: $s_3 r = s_1$.



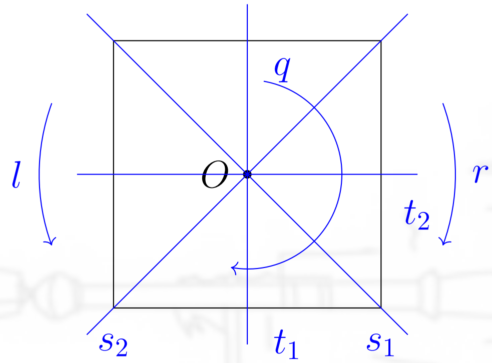
	e	l	r	s_1	s_2	s_3
e	e	l	r	s_1	s_2	s_3
l	l	r	e	s_2	s_3	s_1
r	r	e	l	s_3	s_1	s_2
s_1	s_1	s_3	s_2	e	r	l
s_2	s_2	s_1	s_3	l	e	r
s_3	s_3	s_2	s_1	r	l	e

Proposition 4.3. *1. A group is commutative if and only if its Cayley table is symmetric.*

2. Each row and column of the Cayley table is a permutation of the elements of the group.

Proof. The first part is trivial. If $gg' = gg''$ then cancelling out g yields $g' = g''$ and thus the elements of each row are distinct. □

Exercise 4.4. *Draw the Cayley table of the group D_4. Consider a square with center O. Let e be the identity map, r is the clockwise rotation about O by $90°$, l is the counterclockwise rotation about O by $90°$, q be the rotation about O by $180°$ (= a point reflection), s_1, s_2 be the reflections across the diagonals, t_1, t_2 be the reflections across the lines connecting the midpoints of the opposite edges. Then $D_4 = \{e, r, l, q, t_1, t_2, s_1, s_2\}$.*



Exercise 4.5. *Are the below tables the Cayley tables of certain groups?*

	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	a	b
d	c	d	b	a

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

5 Subgroups

Definition. Let G be group. A non-empty subset $H \subset G$ is a **subgroup** of G (notation: $H < G$) if

I. $hh' \in H$ for any $h, h' \in H$.
II. $h^{-1} \in H$ for any $h \in H$.

Lemma 5.1. *If $H < G$ then $e \in H$.*

Proof. If $h \in H$ then $h^{-1} \in H$ and $e = hh^{-1} \in H$. □

Remark. If H is a subgroup of G, then the H with respect to the restriction of the group operation from G is a group.

Examples. 1. In any group G, there are **trivial** subgroups $\{e\} < G$ and $G < G$.

2. For $m \in \mathbb{N}$, the set $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

3. The set of complex nth roots of unity T_n is a subgroup of $T = \{z \in \mathbb{C} \mid |z| = 1\}$.

4. The set of positive real numbers $\mathbb{R}_{>0}$ is a subgroup of the multiplicative group of $\mathbb{R}$.

5. The set of all matrices with determinant 1 over $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ $\mathrm{SL}_n(k)$ is a subgroup of $\mathrm{GL}_n(k)$ (the **special linear group**).

6. The set of all permutations of n elements with a given fixed point is a subgroup of S_n.

7. The set of all the even permutations of n elements A_n is a subgroup of S_n (the **alternating group**).

8. The subset of all rotations in D_n is a subgroup.

Theorem 5.2. *Any subgroup G of the additive group $\mathbb{Z}$ has the form $m\mathbb{Z}$ for some a non-negative $m \in \mathbb{Z}$.*

Proof. If $G = \{0\}$, one can take $m = 0$. Otherwise, choose m, the least positive element of G, and show that $G = m\mathbb{Z}$. First, for $a \in \mathbb{N}$ one has $ma = \underbrace{m + \cdots + m}_{a \text{ times}} \in G$ and $m(-a) = (-m)a = \underbrace{(-m) + \cdots + (-m)}_{a \text{ times}} \in G$; thus $m\mathbb{Z} \subset G$.

Conversely, let $g \in G$ and $g = mq + r$, $0 \le r < m$. Since $g, mq \in G$, one has $r = g - mq \in G$. Then r must be zero and $g = mq \in m\mathbb{Z}$. □

Lemma 5.3. *Let $\{H_i\}_{i \in I}$ be a family of subgroups of a group G and $H = \bigcap_{i \in I} H_i$. Then $H < G$.*

Proof. If $h, h' \in H$, then $h, h' \in H_i$ for every $i \in I$. Then $hh', h^{-1} \in H_i$ for every $i \in I$, whence $hh', h^{-1} \in H$. □

Exercise 5.1. *Prove that the orthogonal matrices $\{A \in \mathrm{M}_n(\mathbb{R}) \mid AA^T = E_n\}$ form a subgroup of $\mathrm{GL}_n(\mathbb{R})$.*

Exercise 5.2. *Let G, G' be groups and $H < G, H' < G'$. Show that $H \times H' < G \times G'$.*

Problem 5.4. *Prove that the only non-trivial subgroup of $\mathbb{Z}/4\mathbb{Z}$ is $\{\overline{0}, \overline{2}\}$.*

Solution. Let H be a subgroup of $\mathbb{Z}/4\mathbb{Z}$. If $\overline{1}$ or $\overline{3}$ belongs to H then $H = G$ since $G = \{\overline{0}, \overline{1}, \overline{1} + \overline{1}, \overline{1} + \overline{1} + \overline{1}\} \subset H$ and similarly for $\overline{3}$. Since $\overline{0} \in H$, there are only two options remain: $\{\overline{0}\}$ or $\{\overline{0}, \overline{2}\}$. □

Exercise 5.3. *Find all the non-trivial subgroups of $\mathbb{Z}/6\mathbb{Z}$.*

Exercise 5.4. *Prove that the only finite subgroup of $\mathbb{R}^*$ is $\{\pm 1\}$.*

Definition. Let $X \subset G$ be a subset of a group G. The smallest subgroup of G containing X is called the **subgroup generated by** X, and is denoted by $\langle X \rangle$. Thus $\langle X \rangle$ is defined by the following conditions: $X \subset \langle X \rangle$ and if $H < G$, $X \subset H$, then $\langle X \rangle \subset H$. Clearly the subgroup generated by X is unique (if exists).

If $\langle X \rangle = G$, the group G is said to be **generated** by X, or X is a **generating set** of G or a set of **generators** of G.

Remark. For a finite set $X = \{x_1, \ldots, x_n\}$, we often write $\langle x_1, \ldots, x_n \rangle$ instead of $\langle \{x_1, \ldots, x_n\} \rangle$.

Proposition 5.5. *Let G be a group, $X \subset G$. The intersection of all subgroups of G, containing X is the subgroup generated by X.*

Proof. By Lemma 5.3, the intersection of all subgroups of G containing X is a subgroup of G. Denote it by $\langle X\rangle$. The set X is contained in all the intersecting subgroups, thus it is contained in $\langle X\rangle$. On the other hand, if a subgroup H contains X, then H is one of the intersecting subgroups and $\langle X\rangle \subset H$. $\square$

Remark. The above statement proves the existence of $\langle X\rangle$.

Proposition 5.6. *Let G be a group, $X \subset G$. The subgroup generated by X is the set of all the products of elements of X and and their inverses:*

$$\langle X\rangle = \{y_1^{\varepsilon_1}\cdots y_n^{\varepsilon_n} \mid y_i \in X, \varepsilon_i = \pm 1 \text{ for all } i = 1,\dots,n\}.$$

Proof. Denote the set of all the products of elements of X and their inverses by Y. First prove that $Y \subset \langle X\rangle$. Let $y = y_1^{\varepsilon_1}\cdots y_n^{\varepsilon_n} \in Y$. If $H < G$ is an arbitrary subgroup containing X, then H also contains $y_1^{\varepsilon_1},\dots,y_n^{\varepsilon_n}$, and thus contains their product y. Therefore y belongs to the intersection of all such subgroups H, which is equal to $\langle X\rangle$ by Proposition 5.5.

Conversely, one can easily verify that Y is a subgroup of G. Since $X \subset Y$, the inverse inclusion $\langle X\rangle \subset Y$ follows. $\square$

Examples. 1. $\mathbb{Z}$ is generated by 1.

2. $\mathbb{Q}$ is not generated by any finite subset.

3. S_3 is not generated by any single element, but is generated by any set that contains a transposition and a 3-cycle. For example, $S_3 = \langle(132),(231)\rangle$ since $(132)(231) = (321), (231)(132) = (213), (231)^{-1} = (312)$.

Problem 5.7. *Prove that the only non-trivial subgroups of D_3 are $\{e,r,l\},\{e,s_1\},\{e,s_2\},\{e,s_3\}$.*

Solution. Using the Cayley table of D_3, one can see that any set that contains a non-identity rotation and a reflection is a generating set. Thus it remains to consider only subgroups whose non-identity elements are either reflections or rotations. The composition of two different reflections is a non-identity rotation whence a reflection in the subgroup must be unique and the possible subgroups for this case are $\{e,s_1\},\{e,s_2\},\{e,s_3\}$. The inverse of one non-identity rotation is another, thus both must be in the subgroup which gives the only possible subgroup $\{e,r,l\}$. $\square$

Exercise 5.5. *Find all the non-trivial subgroups of D_4.*

6 Order of element

Definition. Let G be a group, $g \in G$ and $n \in \mathbb{Z}$. Define the nth **power** of g by

$$g^n = \begin{cases} \underbrace{gg\cdots g}_{n \text{ times}}, & \text{if } n > 0 \\ \underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{-n \text{ times}}, & \text{if } n < 0 \\ e, & \text{if } n = 0 \end{cases}$$

Proposition 6.1. *For any $g \in G$ and $m, n \in \mathbb{Z}$*

1. $g^{n+m} = g^n g^m$
2. $(g^n)^m = g^{nm}$

Proof. Assume for example that $n > 0, m < 0, n+m > 0$. Then

$$g^{n+m} = \underbrace{gg\cdots g}_{n+m \text{ times}} = \underbrace{gg\cdots g}_{n-(-m) \text{ times}} = \underbrace{gg\cdots g}_{n \text{ times}}\underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{-m \text{ times}} = g^n g^m.$$

The other cases are treated similarly. □

Remark. When the group operation is given by addition, the identity element is denoted by 0, and the inverse of g is $-g$. In this case, the nth power of g is written as ng. This notation is called the **additive** notation, as opposed to the default **multiplicative** notation.

Definition. Let G be a group and $g \in G$. The **order** of g (denoted by $\operatorname{ord}_G g$ or simply $\operatorname{ord} g$) is the least $m \in \mathbb{N}$ such that $g^m = e$. If $g^m \neq e$ for any $m \in \mathbb{N}$, then g is said to be of **infinite order**.

Examples.

1. The order of the identity element is 1, and it is the only element with this property.
2. $\operatorname{ord}_{(\mathbb{Z}/7\mathbb{Z})^*} \overline{2} = 3$, since $2^3 \equiv 1 \pmod 7$ and $2^1, 2^2 \not\equiv 1 \pmod 7$.
3. $\operatorname{ord}_{\mathbb{Z}/7\mathbb{Z}} \overline{2} = 7$, since $7 \cdot 2 \equiv 0 \pmod 7$ and $1 \cdot 2, 2 \cdot 2, 3 \cdot 2, 4 \cdot 2, 5 \cdot 2, 6 \cdot 2 \not\equiv 0 \pmod 7$.
4. $\operatorname{ord}_{\mathbb{Z}} 1 = \infty$.
5. In D_3, the order of every reflection is 2 and the order of every non-identity rotation is 3.

Problem 6.2. *Prove that* $\operatorname{ord} g^{-1} = \operatorname{ord} g$.

Solution. Since $(g^{-1})^m = g^{-m} = (g^m)^{-1}$, one has $(g^{-1})^m = e$ iff $g^m = e$. Thus the smallest $m > 0$ satisfying one of these conditions is the same as the smallest $m > 0$ that satisfies another (or both do not exist). □

Exercise 6.1. *Let G be a group and $g, h \in G$. Show that* $\operatorname{ord} gh = \operatorname{ord} hg$.

Proposition 6.3. *Let $g \in G$ be an element of finite order n. If $m \in \mathbb{Z}$, then $g^m = e$ if and only if $n|m$.*

Proof. If $m = ns + r, 0 \leq r < n$ then $g^m = g^{ns+r} = (g^n)^s g^r = e^s g^r = g^r$. If $r = 0$, then $g^m = e$. If $r \neq 0$, then $g^r \neq e$ since $r < n, g^n = e$ and n is the least exponent satisfying this property. □

Exercise 6.2. *Show that* $\operatorname{ord} g^s = n/d$ *where* $n = \operatorname{ord} g, d = \gcd(n, s)$.

Hint. Use Proposition 6.3.

Proposition 6.4. *If G is a group and $g \in G$ then $|\langle g \rangle| = \operatorname{ord}(g)$.*

Proof. If $\operatorname{ord} g$ is a finite n it suffices to prove that $g^m = g^{m'}$ iff $m \equiv m' \pmod{n}$ which will imply that $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$. Now $g^m = g^{m'}$ iff $g^{m-m'} = e$ iff $m \equiv m' \pmod{n}$ by Proposition 6.3. If g is of infinite order, then $g^m \neq g^{m'}$ for distinct m, m' since otherwise $g^{m'-m} = e$ for $|m - m'| \in \mathbb{N}$. □

Proposition 6.5. *Let G be a group, $a, b \in G$ commute and $\langle a \rangle \cap \langle b \rangle = \{e\}$. If $\operatorname{ord} a = n, \operatorname{ord} b = m$, then $\operatorname{ord} ab = \operatorname{lcm}(n, m)$.*

Proof. Let $N = \operatorname{lcm}(n, m)$. Then $n, m | N$, whence $a^N = b^N = e$ and $(ab)^N = a^N b^N = e$. If $(ab)^k = e$ for some $k > 0$ then $a^k = b^{-k}$ and $a^k = b^k = e$. Now Proposition 6.3 implies $n, m \mid k$ whence $k \geq N$. □

Corollary 6.6. *The order of a permutation represented as the product of disjoint cycles equals the least common multiple of the length of these cycles.*

7 Cosets and normal subgroups

Definition. Let G be a group, $H < G$, and $g \in G$. The set

$$gH = \{gh \mid h \in H\}$$

is called a **left coset** of H. Similarly, the set

$$Hg = \{hg \mid h \in H\}$$

is a **right coset** of H.

The set of all left cosets of H is denoted by G/H.

Remarks. 1. $eH = He = H$.

2. If G is commutative, the left and right cosets coincide.

Definition. Let G be a group, $H < G$. Introduce the relations $\sim_H$ and ${}_H\!\sim$ on G : $g \sim_H g'$ if $g^{-1}g' \in H$ and $g\,{}_H\!\sim g'$ if $g'g^{-1} \in H$.

Remark. If G is commutative, the above relations coincide.

Proposition 7.1. *The relations $\sim_H$ and ${}_H\!\sim$ are equivalence relations; the equivalence class of $g \in G$ with respect to $\sim_H$ equals gH, and the equivalence class of $g \in G$ with respect to ${}_H\!\sim$ equals Hg.*

Proof. First prove that $\sim_H$ is an equivalence relation. For $g \in G$ one has $g^{-1}g = e \in H$, whence $g \sim_H g$. If $g \sim_H g'$, then $g^{-1}g' \in H$, so $g'^{-1}g = (g^{-1}g')^{-1} \in H$, whence $g' \sim_H g$. Finally, if $g \sim_H g'$ and $g' \sim_H g''$, then $g^{-1}g' \in H$ and $g'^{-1}g'' \in H$, so $g^{-1}g'' = (g^{-1}g')(g'^{-1}g'') \in H$ and $g \sim_H g''$.

Note that $y \in G$ belongs to the equivalence class of $g \in G$ if and only if $g \sim_H y$. This holds if and only if $g^{-1}y \in H$, that is $g^{-1}y = h$ for some $h \in H$. This, in turn, is equivalent to the fact that $y = gh$, i.e., $y \in gH$.

The statement about ${}_H\!\sim$ can be proved in a similar way. □

Corollary 7.2. *Let G be a group, $H < G$. The left (right) cosets of H form a partition of G.*

Examples. 1. $G = \mathbb{Z}, H = m\mathbb{Z}$, the left (= the right) cosets are $\{a + mn \mid m \in \mathbb{Z}\}, 0 \leq a \leq m-1$

2. $G = \mathbb{C}^*, H = T$, the left (= the right) cosets are $\{z \in \mathbb{C} \mid |z| = r\}, r > 0$

3. $G = D_3, H = \{e, s_1\}$, the left cosets are $\{e, s_1\}, \{r, s_3\}, \{l, s_2\}$, the right cosets are $\{e, s_1\}, \{r, s_2\}, \{l, s_3\}$

4. $G = D_3, H = \{e, r, l\}$, the left (= the right) cosets are $\{e, r, l\}, \{s_1, s_2, s_3\}$

Exercise 7.1. *Find the left and the right cosets for*
i) $G = D_4, H = \{e, s_1\}$
ii) $G = D_4, H = \{e, t_1\}$
iii) $G = D_4, H = \{e, q\}$

Definition. Let G be a group. A subgroup $H < G$ is called **normal** (notation: $H \triangleleft G$), if $Hg = gH$ for any $g \in G$.

Lemma 7.3. *Let G be a group, $H < G$. The following conditions are equivalent:*

1. *H is normal;*

2. *$ghg^{-1} \in H$ for all $g \in G, h \in H$.*

Proof. Let $Hg = gH$ and $h \in H$. Then $gh = h'g$ for some $h' \in H$ and $ghg^{-1} = h' \in H$.

Now assume that $ghg^{-1} = h' \in H$ for all $g \in G, h \in H$. Then $gh = h'g$, and hence $gH \subset Hg$. Similarly $g^{-1}h(g^{-1})^{-1} = h'' \in H$ for $g \in G, h \in H$, whence $hg = gh''$ and $Hg \subset gH$. □

Definition. Let G be a group, $g, h \in G$. The element ghg^{-1} is called a **conjugate** of h; or it is said that h and ghg^{-1} are **conjugate**.

Examples. 1. $\{e\} \triangleleft G, G \triangleleft G$.

2. Every subgroup of an abelian group is normal.

3. $\{e, r, l\}$ is a normal subgroup of D_3, $\{e, s_1\}$ is not a normal subgroup of D_3 .

4. $\mathrm{SL}_n(k) \triangleleft \mathrm{GL}_n(k)$. Indeed, if $h \in \mathrm{SL}_n(k)$ and $g \in \mathrm{GL}_n(k)$, then $\det(ghg^{-1}) = \det(g) \cdot \det(h) \cdot \det(g^{-1}) = \det(h) = 1$, so $ghg^{-1} \in \mathrm{SL}_n(k)$.

5. $A_n \triangleleft S_n$. Indeed, if $h \in A_n$ and $g \in S_n$, then $ghg^{-1} \in A_n$ as the product of an even permutation and two permutations of the same parity

Exercise 7.2. *Prove that* $\{A \in \mathrm{GL}_n(\mathbb{C}) \mid \det A \in \mathbb{R}\}$ *is a normal subgroup of* $\mathrm{GL}_n(\mathbb{C})$.

Exercise 7.3. *Prove that the intersection of two normal subgroups is a normal subgroup.*

Exercise 7.4. *Let $n \geq 3$ and $1 \leq m \leq n$. Prove that $\{\sigma \in S_n \mid \sigma(m) = m\}$ is not a normal subgroup of S_n.*

Exercise 7.5. *Let G be a group and $g_1 \sim g_2, g_1, g_2 \in G$ if g_1 is a conjugate of g_2.*

i) *Prove that the relation $\sim$ on G is an equivalence relation*

ii) *Find the partition of $G = D_3, D_4$ into the equivalence classes*

8 Lagrange's Theorem

Definition. Let G be a group, $H < G$. The number of the left cosets of H is called the **index** of H and is denoted by $|G : H|$.

Lemma 8.1. *Let G be a group, $H < G$. Then there is a bijection between the set of the left cosets of H and the set of the right cosets of H. In particular, these numbers are equal if one of them is finite.*

Proof. Consider $\varphi \colon G \to G, \varphi(g) = g^{-1}$. Then $\varphi(gH) = Hg^{-1}$ since for any $h \in H$ one has $\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1}$ and $h^{-1} \in H$, similarly for any $h \in H$ one has $hg^{-1} = (gh^{-1})^{-1} = \varphi(gh^{-1})$ and $h^{-1} \in H$. Since φ is a bijection, it induces bijection from the set of the left cosets to the set of the right cosets. □

Proposition 8.2. *Any subgroup of index 2 is normal.*

Proof. The set of left cosets G/H consists of two elements, one of them is H, denote another by A. Since the cosets form a partition of G, one has $A = G \setminus H$. Moreover, $gH = H$ if and only if $g \in H$. Then,

$$gH = \begin{cases} H, & \text{if } g \in H \\ G \setminus H, & \text{if } g \notin H \end{cases}.$$

Clearly, the same is true for Hg, so they are equal. □

Theorem 8.3 (Lagrange's Theorem)**.** *If G is a finite group, $H < G$, then $|G| = |H| \cdot |G : H|$.*

Proof. First prove that all the left cosets of H are equal-sized. Note that for each $g \in G$ the map $H \to gH$, $h \mapsto gh$, defines a bijection between H and gH. Indeed, if $gh = gh'$, then $h = h'$, and the subjectivity of this map follows from the definition of gH. Since H is one of the cosets, the number of element of any coset equals $|H|$. Thus, G is partitioned into $|G : H|$ cosets of size $|H|$ each which completes the proof. □

Corollary 8.4. *The order of a finite group G is divisible by the order of any of its element.*

Proof. Apply Lagrange's Theorem to the subgroup $\langle g \rangle$ whose order is equal to the order of g by Proposition 6.4. □

Corollary 8.5. *Let G be a finite group. Then $g^{|G|} = e$ for any $g \in G$.*

Proof. Let $\operatorname{ord} g = n$ and $nm = |G|$. Then $g^{|G|} = (g^n)^m = e^m = e$. □

Exercise 8.1. *Let H_1, H_2 be subgroups of a finite group G and $|H_1| = 15, |H_2| = 28$.*

i) *Find the minimum possible order of G.*

ii) *Prove that $H_1 \cap H_2 = \{e\}$.*

Theorem 8.6 (Euler). *Let $m \in \mathbb{N}, a \in \mathbb{Z}$, and $\gcd(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$, where $\varphi(m)$ is the Euler function defined as the number of integers k in the range $1 \leq k \leq n$ for which $\gcd(m, k) = 1$.*

Proof. Consider $G = \{\bar{b} \in \mathbb{Z}/m\mathbb{Z} \mid b \in \mathbb{Z}, \gcd(b, m) = 1\}$. It is a group under multiplication by Proposition 2.3 and $|G| = \varphi(m)$. Now $\bar{a} \in G$ and Corollary 8.5 implies $\bar{a}^{\varphi(m)} = \bar{1}$ which gives the required congruence. □

Example. For $m = 10$ one has $\varphi(m) = 4$ whence $3^4 \equiv 1 \mod 10$.

9 Quotient group and commutator subgroup

Let G be a group, and $H \triangleleft G$. Introduce a binary operation on G/H:

$$(gH)(g'H) = (gg')H, \quad gH, g'H \in G/H.$$

Theorem 9.1. *The above operation is well-defined and is a group operation on G/H.*

Proof. One has to verify that $(\widetilde{g}\widetilde{g}')H = (gg')H$ if $\widetilde{g} \in gH$ and $\widetilde{g}' \in g'H$. These conditions imply $\widetilde{g} = gh$, $\widetilde{g}' = g'h'$ for some $h, h' \in H$; then $\widetilde{g}\widetilde{g}' = (gh)(g'h') = g(hg')h'$. Since $H \triangleleft G$, $hg' = g'h''$ for some $h'' \in H$, one has $\widetilde{g}\widetilde{g}' = gg'h''h' \in gg'H$.

The identity element of G/H is the coset $eH = H$, since $(eH)(gH) = (eg)H = gH = (ge)H = (gH)(eH)$ for any $g \in G$. Further, for $g, g', g'' \in G$ one has $((gH)(g'H))(g''H) = (gg'H)(g''H) = (gg')g''H = g(g'g'')H = (gH)(g'g''H) = (gH)((g'H)(g''H))$. Finally, the coset $g^{-1}H$ is the inverse of gH since $(gH)(g^{-1}H) = gg^{-1}H = eH = g^{-1}gH = (g^{-1}H)(gH)$. □

Definition. The set of left cosets G/H together with above operation is called the **quotient group** of G by H.

Examples.

1. G/G is a one-element group.
2. $G/\{e\}$ can be identified with G. Indeed, each coset of $\{e\}$ is of the form $\{g\}, g \in G$ and hence can identified with g. Clearly, under this identification the operation on the quotient group corresponds to the group operation on G: $\{g\}\{g'\} = \{gg'\}$.
3. The construction of the residue classes modulo n and the definition of addition on them is a particular case of the quotient group G/H for $G = \mathbb{Z}, H = n\mathbb{Z}$.
4. $G = D_4, H = \{e, q\}$. Then G/H contains the following cosets: $H = \{e, q\}, rH = \{r, l\}, s_1H = \{s_1, s_2\}, t_1H = \{t_1, t_2\}$ and its Cayley table is

	H	rH	s_1H	t_1H
H	H	rH	s_1H	t_1H
rH	rH	H	t_1H	s_1H
s_1H	s_1H	t_1H	H	rH
t_1H	t_1H	s_1H	rH	H

Example of calculation: $(s_1H)(rH) = s_1rH = t_2H = t_1H$ since $s_1r = t_2$.

Exercise 9.1. *Consider the group* $G = \{ax \mid a \in (\mathbb{Z}/13\mathbb{Z})^*\} \cup \{a/x \mid a \in (\mathbb{Z}/13\mathbb{Z})^*\}$ *with respect to composition* ($|G| = 24$) *and its subgroups* $H = \{x, \overline{3}x, \overline{9}x\}$, $H' = \{\pm x, \pm\overline{3}/x\}$.

i) *Find the left cosets of* H

ii) *Show that* $H \triangleleft G$

iii) *Show that* H' *is not normal*

iv) *Draw the Cayley table of* G/H

Definition. Let G be a group, $x, y \in G$. The element $[x, y] = xyx^{-1}y^{-1}$ is called the **commutator** of x, y. The subgroup $\langle\{[x, y] \mid x, y \in G\}\rangle$ is the **commutator subgroup** of G and is denoted by $K(G)$.

Theorem 9.2. *Let* G *be a group. Then*

1. $K(G) \triangleleft G$ *and* $G/K(G)$ *is commutative*

2. *If* $H \triangleleft G$ *and* G/H *is commutative, then* $K(G) \subset H$.

Proof. First note that $[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$ whence by Proposition 5.6

$$K(G) = \{[x_1, y_1] \cdots [x_n, y_n] \mid x_1, y_1 \ldots, x_n, y_n \in G\}.$$

Now the identities

$$g([x_1, y_1] \cdots [x_n, y_n])g^{-1} = (g[x_1, y_1]g^{-1})(g[x_2, y_2]g^{-1}) \cdots (g[x_n, y_n]g^{-1})$$

and

$$g[x, y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxyx^{-1}(g^{-1}y^{-1}yg)y^{-1}g^{-1} = (gx)y(gx)^{-1}y^{-1}ygy^{-1}g^{-1} = [gx, y][y, g]$$

imply that $K(G) \triangleleft G$. Furthermore,

$$\begin{aligned}(xK(G))(yK(G))(xK(G))^{-1}(yK(G))^{-1} &= (xK(G))(yK(G))(x^{-1}K(G))(y^{-1}K(G)) \\ &= (xyx^{-1}y^{-1})K(G) = [x, y]K(G) = K(G)\end{aligned}$$

and hence $(xK(G))(yK(G)) = (yK(G))(xK(G))$ for any $x, y \in G$, i.e. $G/K(G)$ is commutative.

Suppose $H \triangleleft G$. If G/H is commutative, then $(xH)(yH) = (yH)(xH)$ for any $x, y \in G$. Hence $H = (xH)(yH)(xH)^{-1}(yH)^{-1} = (xyx^{-1}y^{-1})H = [x, y]H$, so $[x, y] \in H$. Hence $K(G) \subset H$. □

Examples. 1. G is commutative iff $K(G) = \{e\}$

2. $K(S_3) = \{(123), (231), (312)\}$ since $\{(123), (231), (312)\}$ is a normal subgroup (is of index 2), the quotient group by it is commutative and S_3 is not commutative

3. $K(D_4) = \{e, q\}$ since $\{e, q\}$ is a normal subgroup, the quotient group by it is commutative (see an example above) and D_4 is not commutative

Problem 9.3. *Prove that* $K(\mathrm{GL}_2(\mathbb{R})) = K(\mathrm{SL}_2(\mathbb{R})) = \mathrm{SL}_2(\mathbb{R})$.

Solution. For any $A, B \in \mathrm{GL}_2(\mathbb{R})$ one has $\det[A, B] = 1$ which implies that $K(\mathrm{GL}_2(\mathbb{R})) \subset \mathrm{SL}_2(\mathbb{R})$. It remains to show that certain commutators of elements of $\mathrm{SL}_2(\mathbb{R})$ generate $\mathrm{SL}_2(\mathbb{R})$.

For any $x \in \mathbb{R}$ one has

$$\left[\begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix}, \begin{pmatrix} 1 & x/3 \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \left[\begin{pmatrix} 1 & 0 \\ -x/3 & 1 \end{pmatrix}, \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}.$$

Now we prove that matrices of these two types generate $\mathrm{SL}_2(\mathbb{R})$. First,

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and for any $x \neq 0$,

$$\begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1/x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x - x^2 & 1 \end{pmatrix}.$$

Now, let $ad - bc = 1$. If $a \neq 0$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c/a & 1 \end{pmatrix} \begin{pmatrix} 1 & ab \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix},$$

which is a product of commutators. Otherwise, $b \neq 0$ and

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -d/b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/b & 0 \\ 0 & b \end{pmatrix}.$$

□

Exercise 9.2. *Let G be a group and $H < G$. Prove that if $K(G) \subset H$ then $H \triangleleft G$.*

Exercise 9.3. *Prove that* $K(S_4) = A_4$.

Hint. A_4 consists of eight 3-cycles (for example, (3124)) and four products of two disjoint transpositions (for example, (2143)). Show that each permutation of the former type is a commutator and each permutation of the latter type is the product of permutations of the former type.

Exercise 9.4. *Find the commutator subgroup of the group G from Exercise 9.1.*

Definition. Let G be a group. The set $Z(G) = \{a \in G \mid ab = ba \text{ for any } b \in G\}$ is called the **center** of G.

Theorem 9.4. *The center of a group is a normal subgroup.*

Proof. The fact that $Z(G)$ is a subgroup is easily verified. For $a \in Z(G), b \in G$, one has $bab^{-1} = abb^{-1} = a \in Z(G)$, which implies its normality. $\square$

Examples. 1. G is commutative iff $Z(G) = \{G\}$

2. $Z(S_3) = \{(123)\}$

3. $Z(D_4) = \{e, q\}$

Problem 9.5. *Prove that $Z(\mathrm{GL}_2(\mathbb{R})) = \{aE_n \mid a \in \mathbb{R}, a \neq 0\}$.*

Solution. The equalities

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

imply that $a = d$ and $c = 0$ if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(\mathrm{GL}_2(\mathbb{R})).$$

Similarly one gets $b = 0$. Thus $Z(\mathrm{GL}_2(\mathbb{R})) \subset \{aE_2 \mid a \in \mathbb{R}, a \neq 0\}$. The inverse inclusion is obvious. $\square$

10 Homomorphisms

Definition. Let G, H be groups. A map $\varphi\colon G \to H$ is called a **homomorphism** if

$$\varphi(xy) = \varphi(x)\varphi(y) \text{ for any } x, y \in G.$$

A homomorphism from G to G is called an **endomorphism** of G. The set of all homomorphisms from G to H is denoted by $\mathrm{Hom}(G, H)$ and the set of all endomorphisms of G is denoted by $\mathrm{End}(G)$.

Lemma 10.1. *If $\varphi \in \mathrm{Hom}(G, H)$ then $\varphi(e_G) = e_H$ and $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in G$.*

Proof. Note that $e_G e_G = e_G$. Therefore, $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$ whence $e_H = \varphi(e_G)\varphi(e_G)^{-1} = \varphi(e_G)\varphi(e_G)\varphi(e_G)^{-1} = \varphi(e_G)$.

Now let $x \in G$. Then $e_H = \varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$ and $e_H = \varphi(e_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x)$ which gives $\varphi(x)^{-1} = \varphi(x^{-1})$. □

Examples.

1. Let G, H be groups. The map from G to H, $g \mapsto e$, is a **trivial** homomorphism.
2. Let $G = \mathbb{R}, H = \mathbb{R}^*$. The exponent $\exp\colon \mathbb{R} \to \mathbb{R}^*, \exp(x) = e^x$, is a homomorphism since $e^{x+y} = e^x \cdot e^y$ for all $x, y \in \mathbb{R}$.
3. Let $G = \mathbb{C}, H = \mathbb{R}$. The module $|\ \ |\colon \mathbb{C}^* \to \mathbb{R}^*$ is a homomorphism, since $|xy| = |x||y|$ for all $x, y \in \mathbb{C}$.
4. Let $G = S_n, H = \{\pm 1\}$. The sign $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ is a homomorphism by the statement that relates the parities of two permutations and the parity of their product.
5. Let $k = \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/m\mathbb{Z}$ and $G = H = k$ and $a \in k$. The map $\varphi\colon k \to k$, $\varphi(x) = ax$ is a homomorphism.
6. Let $k = \mathbb{R}, \mathbb{Q}, \mathbb{C}$ and $G = \mathrm{GL}_n(k)$, $H = k^*$. The determinant $\det\colon \mathrm{GL}_n(k) \mapsto k^*$ is a homomorphism since $\det(AB) = \det A \cdot \det B$ for all $A, B \in \mathrm{GL}_n(k)$.
7. Let G be an arbitrary finite group of order n, $H = S_n$. The map $\Phi\colon G \to S_n$, $\Phi(g) = \sigma_g$ for $\sigma_g(h) = gh, h \in G$, is a homomorphism since $\Phi(gg')(h) = \sigma_{gg'}(h) = (gg')h$ and $(\Phi(g) \circ \Phi(g'))(h) = \Phi(g)(\Phi(g')(h)) = \sigma_g(\sigma_{g'}(h)) = g(g'h)$ for any $h \in G$.

Proposition 10.2. *Let G_1, G_2, G_3 be groups and $\varphi \in \mathrm{Hom}(G_1, G_2), \psi \in \mathrm{Hom}(G_2, G_3)$. Then $\psi \circ \varphi \in \mathrm{Hom}(G_1, G_3)$.*

Proof. If $\tau = \psi \circ \varphi$ then $\tau(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = \tau(x)\tau(y)$. □

Definition. Let $\varphi \in \mathrm{Hom}(G, H)$. The **kernel** of φ is

$$\mathrm{Ker}(\varphi) = \{x \in G \mid \varphi(x) = e_H\}.$$

The **image** of φ is

$$\mathrm{Im}(\varphi) = \{y \in H \mid y = \varphi(x) \text{ for some } x \in G\}.$$

Proposition 10.3. *If $\varphi \in \mathrm{Hom}(G, H)$ then $\mathrm{Im}(\varphi) < H$, $\mathrm{Ker}(\varphi) \lhd G$.*

Proof. Let $h, h' \in \mathrm{Im}(\varphi)$. Then there exist $g, g' \in G$ such that $\varphi(g) = h, \varphi(g') = h'$. Then $\varphi(gg') = \varphi(g)\varphi(g') = hh'$, whence $hh' \in \mathrm{Im}(\varphi)$. Further, $\varphi(e_G) = e_H$ and $\varphi(g^{-1}) = \varphi(g)^{-1} = h^{-1}$, whence $e_H \in \mathrm{Im}(\varphi)$ and $h^{-1} \in \mathrm{Im}(\varphi)$ whenever $h \in \mathrm{Im}(\varphi)$.

Now let $g, g' \in \mathrm{Ker}(\varphi)$. Then $\varphi(g) = \varphi(g') = e_H$. Now $\varphi(gg') = \varphi(g)\varphi(g') = e_H e_H = e_H$, so $gg' \in \mathrm{Ker}(\varphi)$. Also $\varphi(e_G) = e_H$ and $\varphi(g^{-1}) = \varphi(g)^{-1} = e_H^{-1} = e_H$, whence $e_G \in \mathrm{Ker}(\varphi)$ and $g^{-1} \in \mathrm{Ker}(\varphi)$ for any $g \in \mathrm{Ker}(\varphi)$.

Finally, if $g \in \mathrm{Ker}(\varphi), x \in G$, then $\varphi(xgx^{-1}) = \varphi(x)\varphi(g)\varphi(x^{-1}) = \varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \phi(e_G) = e_H$, whence $xgx^{-1} \in \mathrm{Ker}(\varphi)$. It shows that $\mathrm{Ker}(\varphi)$ is a normal subgroup of G. □

Lemma 10.4. *Let $\varphi \in \mathrm{Hom}(G, H)$. Then φ is injective if and if and only if $\mathrm{Ker}(\varphi) = \{e_G\}$.*

Proof. If φ is injective and $\varphi(g) = e_H$ then $g = e_G$ since $\varphi(e_G) = e_H$.

Conversely, if $\mathrm{Ker}(\varphi) = \{e_G\}$ and $g, g' \in G$ are such that $\varphi(g) = \varphi(g')$, then $\varphi(g^{-1}g') = \varphi(g^{-1})\varphi(g') = \varphi(g)^{-1}\varphi(g') = e_H$, so $g^{-1}g' \in \mathrm{Ker}(\varphi) = \{e_G\}$ and $g = g'$. □

Exercise 10.1. *Prove that $\varphi\colon \mathbb{R}^* \to \mathbb{R}^*, \varphi(x) = x^2$ is a homomorphism. Find its image and kernel.*

Exercise 10.2. *Let $\varphi \in \mathrm{Hom}(G, G')$.*

i) *Prove that $\varphi^{-1}(H') \lhd G$ if $H' \lhd G'$*

ii) *Prove that $\varphi(H) \lhd \mathrm{Im}(\varphi)$ if $H \lhd G$*

Proposition 10.5. *Let G, H be groups and $X \subset G$ be a generating set of G. If $\varphi, \psi \in \mathrm{Hom}(G, H)$ and $\varphi(x) = \psi(x)$ for any $x \in X$ then $\phi = \psi$.*

Proof. By Proposition 5.6, any $g \in G$ can be expressed as $g = y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}, y_i \in X, \varepsilon_i = \pm 1$. Then

$$\varphi(g) = \varphi(y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}) = \varphi(y_1)^{\varepsilon_1} \cdots \varphi(y_n)^{\varepsilon_n} = \psi(y_1)^{\varepsilon_1} \cdots \psi(y_n)^{\varepsilon_n} = \psi(y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}) = \psi(g).$$

□

Problem 10.6. *Prove that if $\varphi \in \mathrm{End}(\mathbb{Z})$ then there is $a \in \mathbb{Z}$ such that $\varphi(x) = ax, x \in \mathbb{Z}$.*

Solution. Put $a = \varphi(1)$ and $\psi_a \in \mathrm{End}(\mathbb{Z}), \psi_a(x) = ax$. Since 1 generates $\mathbb{Z}$ and $\varphi(1) = a = \psi_a(1)$, Proposition 10.5 completes the proof. □

Problem 10.7. *Prove that there is only the trivial homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}$.*

Solution. If $\varphi \in \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$ then

$$0 = \varphi(\bar{0}) = \varphi(\underbrace{\bar{1} + \cdots + \bar{1}}_{m \text{ times}}) = \underbrace{\varphi(\bar{1}) + \cdots + \varphi(\bar{1})}_{m \text{ times}} = m\varphi(\bar{1})$$

whence $\varphi(\bar{1}) = 0$. Since $\bar{1}$ generates $\mathbb{Z}/m\mathbb{Z}$, Proposition 10.5 completes the proof. □

Problem 10.8. *Prove that there is only one non-trivial homomorphisms from D_3 to $\mathbb{Z}/6\mathbb{Z}$.*

Solution. Let $\varphi \in \mathrm{Hom}(D_3, \mathbb{Z}/6\mathbb{Z})$. Since $r^2 s_1 = s_2 = s_1 r$, one has $2\varphi(r) + \varphi(s_1) = \varphi(r^2 s_1) = \varphi(s_1 r) = \varphi(s_1) + \varphi(r)$. It gives $\varphi(r) = \bar{0}$ and hence $\varphi(l) = \bar{0}$ and $\varphi(s_1) = \varphi(s_2) = \varphi(s_3)$. Further, $s_1^2 = e$ implies $2\varphi(s_1) = \bar{0}$ whence $\varphi(s_1) = \bar{0}$ or $\bar{3}$. Overall, we get only one non-trivial homomorphism $\varphi(s_1) = \varphi(s_2) = \varphi(s_3) = \bar{3}, \varphi(r) = \varphi(l) = 0$. □

Exercise 10.3. *Find all the endomorphisms of $\mathbb{Z}/6\mathbb{Z}$.*

Exercise 10.4. *Find all the homomorphisms from D_4 to $\mathbb{Z}/6\mathbb{Z}$.*

11 Isomorphisms

Definition. Let G, H be groups. A map $\varphi\colon G \to H$ is called an **isomorphism** if φ is a bijective homomorphism. Groups G, H are called **isomorphic** (notation: $G \cong H$) if there exists an isomorphism between them.

Remark. If the groups are finite, they are isomorphic if one can rearrange the elements of one of them so that their Cayley tables become identical.

Examples.

1. The identity map $\mathrm{id}_G\colon G \to G$ is an isomorphism.
2. Let $G = \{\pm 1\}$ be a group under multiplication, $H = \mathbb{Z}/2\mathbb{Z}$. The map $1 \mapsto \overline{0}, -1 \mapsto \overline{1}$ is an isomorphism.
3. Let $G = \mathbb{R}_{>0}$ be the group of positive real numbers under multiplication, $H = \mathbb{R}$. The logarithm $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ is an isomorphism.
4. $\mathbb{Z}/n\mathbb{Z} \cong T_n$. The map $\overline{\ell} \mapsto \cos(\ell/2\pi n) + i\sin(\ell/2\pi n)$ is an isomorphism.
5. Let $G = D_3, H = S_3$. Any isometry of a regular triangle generates a permutation of its three vertices. The corresponding map from G to H is an isomorphism.

Lemma 11.1. *Isomorphism is an equivalence relation on the set of all groups.*

Proof. Since the identity map is an isomorphism, it is obvious that any group is isomorphic to itself. Further, the inverse of an isomorphism is also an isomorphism. Indeed, let $\varphi\colon G \to H$ be an isomorphism. Then $\varphi(\varphi^{-1}(a)\varphi^{-1}(b)) = \varphi(\varphi^{-1}(a))\varphi(\varphi^{-1}(b)) = ab = \varphi(\varphi^{-1}(ab))$ for any $a, b \in H$. Since φ is injective, it gives $\varphi^{-1}(a)\varphi^{-1}(b) = \varphi^{-1}(ab)$ as required. Thus $G \cong H$ implies $H \cong G$.

Finally, suppose that $G_1 \cong G_2, G_2 \cong G_3$ and $\varphi\colon G_1 \to G_2$ and $\psi\colon G_2 \to G_3$ are isomorphisms. Then $\psi \circ \varphi\colon G_1 \to G_3$ is a homomorphism by Proposition 10.2 and a bijection as the composition of bijections, i.e., G_1 and G_3 are isomorphic. $\square$

Proposition 11.2. *A group isomorphic to a commutative group is commutative.*

Proof. Let $\varphi\colon G \to H$ be an isomorphism and G be commutative. Then $xy = \varphi(\varphi^{-1}(x)\varphi^{-1}(y)) = \varphi(\varphi^{-1}(y)\varphi^{-1}(x)) = yx$ for any $x, y \in H$. $\square$

Proposition 11.3. *If $\varphi\colon G \to H$ is an isomorphism, then $\mathrm{ord}_G\, g = \mathrm{ord}_H\, \varphi(g)$ for any $g \in G$.*

Proof. If $\mathrm{ord}_G\, g = n$, then $\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_H$, whence $\mathrm{ord}_H\, \varphi(g) = m$ and $n \geq m$. On the other hand, $\varphi(g^m) = \varphi(g)^m = e_H = \varphi(e_G)$, whence $g^m = e_G$, and so $m \geq n$.

If g is of infinite order then $g^k \neq g^\ell$ for $n \neq \ell$. Therefore $\varphi(g)^k \neq \varphi(g)^\ell$ for $n \neq \ell$ and $\varphi(g)$ is of infinite order. $\square$

Generally, isomorphic groups have identical group properties. Thus, in order to show that two groups are non-isomorphic it is enough to find a property that holds in one group and does not hold in another.

Exercise 11.1. *Let G, H be isomorphic groups and G can be generated by two elements. Show that H satisfies the same property.*

Examples. 1. $\mathbb{Z}/6\mathbb{Z} \ncong S_3$, since $\mathbb{Z}/6\mathbb{Z}$ is commutative and S_3 not.

2. $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, since $\mathbb{Z}/4\mathbb{Z}$ has an element of order 4 and $\mathbb{Z}/4\mathbb{Z}$ has not.

3. $\mathbb{R}^* \ncong \mathbb{C}^*$, since $\mathbb{C}^*$ has elements of order 3 and $\mathbb{R}^*$ has not.

Problem 11.4. *Prove that $\mathbb{Q} \ncong \mathbb{Q}_{>0}$ where $\mathbb{Q}_{>0}$ is the group of positive rational numbers under multiplication.*

Solution. Let φ be an isomorphism from $\mathbb{Q}$ to $\mathbb{Q}_{>0}$ and $\varphi(1) = q \in \mathbb{Q}, q \neq 1$. Then for any $n \in \mathbb{N}$ one has $q = \varphi(n \cdot 1/n) = \varphi(1/n)^n$. Thus for any $n \in \mathbb{N}$ the equation $x^n = q$ has a solution in $\mathbb{Q}$, which is false. $\square$

Exercise 11.2. *Prove that $D_3 \times \mathbb{Z}/5\mathbb{Z} \ncong D_5 \times \mathbb{Z}/3\mathbb{Z}$*

Hint. Compare the number of elements of a given order in both groups.

Exercise 11.3. *Prove that $\mathbb{Q} \ncong \mathbb{Q} \times \mathbb{Q}$*

Hint. For any $p, q \in \mathbb{Q}$, there is $r \in \mathbb{Q}$ such that both p and q are multiples of r.

Theorem 11.5 (Fundamental theorem on homomorphisms)**.** *Let G, H be groups, $\varphi \in \mathrm{Hom}(G, H)$. Then $G/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$.*

Proof. Denote $J = \operatorname{Ker}(\varphi)$ which is a normal subgroup of G by Proposition 10.3 and define the map $\Phi\colon G/J \to \operatorname{Im}(\varphi), \Phi(gJ) = \varphi(g)$. The map is well-defined: if $gJ = g'J$, then $g = g'x$ for some $x \in J$ and $\varphi(g) = \varphi(g'x) = \varphi(g')\varphi(x) = \varphi(g')$.

Check that Φ is a homomorphism:

$$\Phi(gJ)\Phi(g'J) = \varphi(g')\varphi(g') = \varphi(gg') = \Phi((gg')J) = \Phi(gJ \cdot g'J), \quad g, g' \in G.$$

If $gJ \in \operatorname{Ker}\Phi$ then $e_H = \Phi(gJ) = \varphi(g)$ so $g \in J$ and $gJ = J$. Thus $\operatorname{Ker}\Phi$ is trivial and Φ is injective by Lemma 10.4. If $h \in \operatorname{Im}(\varphi)$ then $\varphi(g) = h$ for some $g \in G$ and $\Phi(gJ) = \varphi(g) = h$ which shows that Φ is surjective. $\square$

Examples. 1. If $\det\colon \mathrm{GL}_n(\mathbb{R}) \mapsto \mathbb{R}^*$ then $\operatorname{Ker}(\det) = \mathrm{SL}_n(\mathbb{R}), \operatorname{Im}(\det) = \mathbb{R}^*$, which gives $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$.

2. Let G, H be arbitrary groups, consider the projection $\mathrm{pr}_G\colon G \times H \to G$, $\mathrm{pr}_G((g, h)) = g$. Clearly it is a homomorphism and $\operatorname{Ker}(\mathrm{pr}_G) = \{e_G\} \times H, \operatorname{Im}(\mathrm{pr}_G) = G$, whence $G \times H/\{e_G\} \times H \cong G$. Note that $\{e_G\} \times H \cong H$.

Problem 11.6. *For $G = \mathrm{GL}_n(\mathbb{C}), H = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid \det A \in \mathbb{R}, \det A > 0\}$, show that $G/H \cong T$*

Solution. We will use the fundamental theorem on homomorphisms. To that end, one needs to find a surjective $\varphi \in \mathrm{Hom}(G, T)$ such that $\mathrm{Ker}\,\varphi = H$. Put $\varphi(A) = \det A/|\det A|$. Then $\varphi(AB) = \det AB/|\det AB| = \det A/|\det A| \cdot \det B/|\det B| = \varphi(A)\varphi(B)$ and $\varphi(A) = 1$ iff $\det A = |\det A|$, that is $\det A \in \mathbb{R}$ and $\det A > 0$. Finally if $a \in \mathbb{C}, |a| = 1$ then $\varphi(A) = a$ for

$$A = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

□

Exercise 11.4. *For $G = \mathrm{GL}_n(\mathbb{C}), H = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid \det A = \pm 1, \pm i\}$, show that $G/H \cong \mathbb{C}^*$*

12 Classifications of groups

Definition. A group G is **cyclic** if it is generated by one element, i.e., there exists $g \in G$ such that $G = \langle g \rangle$.

Examples. 1. $\mathbb{Z}$ is cyclic

2. $\mathbb{Z}/m\mathbb{Z}$ is cyclic

3. $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. If (a, b) generates $\mathbb{Z} \times \mathbb{Z}$ then $(a + 1, b)$ can not be generated.

Theorem 12.1. *A finite cyclic group of order m is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. An infinite cyclic group is isomorphic to $\mathbb{Z}$.*

Proof. Let G be a cyclic group generated by $g \in G$. Consider the homomorphism $\psi_g \colon \mathbb{Z} \to G, \psi_g(n) = g^n$. Its image equals $\langle g \rangle = G$. Theorem 11.5 implies $\mathbb{Z}/\mathrm{Ker}(\psi_g) \cong G$. By Theorem 5.2 the subgroup $\mathrm{Ker}(\psi_g)$ is either zero or has the form $m\mathbb{Z}$ for some $m \in \mathbb{N}$, which gives the required statement. □

Proposition 12.2. *If G is a finite group of prime order p, then $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. By Corollary 8.4, the order of any element of G must be a divisor of p, and thus is equal to 1 or p. The only element of order 1 is e, therefore, there is $g \in G$ of order p. But $|\langle g \rangle| = \mathrm{ord}_G\, g = p$ by Proposition 6.4 and thus $\langle g \rangle = G$. Therefore G is a cyclic group generated by g and is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by Theorem 12.1. □

Proposition 12.3. $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ *if and only if* $(m, n) = 1$.

Proof. Suppose $\gcd(m,n)=1$. It suffices to show that $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ is cyclic. We check that $(\overline{1},\overline{1})$ is its generator. For any $a,b\in\mathbb{Z}$, it suffices to check that the system

$$\begin{cases} x\equiv a \pmod m \\ x\equiv b \pmod n \end{cases}$$

is solvable which follows from the Chinese remainder theorem.

Now let $\gcd(m,n)=d>1$. Then $\operatorname{lcm}(m,n)=N=mn/d<mn$, so $N(\overline{a},\overline{b})=(N\overline{a},N\overline{b})=(\overline{0},\overline{0})$ for any $(\overline{a},\overline{b})\in\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$. On the other hand, $N\overline{1}\neq\overline{0}$ in $\mathbb{Z}/mn\mathbb{Z}$, therefore $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/mn\mathbb{Z}$ are not isomorphic. □

Proposition 12.4. *1. A group of order 4 is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.*

2. A group of order 6 is isomorphic to either $\mathbb{Z}/6\mathbb{Z}$ or S_3.

Proof. 1. Let $|G|=4$. The order of any non-identity elements of G can be either 2 or 4 by Corollary 8.4. If there is an element of G of order 4, then G is a cyclic group and thus is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. If the orders of all non-identity elements of G are 2, then for any non-identity distinct $a,b\in G$ one has $G=\{e,a,b,ab\}$, whence $ba=ab$. Indeed, $ba\neq a$ since $b\neq e$, $ba\neq b$ since $a\neq e$ and $ba\neq e$ since $a\neq b$. Now the bijection from G to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ given by $e\mapsto(\overline{0},\overline{0}), a\mapsto(\overline{1},\overline{0}), b\mapsto(\overline{0},\overline{1}), ab\mapsto(\overline{1},\overline{1})$ is a homomorphism since the correspondent Cayley tables are identical.

2. Let $|G|=6$. If G contains an element of order 6, then G is a cyclic group and thus is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. Otherwise, the orders of the non-identity elements of G may be 2 or 3. All non-identity elements cannot be of order 2, because if $\operatorname{ord}_G a=\operatorname{ord}_G b=\operatorname{ord}_G ab=2$, then $\langle a,b\rangle=\{e,a,b,ab\}<G$, which contradicts Lagrange's theorem. Also, all non-identity elements cannot be of order 3, since the inverse of an element of order 3 is a distinct element of order 3, so their number is even. Therefore there are $a,b\in G$ such that $\operatorname{ord}_G a=2,\operatorname{ord}_G b=3$.

Now we claim that $G=\{e,b,b^2,a,ab,ab^2\}$, since these elements are all distinct. For example, if $b=ab^2$, then $ab=e$, whence $b=a$, a contradiction. If $b^2=a$ then $b=b^4=a^2=e$, a contradiction. The remaining cases are treated similarly. We now want to find ba in this list. It is clear that $ba\neq e,a,b,b^2$. If $ba=ab$, then $(ab)^2=b^2,(ab)^3=a,(ab)^4=b,(ab)^5=ab^2$, whence $\operatorname{ord}_G ab=6$, a contradiction. Thus the only remaining possibility is $ba=ab^2$ and in this case $G\cong S_3$. Indeed, one can match a to an arbitrary transposition, b to one of two 3-cycles and the remaining elements to the correspondent products of these transposition and cycle. Then the correspondent Cayley tables of G and S_3 are identical. □

Exercise 12.1. *Prove that any abelian group of order 8 is isomorphic to one of the following groups: $\mathbb{Z}/8\mathbb{Z},\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.*

Hint. Show that $G=\{0,a,b,c,a+b,a+c,b+c,a+b+c\}$ if there are distinct $a,b,c\in G$ of order 2 with $c\neq a+b$. Show that $G=\{0,a,2a,3a,b,a+b,2a+b,3a+b\}$ if $\operatorname{ord} a=4$ and $b\neq 0,a,2a,3a$.

Exercise 12.2. *Let p be a prime, G be a finite abelian group and $\operatorname{ord} g=p$ for any non-zero $g\in G$. Prove that G is isomorphic to $\mathbb{Z}/p\mathbb{Z}\times\cdots\times\mathbb{Z}/p\mathbb{Z}$.*

Hint. G can be considered as a vector space over $\mathbb{Z}/p\mathbb{Z}$.

13 Group action

Definition. An **action** of a group G on a set M is given by a mapping $G \times M \to M, (g, m) \mapsto gm$, that satisfies the following properties:

I. $g_2(g_1 m) = (g_2 g_1)m$ for any $g_1, g_2 \in G, m \in M$

II. $em = m$ for any $m \in M$

Examples. 1. The **trivial** action of an arbitrary group G on a set M given by $gm = m$ for all $g \in G, m \in M$

2. Let $M = \mathrm{M}_{n,1}(\mathbb{R}), G = \mathrm{GL}_n(\mathbb{R})$. The multiplication $(A, v) \mapsto Av$, where $A \in \mathrm{GL}_n(\mathbb{R}), v \in \mathrm{M}_{n,1}(\mathbb{R})$, gives an action of G on M, since $B(Av) = (BA)v$ and $E_n v = v$.

3. Let M be the set of colorings of the vertices of a regular n-gon in s colors and $G = D_n$. Each symmetry permutes the vertices, mapping one coloring to another, which defines an action of G on M.

4. The group S_n acts on $\mathbb{R}[x_1, \ldots, x_n]$ by $(\sigma \cdot f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

5. Let G be a group, $M = G$. Multiplication $((g, m) \mapsto gm)$ gives an action of G on itself.

6. Let G be a group, $M = G$. Conjugation $((g, m) \mapsto gmg^{-1})$ defines an action of G on itself.

Definition. Let a group G act on M and $m \in M$. The **stabilizer subgroup** of m is defined as $G_m = \{g \in G : gm = m\}$ and the **orbit** of m is defined as $\operatorname{Orb} m = \{gm, g \in G\} \subset M$.

An action of G on M is **transitive**, if there is only one orbit, i.e., for any two elements $m_1, m_2 \in M$, there exists $g \in G$ such that $gm_1 = m_2$. An element $m \in M$ is a **fixed point** of $g \in G$ if $gm = m$.

Proposition 13.1. $G_m < G$

Proof. If $g_1, g_2 \in G_m$, then $(g_2 g_1)m = g_2(g_1 m) = g_2 m = m$, i.e. $g_2 g_1 \in G_m$. Moreover, $e \in G_m$ since $em = m$. If $gm = m$, then $g^{-1}m = g^{-1}(gm) = (g^{-1}g)m = em = m$, thus $g \in G_m$ implies $g^{-1} \in G_m$. $\square$

Proposition 13.2. *Let G act on M. The relation $\sim$ on M, defined by $m_1 \sim m_2$ if $gm_1 = m_2$ for some $g \in G$, is an equivalence relation.*

Proof. If $gm_1 = m_2$ then $g^{-1}m_2 = m_1$ and $m_1 \sim m_2$ implies $m_2 \sim m_1$. If $gm_1 = m_2$ and $g'm_2 = m_3$, then $(g'g)m_1 = g'(gm_1) = g'm_2 = m_3$ and $m_1 \sim m_2, m_2 \sim m_3$ imply $m_2 \sim m_1$. Finally, $em = m$ and $m \sim m$ which completes the proof. $\square$

Remark. Clearly, the equivalence class of $m \in M$ with respect to $\sim$ is $\operatorname{Orb} m$. Thus any group action on M partitions it into the disjoint union of orbits.

Theorem 13.3 (Orbit-Stabilizer Theorem). *For a finite group G acting on a set M*

$$|\operatorname{Orb} m| \cdot |G_m| = |G|$$

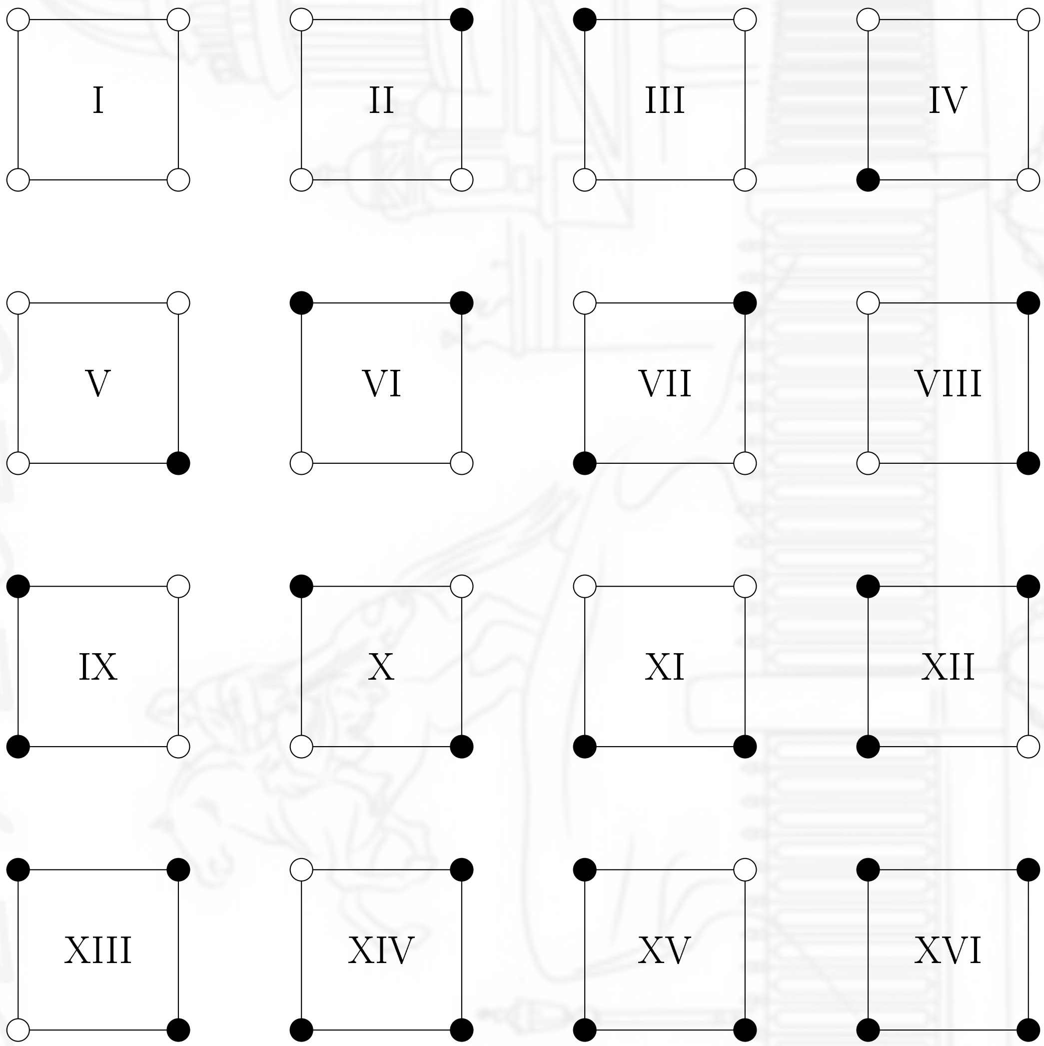
for any $m \in M$.

Proof. Denote $H = G_m$ and define the map $\Gamma\colon G/H \to \operatorname{Orb} m$ by $\Gamma(gH) = gm$. If $gH = g'H$, then $g' = ga$ for some $a \in H$, whence $g'm = (ga)m = g(am) = gm$, i.e. Γ is well-defined.

We will show that Γ is bijective. The surjectivity is obvious and if $\Gamma(gH) = \Gamma(g'H)$, then $m = (g^{-1}g')m$, whence $g^{-1}g' \in H$, thus $gH = g'H$.

By Lagrange's theorem, the index of H in G equals $|G|/|H|$, which yields the required identity. $\square$

Example. Consider the action of D_4 on the colorings of the vertices of a square in 2 colors. It has the following orbits: {I}, {II,III,IV,V}, {VI,VIII,IX,XI}, {VII,X}, {XII,XIII,XIV,XV}, {XVI}. The stabilizer of II is $\{e, s_2\}$, the stabilizer of VI is $\{e, t_1\}$, the stabilizer of VII is $\{e, s_1, s_2, q\}$.



Exercise 13.1. *Let a group G act on a set M. Prove that $G_m \cong G_{m'}$ if m, m' belong to the same orbit.*

Hint. G_m and $G_{m'}$ are conjugates, that is $G_{m'} = gG_mg^{-1}$ for some $g \in G$.

Exercise 13.2. *Let $G = \{A \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \mid AA^T = E_2\}$. Find the orbits and the stabilizers for its action on $\mathrm{M}_{2,1}(\mathbb{Z}/3\mathbb{Z})$ by multiplication.*

Hint.

$$G = \left\{ \begin{pmatrix} \overline{1}, \overline{0} \\ \overline{0}, \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1}, \overline{0} \\ \overline{0}, \overline{2} \end{pmatrix}, \begin{pmatrix} \overline{0}, \overline{1} \\ \overline{1}, \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0}, \overline{1} \\ \overline{2}, \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0}, \overline{2} \\ \overline{1}, \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0}, \overline{2} \\ \overline{2}, \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{2}, \overline{0} \\ \overline{0}, \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{2}, \overline{0} \\ \overline{0}, \overline{2} \end{pmatrix} \right\}$$

Lemma 13.4 (Burnside)**.** *Let a group G act on a set M. The number of orbits equals*

$$N = \frac{1}{|G|} \sum_{g \in G} |M^g|,$$

where $M^g = \{m \in M : gm = m\}$.

Proof. We count the number of elements of the set $W = \{(g, m) \in G \times M : gm = m\}$ in two different ways. On one hand, $|W| = \sum_{g \in G} |\{m \in M : gm = m\}| = \sum_{g \in G} |M^g|$. On the other hand, if $\Omega_1, \dots, \Omega_N$ are the orbits then

$$\begin{aligned} |W| = \sum_{m \in M} |\{g \in G : gm = m\}| = \sum_{m \in M} |G_m| = \sum_{m \in M} \frac{|G|}{|\operatorname{Orb} m|} = |G| \sum_{i=1}^{N} \sum_{m \in \Omega_i} \frac{1}{|\operatorname{Orb} m|} \\ = |G| \sum_{i=1}^{N} \sum_{m \in \Omega_i} \frac{1}{|\Omega_i|} = |G| \sum_{i=1}^{N} 1 = |G| \cdot N. \end{aligned}$$

□

Problem 13.5. *How many different necklaces can be formed with 6 black and white beads?*

Solution. Consider the set M of all possible colorings of the vertices of a regular hexagon in two colors and the action of D_6 on it. Clearly, $|M| = 2^6 = 64$. It is easy to see that the number of different necklaces is equal to the number of orbits under this action which can be calculated using Burnside's lemma.

The group D_6 consists of 12 symmetries:

- the identity transformation
- two rotations by $\pi/3$
- two rotations by $2\pi/3$
- the central symmetry
- three reflections across the diagonals
- three reflections across the lines connecting the midpoints of the opposite edges.

For each symmetry g we count M^g, the number of colorings of the hexagon in two colors that remain unchanged under g. For example, if g is the rotation by $2\pi/3$, there are 4 such colorings: two monochromatic colorings and two colorings with alternating colors. As a result, one has

$$N = \frac{1}{12}(64 + 2 \cdot 2 + 2 \cdot 4 + 8 + 3 \cdot 16 + 3 \cdot 8) = 13.$$

$\square$

Remark. Let D_n act on the set M of the colorings of the vertices of a regular n-gon in k colors. The size of M^g can be calculated as follows. A symmetry g defines a permutation $\sigma \in S_n$ of the vertices which can be expressed as the product of q disjoint cycles. Clearly, a coloring belongs to M^g iff all the vertices belonging to the same cycle are of the same color. It gives $|M^g| = k^q$.

Exercise 13.3. *Find the number of rotationally distinct colorings of the faces of a cube using three colors.*

Hint. The group of the rotational symmetries of a cube consists of the following 24 elements: the identity, the rotations through 120° and 240° about 4 axes connecting the opposite vertices of the cube, the rotations through 180° about 6 axes connecting the midpoints of the opposite edges, and the rotations through 90°, 180° and 270° about 3 axes connecting the centers of the opposite faces.

14 Application of group action

Theorem 14.1 (Cauchy)**.** *Let p be a prime. If $p||G|$, then G contains an element of order p.*

Proof. Put $M = \{(x_1, x_2, \ldots, x_p) \in G^p \,|\, x_1 x_2 \cdots x_p = e\}$. Every p-tuple from M is uniquely defined by its first $p-1$ entries, thus M consists of $|G|^{p-1}$ elements.

Note that if $x_1 x_2 \cdots x_p = e$, then $x_2 \cdots x_p x_1 = e$, which allows one to define an action of the cyclic group $\mathbb{Z}/p\mathbb{Z}$ on M:

$$\overline{n} \cdot (x_1, x_2, \ldots, x_p) = (x_{n+1}, \ldots, x_p, x_1, \ldots, x_n), \quad 0 \leq n \leq p-1.$$

By the Orbit-Stabilizer Theorem, the orbits in M contain 1 or p elements. An orbit consists of one element if and only if its only element is of the form $(x, x, \ldots, x)$ and $x^p = e$. Since $|M|$ is equal to the sum of the sizes of the orbits, the number of x such that $x^p = e$ is a multiple of p. The identity element is one of these elements, hence there are at least $p-1$ non-identity elements that are of order p, i.e. the set of such elements is nonempty. $\square$

Theorem 14.2. *If $|G| = p^n$, then $Z(G)$ is non-trivial.*

Proof. Consider the action of the group G on itself by conjugation. It defines a partition of G into the disjoint orbits whose size is equal to 1 or $p^k, k \in \mathbb{N}$, by the Orbit-Stabilizer Theorem. Therefore the number of one-element orbits is divisible by p. An element has one-element orbit under conjugation if and only if is in $Z(G)$, and hence $p||Z(G)|$. Since $e \in Z(G)$, its size cannot be less than p. $\square$

Corollary 14.3. *Any group of order p^2 is abelian.*

Proof. If $G \neq Z(G)$, pick up $g \notin Z(G)$. Let $H = \{h \in G \mid gh = hg\}$ which is a subgroup of G and $Z(G) \subset H, g \in H$. Further, $H \neq Z(G)$ since $g \notin Z(G), g \in H$ and $H \neq G$ since otherwise $g \in Z(G)$. By Lagrange's Theorem, $|Z(G)|, |H|$ divide $|G| = p^2$ while $1 < |Z(G)| < |H| < p^2$ which is not possible. $\square$

Proposition 14.4. *Let G be a finite group and p be the smallest prime divisor of $|G|$. Then any subgroup of H of index p is normal.*

Proof. Let $\Omega = G/H, |\Omega| = p$. Consider the action of H on Ω by left multiplication: $h \cdot gH = (hg)H,\ h \in H, g \in G$. It gives a partition of Ω into a disjoint union of orbits whose sizes by the Orbit-Stabilizer Theorem are divisors of $|H|$ and hence of $|G|$. Since p is the smallest prime divisor of $|G|$, the size of an orbit can be either 1 or p.

Obviously the orbit of $H \in \Omega$ consists of one element, hence the other orbits also consist of one element. Therefore $(hg)H = gH$ for all $h \in H, g \in G$, whence $hg = gh'$ for some $h' \in H$, which implies $H \triangleleft G$. $\square$

Chapter II: Rings and Fields

15 Definitions and examples

Definition. Let R be a set with two binary operations denoted by $+$ and $\cdot$ and call *addition* and *multiplication*, respectively. Assume the following properties are satisfied:

1. $a + (b + c) = (a + b) + c$ for any $a, b, c \in R$ (that is, $+$ is associative)
2. there exists $\mathbf{0} \in R$ such that $\mathbf{0} + a = a = a + \mathbf{0}$ for all $a \in R$ (that is, $\mathbf{0}$ is the identity element with respect to $+$; it is called **zero**);
3. for any $a \in R$, there exists $a' \in R$ such that $a + a' = \mathbf{0} = a' + a$ (that is, a has the inverse with respect to $+$; it is usually denoted by $-a$);
4. $a + b = b + a$ for any $a, b \in R$ (that is, $+$ is commutative);
5. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for any $a, b, c \in R$ (*distributivity*).
6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for any $a, b, c \in R$ (that is $\cdot$ is associative);
7. there exists an element $\mathbf{1} \in R$ such that $\mathbf{1} \cdot a = a = a \cdot \mathbf{1}$ for any $a \in R$ (that is, $\mathbf{1}$ is the identity element with respect to $\cdot$; it is called a **unity**);
8. $a \cdot b = b \cdot a$ for any $a, b \in R$ (that is, $\cdot$ is commutative);

Then R with the above two operations is called an **associative commutative ring with unity** or simply a **ring**.

Remark. Any ring is a commutative group with respect to addition

Examples.

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ with respect to standard addition and multiplication.
2. $\mathbb{Z}/m\mathbb{Z}$ with respect to addition and multiplication of residue classes.
3. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$
4. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$
5. If R is a ring, $R[t]$ is a ring
6. The set of all subsets of a given set X with respect to $A + B = A \triangle B$, $A \cdot B = A \cap B$
7. If R is a ring, $\mathrm{M}_n(R)$ is a non-commutative ring with unity
8. $2\mathbb{Z}$ is a commutative ring without unity

Lemma 15.1. *If R is a ring then*

1. $a \cdot \mathbf{0} = \mathbf{0} \cdot a = \mathbf{0}$ *for all* $a \in R$
2. $(-a)b = -(ab)$ *for any* $a, b \in R$

Proof. One has $a \cdot \mathbf{0} + a \cdot \mathbf{0} = a \cdot (\mathbf{0} + \mathbf{0}) = a \cdot \mathbf{0}$. Canceling out $a \cdot \mathbf{0}$ gives the first result.
The equality $(-a)b + ab = (-a + a)b = \mathbf{0} \cdot b = \mathbf{0}$ implies the second result. □

Exercise 15.1. *Let R be a ring. Prove that $a^2 + (-b^2) = (a + b)(a + (-b))$ for any $a, b \in R$. Refer to each axiom or property you use.*

Definition. A **field** k is a ring such that for any $a \in k, a \neq \mathbf{0}$, there exists $a' \in k$ such that $a \cdot a' = a' \cdot a = \mathbf{1}$ (that is, a has the inverse with respect to $\cdot$; it is usually denoted by a^{-1}).

The **characteristic** of a field is the order of $\mathbf{1}$ in its additive group, i.e., the smallest positive integer p such that $\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{p \text{ times}} = \mathbf{0}$. If the order is infinite then the characteristic is said to be 0. Notation: $\mathrm{char}(k) = p$.

Examples.

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are field of zero characteristic
2. $\mathbb{Z}/p\mathbb{Z}$ for a prime p is a field of characteristic p
3. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field of zero characteristic

Definition. An **integral domain** R is a ring such that $ab \neq \mathbf{0}$ for any $a, b \in R, a, b \neq \mathbf{0}$.

Examples.

1. Any field is an integral domain
2. $\mathbb{Z}$
3. $R[t]$ is an integral domain if R is an integral domain

4. $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain if m is a composite number

Proposition 15.2 (Cancellation is integral domains). *Let R be an integral domain and $a, b, c \in R$. If $a \neq \mathbf{0}$ and $ab = ac$ then $b = c$.*

Proof. One has $a(b - c) = \mathbf{0}$ whence $b - c = \mathbf{0}$. □

Exercise 15.2. *Prove that every finite integral domain is a field*

Hint. Show that if $x \neq \mathbf{0}$ then $x^n = \mathbf{1}$ for a certain $n \in \mathbb{N}$.

Exercise 15.3. *Let $F = \{(a, b) \mid a, b \in \mathbb{Z}/3\mathbb{Z}\}$. Define on F two operations:*

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Show that F with respect to the above operations is a field of characteristic 3 proving explicitly

- *Distributivity of multiplication over addition*
- *Existence of multiplicative inverses*
- char $F = 3$

Hint. Notice that $(\overline{0}, \overline{1})^2 = (-\overline{1}, \overline{0})$. One can associate (a, b) with $a + bi$ where $i^2 = -\overline{1}$.

Definition. Rings R_1, R_2 are **isomorphic** if there exists a bijection $\Phi\colon R_1 \to R_2$ such that $\Phi(a + b) = \Phi(a) + \Phi(b)$ and $\Phi(ab) = \Phi(a)\Phi(b)$ for all $a, b \in R_1$.

Example. Let V be an n-dimensional vector space over a field k. Then $\mathcal{L}(V)$ is isomorphic to $\mathrm{M}_n(k)$.

Exercise 15.4. *Let*

$$F = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

i) *Show that F is a ring with respect to matrix addition and multiplication.*
ii) *Show that F is isomorphic to $\mathbb{C}$ by considering $\Phi\colon F \to \mathbb{C}$,*

$$\Phi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a + bi.$$

Exercise 15.5. *Show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are not isomorphic.*

Hint. If an isomorphism exists, consider the image of $\sqrt{2}$ under it.

16 Ideals

Let R be an integral domain.

Definition. A non-empty subset $I \subset R$ is an **ideal** of R if:

I. $a + a' \in I$ for all $a, a' \in I$

II. $ra \in I$ for all $a \in I, r \in R$

Examples. 1. $\{\mathbf{0}\}, R$ are ideals of R

2. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$

3. $\{f \in R[x] \mid f(a) = 0\}$ is an ideal of $R[x]$, where $a \in R$ is fixed

Proposition 16.1. *Let I be an ideal of R. Then I is a subgroup of the additive group of R.*

Proof. If $a \in I$ then $\mathbf{0} = \mathbf{0} \cdot a \in I$ and $-a = (-1) \cdot a \in I$. □

Corollary 16.2. *Any ideal I of $\mathbb{Z}$ has the form $m\mathbb{Z}$ for some a non-negative $m \in \mathbb{Z}$.*

Proposition 16.3. *Let $a_1, \ldots, a_n \in R$. Then $I = \{r_1 a_1 + \cdots + r_n a_n \mid r_1, \ldots, r_n \in R\}$ is an ideal of R.*

Proof. If $a = r_1 a_1 + \cdots + r_n a_n, a' = r'_1 a_1 + \cdots + r'_n a_n$ for some $r_1, r'_1, \ldots, r_n, r'_n \in R$, then $a + b = (r_1 + r'_1) a_1 + \cdots + (r_n + r'_n) a_n \in I$. Similarly, if $a = r_1 a_1 + \cdots + r_n a_n$ for some $r_1, \ldots, r_n \in R$ and $r \in R$, then $ra = (rr_1) a_1 + \cdots + (rr_n) a_n \in I$. □

Definition. The ideal defined in Proposition 16.3 is called the ideal **generated** by $a_1, \ldots, a_n$ and is denoted by $(a_1, \ldots, a_n)$. An ideal **principal** if it is generated by a single element.

An element $a \in R$ is **divisible** by $b \in R, b \neq 0$ (or b **divides** a) (notation: $b \mid a$) if $a = bc$ for some $c \in R$. Elements $a, b \in R, a, b \neq \mathbf{0}$ are **associated** if a divides b and b divides a.

A **unit** is an element having a multiplicative inverse. The set of units of a ring R is denoted R^*.

Remark. R^* is a group under multiplication

Examples. 1. $k^* = k \setminus \{\mathbf{0}\}$ if k is a field

2. $\mathbb{Z}^* = \{\pm 1\}$

3. $R[t]^* = R^*$

4. $\mathbb{Z}[\sqrt{2}]^* = \{\pm(1 + \sqrt{2})^n, \pm(1 - \sqrt{2})^n \mid n \geq 0\}$

Exercise 16.1. *Let I, J be ideals of R. Define*

$$I + J = \{a + b \mid a \in I, b \in J\}, \quad IJ = \{a_1 b_1 + \cdots a_n b_n \mid a_1, \ldots, a_n \in I, b_1, \ldots, b_n \in J\}.$$

i) *Prove that $I + J, IJ$ are ideals of R*

ii) *Prove that $I(J + J') = IJ + IJ'$*

iii) *Find a generating set for IJ if $I = (a_1, \ldots, a_n), J = (b_1, \ldots, b_m)$*

Proposition 16.4. *1. $b \mid a$ if and only if $(a) \subset (b)$*

2. a, b are associated if and only if $(a) = (b)$

3. a, b are associated if and only if $a = bu$ for some $u \in R^*$

Proof. If $b \mid a$, then $a = bc$ for some $c \in R$. For any $x \in (a)$ one has $x = ay, y \in R$ and $x = b(cy) \in (b)$. Conversely, if $(a) \subset (b)$, then $a = a \cdot 1 \in (a) \subset (b)$, hence $a = bc, c \in R$. The second statement follows from the first one.

If a, b are associated then $a = bu, b = va$ for some $u, v \in R$. Then $a = uva$ and $uv = \mathbf{1}$ since $a \neq \mathbf{0}$ and R is an integral domain. It shows that $u \in R^*$. The inverse statement is trivial. □

Problem 16.5. *For $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$, find R^*.*

Solution. Define $N\colon R \to \mathbb{Z}, N(a + b\sqrt{-3}) = |a + b\sqrt{-3}|^2 = a^2 + 3b^2$. Then $N(z_1 z_2) = N(z_1)N(z_2)$ for any $z_1, z_2 \in R$. If $u = a + b\sqrt{-3} \in R^*$ then $uv = 1$ for some $v \in R$ whence $N(u)N(v) = N(1) = 1$. Then $a^2 + 3b^2 = N(u) = 1$ whence $a = \pm 1, b = 0$. Clearly $\pm 1 \in R^*$ and thus $R^* = \{\pm\}$. □

Exercise 16.2. *Let ξ be a complex cube root of 1. For $R = \mathbb{Z}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Z}\}$, find R^*.*

Hint. Define N similarly to Problem 16.5.

Proposition 16.6. *A ring k is a field iff $\{\mathbf{0}\}, k$ are its only ideals.*

Proof. Let I be an ideal of a field k and $a \in I, a \neq \mathbf{0}$. Then $b = (ba^{-1})a \in I$ for any $b \in k$ whence $I = k$.

If $a \in k, a \neq \mathbf{0}$, consider the ideal (a). If $\{\mathbf{0}\}, k$ are its only ideals of k then $(a) = k$. In particular $\mathbf{1} \in (a)$ whence a is invertible and k is a field. □

Theorem 16.7. *Let k be a field. Any ideal of $k[t]$ is principal. In particular, $(f, g) = (\gcd(f, g))$.*

Proof. Let I be an ideal in $k[t]$. Denote by f its element of minimum degree. Then for any $g \in I$ one has $g = fh + f_1$ for some $h, f_1 \in k[t], \deg f_1 < \deg f$. Since $f, g \in I$, one can conclude that $f_1 \in I$ whence $f_1 = 0$. Thus $I \subset (f)$. The inverse inclusion is obvious.

Now let $f, g \in k[t]$. By Bezout's identity, there exist $h_1, h_2 \in k[t]$ such that $fh_1 + gh_2 = d$, where $d = \gcd(f, g)$. Then $rd = (rh_1)f + (rh_2)g \in (f, g)$ for any $r \in k[t]$ that is $(d) \subset (f, g)$. The inverse inclusion follows from the fact that $d \mid h_1 f + h_2 g$ for any $h_1, h_2 \in k[t]$. □

Example. Consider the ideal $I = (x, 2)$ in the ring $\mathbb{Z}[x]$. Assume $I = (f)$ for some $f \in \mathbb{Z}[x]$. Then $f \mid 2$ and $f \mid x$, whence $f = \pm 1$. But $1 \notin I$ since 1 cannot be expressed as $xg(x) + 2h(x)$ for any $g, h \in \mathbb{Z}[x]$. Therefore I is not a principal ideal.

Exercise 16.3. *Consider the ring $R = \mathbb{Z}[\sqrt{-3}]$ and prove that its ideal $I = (2, 1 + \sqrt{-3})$ is not principal.*

Hint. It suffices to show that any common factor of 2 and $1 + \sqrt{-3}$ is a unit and $I \neq R$. Use N from Problem 16.5.

17 Quotient ring

Let I be an ideal of R. Any ideal is a subgroup of the additive group of R, thus the quotient group R/I can be considered.

Proposition 17.1. *Multiplication $\overline{a} \cdot \overline{b} = \overline{ab}$ is a well-defined operation on R_+/I which together with addition determines the structure of a (commutative associative unitary) ring.*

Proof. Suppose $a' - a = s, b' - b = t$ for some $a, a', b, b' \in R$ and $s, t \in I$. Then $a'b' - ab = (a+s)(b+t) - ab = at + sb + st \in I$, which proves that multiplication is well-defined.

The commutativity of multiplication follows from the commutativity of the ring R and the definition of multiplication: $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$.

The other axioms of the ring are verified in a similar manner. □

Definition. The quotient group R/I with above defined multiplication is called the **quotient ring** of R by I.

Exercise 17.1. *Prove the distributivity of $+$ and $\cdot$ in R/I. Explain every equality you write.*

Proposition 17.2. *Let k be a field, $f \in k[t]$ be an irreducible polynomial. Then $k[t]/(f)$ is a field.*

Proof. It suffices to prove that $\overline{g}$ is invertible for any $g \in k[t], g \notin (f)$. Since f is irreducible, either $f \mid g$ or $\gcd(f, g) = 1$. The former case is impossible since $g \notin (f)$, thus $\gcd(f, g) = 1$. Then Bezout's identity implies that there exist $h_1, h_2 \in k[t]$ such that $h_1 f + h_2 g = 1$. Thus $\overline{h_2} \cdot \overline{g} = \overline{h_2 g} = \overline{1}$ in $k[t]/(f)$ as required. □

Exercise 17.2. *Let k be a field, $f \in k[t]$ be a reducible polynomial. Show that $k[t]/(f)$ is not a field.*

Proposition 17.3. $\mathbb{R}[t]/(t^2+1)$ *is isomorphic to* $\mathbb{C}$.

Proof. Define the mapping $\Phi\colon \mathbb{R}[t]/(t^2+1) \to \mathbb{C}$ by $\Phi(\overline{g}) = g(i)$.

First, if $f \mid g_1 - g_2$, then $g_1(t) - g_2(t) = (t^2+1)h(t)$ for some $h \in \mathbb{R}[t]$, whence $g_1(i) - g_2(i) = 0$. It shows that Φ is well-defined.

Further,

$$\Phi(\overline{g}_1 + \overline{g}_2) = \Phi(\overline{g_1 + g_2}) = (g_1 + g_2)(i) = g_1(i) + g_2(i) = \Phi(\overline{g}_1) + \Phi(\overline{g}_2)$$

which implies that Φ preserves addition. A similar argument can be given for multiplication.

It remains to check that Φ is bijective. The surjectivity is evident. If $\Phi(\overline{g}_1) = \Phi(\overline{g}_2)$ then $h(i) = 0$ for $h = g_1 - g_2$. Then $h(-i) = h(\overline{i}) = \overline{h(i)} = 0$ and h is divisible both by $t - i$ and $t + i$ and thus by $(t - i)(t + i) = t^2 + 1$. Therefore $\overline{g}_1 = \overline{g}_2$. □

Exercise 17.3. *Prove that $\mathbb{R}[t]/(f)$ is isomorphic to $\mathbb{C}$ if $f(t) = at^2 + bt + c$, where $a \neq 0, b, c \in \mathbb{R}$ and $b^2 - 4ac < 0$.*

Hint. Follow the proof of Proposition 17.3. What will be the image of $\overline{t}$ in this case?

Exercise 17.4. *Let $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ and $I = (2 + i)$. Prove that R/I is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.*

18 Irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$

Definition. A **monic** polynomial is a polynomial in which the leading coefficient is equal to 1.

Proposition 18.1. *Let k be a field, $f \in k[t]$. Then f is divisible by a polynomial of degree 1 iff it has a root.*

Proof. If $\alpha \in k, f(\alpha) = 0$ then $(t-\alpha)|f(t)$ by the factor theorem. If $(at+b)|f(t)$ for $a, b \in k, a \neq 0$ then clearly $f(-ba^{-1}) = 0$. □

Proposition 18.2. *Let k be a field, $f \in k[t]$ and $\deg f = n$. If f is reducible, it is divisible by a monic polynomial $g \in k[t], \deg g \leq [n/2]$.*

Proof. Since f is reducible, $f = gh$ for some $g, h \in k[t], \deg g, \deg h < n$. Assume $\deg g \leq \deg h$. Then $\deg g + \deg h = n$ implies $\deg g \leq [n/2]$. Finally $f = (a^{-1}g)(ah)$ where a is the leading coefficient of g. Now $a^{-1}g$ is monic and $\deg a^{-1}g = \deg g \leq [n/2]$. □

The above statement allows one to search the irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ of a given degree n using the list of the irreducible polynomials of degree $\leq [n/2]$.

Problem 18.3. *Prove that $f = t^5 + t^2 + \overline{1}$ over $\mathbb{Z}/2\mathbb{Z}$ is irreducible.*

Solution. It suffices to verify that f is not divisible by any irreducible (monic) polynomial over $\mathbb{Z}/2\mathbb{Z}$ of degree 1 and 2. Since f has no roots, the first case is impossible. Next, we need a list of irreducible polynomials of degree 2 over $\mathbb{Z}/2\mathbb{Z}$. We write down all polynomials of degree 2 and cross out the reducible ones, i.e., those having a root:

$\cancel{t^2}$

$\cancel{t^2 + \overline{1}}$

$\cancel{t^2 + t}$

$t^2 + t + \overline{1}$

We see that there exists a unique irreducible polynomial over $\mathbb{Z}/2\mathbb{Z}$ of degree 2. Since it does not divide f, f is irreducible. □

Problem 18.4. *Prove that $f = t^6 + t^3 + \overline{1}$ over $\mathbb{Z}/2\mathbb{Z}$ is irreducible.*

Solution. Suppose

$$t^6 + t^3 + \overline{1} = (t^3 + a_2t^2 + a_1t + a_0)(t^3 + b_2t^2 + b_1t + b_0).$$

Since $a_0b_0 = \overline{1}$, we must have $a_0 = b_0 = \overline{1}$. By looking at the coefficients at t^5 and t, one can see $a_2 = b_2$ and $a_1 = b_1$. Then the coefficient at t^3 is $a_0 + a_1b_2 + a_2b_1 + b_0 = \overline{0}$, which is false. Now suppose

$$t^6 + t^3 + \overline{1} = (t^4 + a_3t^3 + a_2t^2 + a_1t + a_0)(t^2 + b_1t + b_0).$$

Again $a_0 = b_0 = \overline{1}$ and $a_3 = b_1, a_1 = b_1$. The coefficient at t^3 is $a_1 + a_2b_1 + a_3b_0 = \overline{0}$, whence $a_2 = b_1 = \overline{1}$. Now the coefficient at t^2 is $a_0 + a_1b_1 + a_2b_0 = \overline{1}$, which is false. □

Exercise 18.1. *Prove that $t^5 + \overline{2}t + \overline{1} \in \mathbb{Z}/3\mathbb{Z}[t]$ is irreducible.*

Exercise 18.2. *Prove that* $t^8 + t^7 + t^2 + t + \overline{1} \in \mathbb{Z}/2\mathbb{Z}[t]$ *is irreducible.*

Exercise 18.3. *Prove that* $f = 5t^5 + 4t^4 - 3t^2 + 9$ *is irreducible over* $\mathbb{Z}$.

Hint. Consider the reduction modulo 2 from $\mathbb{Z}[t]$ to $(\mathbb{Z}/2\mathbb{Z})[t]$, $\varphi = \sum_{j=0}^{n} a_j t^j \mapsto \overline{\varphi} = \sum_{j=0}^{n} \overline{a}_j t^j$. Clearly $\overline{\varphi\psi} = \overline{\varphi}\overline{\psi}$. Notice that $\overline{f}$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$.

19 Finite fields

Proposition 19.1. *If k is a finite field, then the characteristic of k is a prime number.*

Proof. If $\operatorname{char} k = ab, a, b > 1$, notice that $\mathbf{0} = \underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{ab \text{ times}} = (\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{a \text{ times}})(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{b \text{ times}})$. The field is an integral domain, so one of the two multipliers is equal to $\mathbf{0}$, but $a, b < ab$, a contradiction. □

Proposition 19.2. *Let k be a field.*

1. *If* $\operatorname{char} k = p$*, then k contains a field isomorphic to* $\mathbb{Z}/p\mathbb{Z}$.
2. *If k is finite, then* $\operatorname{char} k = p$ *and* $|k| = p^n$.

Proof. (1) Consider $L = \{\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{n \text{ times}} \mid n \geq 0\} \subset k$. Since $-\mathbf{1} = \underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{p-1 \text{ times}}$, one can see that L is a subgroup of the additive group of k generated by $\mathbf{1}$. Proposition 6.4 implies that $|L| = p$.

Now show that L is a field. Since L is a group under addition, we need only to verify the properties related to multiplication. First, L is closed under multiplication:

$$(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{m \text{ times}}) \cdot (\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{n \text{ times}}) = \underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{mn \text{ times}}.$$

Obviously $\mathbf{1} \in L$, and it remains to prove the existence of the multiplicative inverse of any non-zero element of L which can be represented as $(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{r \text{ times}})$, $0 < r < p$. Since $\gcd(r, p) = 1$, one has $rx + py = 1$ for some $x, y \in \mathbb{Z}$. Then also $r(x + pa) + p(y - ra) = 1$ for any $a \in \mathbb{Z}$ and thus one can assume that $x > 0, y < 0$. It remains to note that in this case

$$(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{r \text{ times}}) \cdot (\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{x \text{ times}}) = \underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{rx \text{ times}} = \mathbf{1} + (\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{p \text{ times}}) \cdot (\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{-y \text{ times}}) = \mathbf{1}.$$

Finally, it is easy to see that the map $(\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{n \text{ times}}) \mapsto \overline{n}$ from L to $\mathbb{Z}/p\mathbb{Z}$ is a field isomorphism.

(2) Consider the sequence $\mathbf{1}, \mathbf{1}+\mathbf{1}, \mathbf{1}+\mathbf{1}+\mathbf{1}, \ldots$ in k. Since k is finite, one has $\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{n \text{ times}} = \underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{m \text{ times}}$ for some $m > n$. Then $\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{m-n \text{ times}} = \mathbf{0}$, that is, $\operatorname{char} k = p$ for some prime p. Hence k contains a field L consisting of p elements. Consider k as a vector space over L. Since k is finite, the the dimension of this vector space is finite, denote it by n. Let $a_1, \ldots, a_n \in k$ be its basis. Then each $a \in k$ can be uniquely expressed in the form $a = \alpha_1 a_1 + \cdots + \alpha_n a_n$, which gives a bijection between k and L^n. Since the latter set has p^n elements, k also has p^n elements. □

Proposition 19.3. *If $f \in \mathbb{Z}/p\mathbb{Z}[x]$ is irreducible and $\deg f = n$, then $|\mathbb{Z}/p\mathbb{Z}[x]/(f)| = p^n$.*

Proof. It suffices to prove that $\mathbb{Z}/p\mathbb{Z}[x]/(f) = \{\overline{h} \in \mathbb{Z}/p\mathbb{Z}[x] \mid \deg h < n\}$ and all elements of this set are distinct. Clearly, $\overline{g} = \overline{h}$, where $g = fg_1 + h$ and $\deg h < \deg f = n$. If $\overline{h_1} = \overline{h_2}$ with $\deg h_1, \deg h_2 < n$, then $h_1 - h_2 = fh$ for some $h \in \mathbb{Z}/p\mathbb{Z}[x]$ and $\deg(h_1 - h_2) < n$. This is possible only if $h_1 - h_2 = 0$. □

Example. One can easily verify that $f(x) = x^2 + x + \overline{1}$ is the only irreducible quadratic polynomial over $\mathbb{Z}/2\mathbb{Z}$. The field $\mathbb{Z}/2\mathbb{Z}[x]/(f)$ consists of four elements: $\overline{0}, \overline{1}, \overline{x}, \overline{x+\overline{1}}$. Its Cayley tables are given below.

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+\overline{1}}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+\overline{1}}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+\overline{1}}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+\overline{1}}$	$\overline{0}$	$\overline{1}$
$\overline{x+\overline{1}}$	$\overline{x+\overline{1}}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+\overline{1}}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+\overline{1}}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+\overline{1}}$	$\overline{1}$
$\overline{x+\overline{1}}$	$\overline{0}$	$\overline{x+\overline{1}}$	$\overline{1}$	$\overline{x}$

Exercise 19.1. *Construct a field of 8 elements. Write some non-evident entries of its Cayley tables.*

Exercise 19.2. *Let $f(x) = x^3 - x + \overline{1} \in \mathbb{Z}/3\mathbb{Z}[x]$. Using the representation of the elements of the field $\mathbb{Z}/p\mathbb{Z}[x]/(f)$ as $a\overline{x}^2 + b\overline{x} + c \mid, a, b, c \in \mathbb{Z}/3\mathbb{Z}$, find $(\overline{x}^2 + \overline{1})^{-1}$.*

Hint. Follow the proof of Proposition 17.2.

20 Field extensions and minimal polynomials

Definition. If a subset K of a field L is a field with respect to the operations induced from L, then K is called a **subfield** of L and L is an **extension** of K (notation: L/K).

A **basis** of an extension L/K is a basis of L as a vector space over K. The **degree** of L/K is the dimension of L as a vector space over K (notation: $[L : K]$). An extension is **finite** if its degree is finite.

Examples.
1. K/K with basis 1; $[K : K] = 1$
2. $\mathbb{C}/\mathbb{R}$ with basis $1, i$; $[\mathbb{C} : \mathbb{R}] = 2$
3. $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$, where $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, with basis $1, \sqrt{2}$; $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$
4. $\mathbb{R}/\mathbb{Q}$ is an infinite extension

Proposition 20.1. *If L/K and N/L are finite extensions, then N/K is also finite and $[N : K] = [N : L][L : K]$.*

the tower of extension.

Proof. Let $\{a_i\}_{i=1}^n$ be a basis of L/K, $\{b_j\}_{j=1}^m$ be a basis of N/L. It suffices to prove that $\{a_ib_j\}_{1\leq i\leq n, 1\leq j\leq m}$ is a basis of N/K.

Let $\sum_{1\leq i\leq n,1\leq j\leq m}\gamma_{ij}a_ib_j = 0$ for some $\gamma_{ij}\in K, 1\leq i\leq n, 1\leq j\leq m$. Since $\{b_j\}_{j=1}^m$ is a basis of N/L , then $\sum_{j=1}^m(\sum_{i=1}^n\gamma_{ij}a_i)b_j = 0$ implies $\sum_{i=1}^n\gamma_{ij}a_i = 0$ for any $1\leq j\leq m$. Since $\{a_i\}_{i=1}^n$ is a basis of L/K, these equalities imply $\gamma_{ij} = 0$ for any $1\leq i\leq n$.

Now take an arbitrary $c\in N$. Since $\{b_j\}_{j=1}^m$ is a basis of N/L, then $c = \sum_{j=1}^m\alpha_jb_j$ for some $\alpha_1,\ldots,\alpha_m\in L$. Since $\{a_i\}_{i=1}^n$ is a basis of L/K , then for every $1\leq j\leq m$ one can find $\gamma_{ij}\in K, 1\leq i\leq n$ such that $\alpha_j = \sum_{i=1}^m\gamma_{ij}a_i$. This gives $c = \sum_{j=1}^m(\sum_{i=1}^m\gamma_{ij}a_i)b_j = \sum_{1\leq i\leq n,1\leq j\leq m}\gamma_{ij}a_ib_j$. □

Definition. Let L/K be and extension and $\alpha\in L$. If there is $f\in K[t]$ such that $f(\alpha)=0$ then α is said to be **algebraic** over K, otherwise α is **transcendental** over K.

Examples.

1. $\sqrt{2}$ is algebraic over $\mathbb{Q}$
2. e and π are transcendental over $\mathbb{Q}$

Lemma 20.2. *Let L/K be a finite extension. Then each $\alpha\in L$ is algebraic over K.*

Proof. Let $[L:K]=n$. Consider $1,\alpha,\alpha^2,\ldots,\alpha^n\in L$. They are linearly dependent as elements of the vector space L over K, so $\sum_{j=0}^n a_j\alpha^j = 0$ for some $a_0,\ldots,a_n\in K$. Then $f(t)=\sum_{j=0}^n a_jt^j$ is a required polynomial. □

Definition. Let L/K be an extension, $\alpha\in L$ is algebraic over K. A polynomial $f\in K[t]$ is called **minimal** for α if $f(\alpha)=0$ and $\deg g\geq\deg f$ for any $g\in K[t]$ such that $g(\alpha)=0$.

Examples.

1. A minimal polynomial for $\alpha\in K$ over K is $t-\alpha$
2. A minimal polynomial for i over $\mathbb{R}$ is t^2+1

Proposition 20.3. *Let L/K be an extension, $\alpha\in L$ is algebraic over K.*

1. *A minimal polynomial for α is irreducible.*
2. *If f is a minimal polynomial for α and $g\in K[t], g(\alpha)=0$, then $f\mid g$.*
3. *If $f\in K[t]$ is irreducible and $f(\alpha)=0$, then f is a minimal polynomial for α*
4. *A minimal polynomial is uniquely defined up to associativity. A monic minimal polynomial is unique.*

Proof. (1) Let f be a minimal polynomial for α and $f=gh, g,h\in K[t], \deg g,\deg h<\deg f$. Then $g(\alpha)h(\alpha)=f(\alpha)=0$, so either $g(\alpha)=0$ or $h(\alpha)=0$, a contradiction.

(2) One has $g=fh+r, h,r\in K[t]$ and $\deg r<\deg f$. Then $r(\alpha)=g(\alpha)-f(\alpha)h(\alpha)=0$, whence $r=0$.

(3) By the previous property f is divisible by a minimal polynomial, which is irreducible. Since f itself is irreducible, f is associated with the minimal polynomial, and hence has the minimum degree.

(4) If f_1,f_2 are minimal polynomials for α, then $f_1\mid f_2$ and $f_2\mid f_1$, therefore they are associated. □

这一过程说明了. $\sqrt{\cdots} + \sqrt{\cdots} + \sqrt{\cdots}$
始终是 algebraic 的.

Problem 20.4. *Find the minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.*

Solution. Denote $\alpha = \sqrt{2} + \sqrt{3}$. Then $\alpha^2 - 2\alpha\sqrt{2} + 2 = (\alpha - \sqrt{2})^2 = 3$, whence $(\alpha^2 - 1)^2 = (2\alpha\sqrt{2})^2 = 8\alpha^2$. Now $f(\alpha) = 0$ for $f(t) = (t^2 - 1)^2 - 8t^2$. Clearly no linear or quadratic polynomial over $\mathbb{Q}$ has α as its root, hence f is the minimal polynomial for α. $\square$

Problem 20.5. *Let $F = \mathbb{Z}/2\mathbb{Z}[t]/(t^4 + t + \bar{1})$. Find the minimal polynomial for $\overline{t^2 + t} \in F$ over $\mathbb{Z}/2\mathbb{Z}$.*

Solution. Denote $\alpha = \overline{t^2 + t}$. Then $\alpha^2 = \overline{t^4 + t^2} = \overline{t^2 + t + 1}, \alpha^3 = \bar{t}, \alpha^4 = \overline{t^3 + t^2}$. Now the identity $a_4(\bar{t}^3 + \bar{t}^2) + a_3\bar{t} + a_2(\bar{t}^2 + \bar{t} + \bar{1}) + a_1(\bar{t}^2 + \bar{t}) + a_0 = \bar{0}$ is equivalent to the system of linear equations

$$\begin{cases} a_0 + a_2 = \bar{0} \\ a_1 + a_2 + a_3 = \bar{0} \\ a_1 + a_2 + a_4 = \bar{0} \\ a_4 = \bar{0} \end{cases}.$$

It has a non-zero solution $a_4 = a_3 = \bar{0}, a_2 = a_1 = a_0 = \bar{1}$ whence $f(x) = x^2 + x + \bar{1}$ is the minimal polynomial for α. $\square$

Exercise 20.1. *Let $F = \mathbb{Z}/3\mathbb{Z}[t]/(t^3 - t + \bar{1})$. Find the minimal polynomial for $\overline{t^2} \in F$ over $\mathbb{Z}/3\mathbb{Z}$.*

Exercise 20.2. *Let L/K be a finite extension, $\alpha \in L$. Consider $T_\alpha \colon L \to L, T_\alpha(x) = \alpha x$ which is an operator on the vector space L over K.*

i) *Find χ_{T_α} for the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.*

ii) *Prove that $\chi_{T_\alpha}(\alpha) = 0$.*

Hint. In (ii), use the Cayley-Hamilton theorem.

21 Field extensions generated by algebraic elements

Proposition 21.1. *Let L/K be an extension, $\alpha \in L$ be algebraic over K. Define $K(\alpha) = \{g(\alpha) \mid g \in K[t]\} \subset L$. Then*

1. *$K(\alpha)$ is a field*

2. *$K(\alpha)$ is the minimal subfield of L containing K and α.*

3. *$1, \alpha, \ldots, \alpha^{n-1}$ is a basis of the extension $K(\alpha)/K$ and $[K(\alpha) : K] = \deg f$, where f is the minimal polynomial of α over K.*

Proof. (1) The fact that $K(\alpha)$ is closed with respect to addition, multiplication and taking additive inverses is obvious, $0, 1 \in K(\alpha)$. It remains to check that for any $g(\alpha) \neq 0$, its multiplicative inverse also belongs to $K(\alpha)$. Since $g(\alpha) \neq 0$ and f is irreducible, one has

$\gcd(f,g)=1$. Thus $fh_1+gh_2=1$ for some $h_1,h_2\in K[t]$ by Bézout's identity and $g(\alpha)h_2(\alpha)=1$ as required.

(2) Obviously, $K(\alpha)$ contains both K and α. If L' is an extension of K which contains α, then L' contains $g(\alpha)$ for any $g\in K[t]$, hence $K(\alpha)\subset L$.

(3) If $n=\deg f$, we prove that $1,\alpha,\dots,\alpha^{n-1}$ form a basis of $K(\alpha)$ over K. Indeed, if $g(\alpha)\in K(\alpha)$ for $g\in K[t]$, then $g=fh+g_1$ for some $h,g_1\in K[t]$ and $\deg g_1<n$. Then $g_1=\sum_{j=1}^{n-1}a_jt^j$ for $a_0,\dots,a_{n-1}\in K$ and $g(\alpha)=g_1(\alpha)=\sum_{j=1}^{n-1}a_j\alpha^j$.

If $\sum_{j=1}^{n-1}a_j\alpha^j=0$ then $g(\alpha)=0$ for $g=\sum_{j=1}^{n-1}a_jt^j$. If $g\neq 0$ then $\gcd(f,g)=1$ since f is irreducible and $\deg g<\deg f$. By Bézout's identity, $fh_1+gh_2=1$ for some $h_1,h_2\in K[t]$ which leads to a contradiction. Thus $g=0$ and $a_0=a_1=\dots=a_{n-1}=0$. □

Corollary 21.2. *If $f\in K[t]$ is a minimal polynomial for $\alpha\in L$, then $\deg f\mid[L:K]$*

Proof. One has $[K(\alpha):K][L:K(\alpha)]=[L:K]$ by Propositions 20.1. □

Example. $\mathbb{Q}(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}\mid a,b,c\in\mathbb{Q}\}$

Definition. The field $K(\alpha)$ constructed in the above proposition is called the **extension of K generated by α.**

Problem 21.3. *Remove the irrationality in the denominator in $\frac{1}{(\sqrt[4]{2}+1)^3+2}$.*

Solution. First, it is obvious that $\sqrt[4]{2}$ is a root of the irreducible polynomial $f(t)=t^4-2$ over $\mathbb{Q}$. We find the greatest common divisor of f and $g(t)=(t+1)^3+2$ and multipliers of Bézout's identity:

$$-(6t^2+42t+59)f(t)+(6t^3+24t^2-31t+3)g(t)=127,$$

so it suffices to multiply the numerator and the denominator of the fraction by $6\sqrt[4]{8}+24\sqrt[4]{4}-31\sqrt[4]{2}+3$. □

Definition. Let L/K be an extension, $M\subset L$. The **extension of K generated by M** is an extension $K(M)$ of K containing M such that if L is an extension of K and $M\subset L$ then $K(M)\subset L$.

Proposition 21.4. *There exists a unique $K(M)$. Moreover, $K(M_1)(M_2)=K(M_1\cup M_2)$ for any $M_1,M_2\subset L$.*

Proof. Let $K(M)$ be the intersection of all extensions of K containing M. The intersection of fields is a field therefore $K(M)$ is an extension of K containing M. Clearly if L is an extension of K and $M\subset L$ then $K(M)\subset L$.

Since $M_1,M_2\subset K(M_1)(M_2)$, one has $K(M_1\cup M_2)\subset K(M_1)(M_2)$. Conversely, $K(M_1\cup M_2)$ is an extension of $K(M_1)$ containing M_2 and thus $K(M_1)(M_2)\subset K(M_1\cup M_2)$. □

Problem 21.5. *Show that $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.*

Solution. Put $\alpha=\sqrt{2}+\sqrt{3}$. Since $\alpha^3=11\sqrt{2}+9\sqrt{3}$, one has $\sqrt{2}=\frac{1}{2}(\alpha^3-9\alpha)$, $\sqrt{3}=-\frac{1}{2}(\alpha^3-11\alpha)$. Now $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is a field containing $\sqrt{2},\sqrt{3}$ and clearly for any extension $L/\mathbb{Q}$ with $\sqrt{2},\sqrt{3}$ one has $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subset L$. □

Exercise 21.1. *Prove that* $\mathbb{Q}(i, \sqrt[3]{2}) = \mathbb{Q}(i\sqrt[3]{2})$.

Exercise 21.2. *Show that* $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$.

Hint. Use Problem 21.5.

Exercise 21.3. *Remove the irrationality in the denominator in* $\frac{1}{1+\sqrt{2}+\sqrt{3}-\sqrt{6}}$.

Hint. Find a polynomial $f \in \mathbb{Q}[t]$ such that $f(1 + \sqrt{2} + \sqrt{3} - \sqrt{6}) = 0$.

Exercise 21.4. *Find the minimal polynomial of* $\alpha = \sqrt{2} + \sqrt[3]{3}$ *over* $\mathbb{Q}$. *Don't forget to prove its minimality.*

Hint. Since $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{3})$ are subfields of $\mathbb{Q}(\alpha)$, the degree of the minimal polynomial for α over $\mathbb{Q}$ must be at least 6.

22 Angle trisection and doubling the cube

Problem I: *Construct an angle equal to one-third of a given arbitrary angle, using only a compass and an (unmarked) straightedge.*
Problem II: *Construct the edge of a cube whose volume is double that of the given cube, using only a compass and an (unmarked) straightedge.*

Reminder from elementary geometry: Using a compass and a straightedge, one can construct

- The perpendicular line through a given point to a given line
- The line through a given point parallel to a given line

Definition. Given a set $M \subset \mathbb{R}^2$, a point $P \in \mathbb{R}^2$ is **constructible in one step** from M if P is the intersection of two distinct figures where each figure is either:

a) the line $\overline{AB}$ where $A, B \in M$.

b) the circle with radius $|AB|$ centered on C where $A, B, C \in M$.

A point $P \in \mathbb{R}^2$ is **constructible** from M if there are $P_1, P_2, \ldots, P_n \in \mathbb{R}^2$ such that $P_n = P$ and P_i is constructible in one step from $M \cup \{P_1, P_2, \ldots, P_{i-1}\}$ for each $1 \leq i \leq n$.

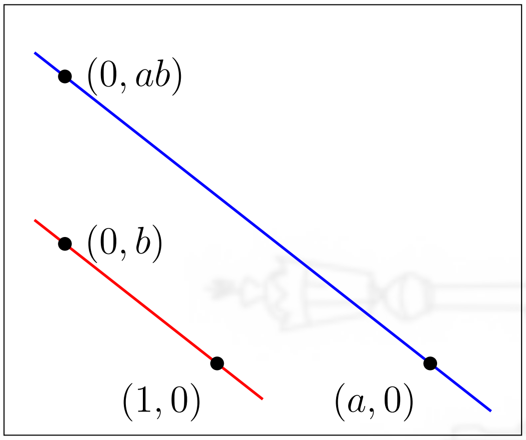
A real number $x \in \mathbb{R}$ is **constructible** if $(x, 0)$ is constructible from $\{(0, 0), (1, 0)\}$.

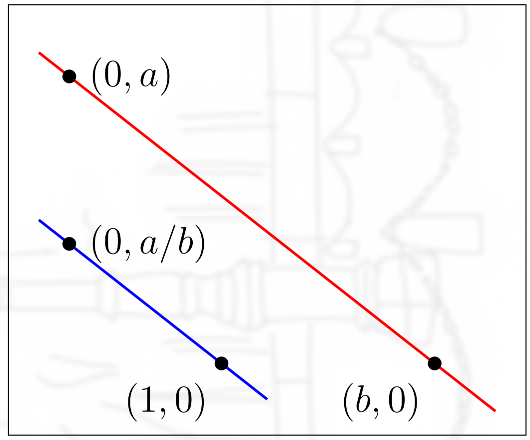
Proposition 22.1. *1. A point* $(x, y) \in \mathbb{R}^2$ *is constructible if and only if* x, y *are constructible*

2. A point $(x, y) \in \mathbb{R}^2$ *is constructible if* $(y, x) \in \mathbb{R}^2$ *is constructible*

3. If $x, y \in \mathbb{R}$ *are constructible then* $x + y, xy$ *and* x/y *are constructible.*

Proof. The first two statements are evident. The third statement follows from the below pictures





□

Corollary 22.2. *The constructible numbers form a field.*

Proposition 22.3. *If a point $(x, y) \in \mathbb{R}^2$ is constructible in one step from a subset $M \subset \mathbb{R}^2$ then either $x, y \in \mathbb{Q}(M')$ or x, y are roots of quadratic polynomials over $\mathbb{Q}(M')$, where M' is the set of the coordinates of the points of M.*

Proof. Below are the equations for the line $\overline{AB}$ and the circle with radius $|DE|$ centered on C, respectively:

$$(x_B - x_A)(y - y_A) = (y_B - y_A)(x - x_A)$$
$$(x_C - x)^2 + (y_C - y)^2 = (x_D - x_E)^2 + (y_D - y_E)^2.$$

If $A, B, A', B' \in M$ then the intersection of the lines $\overline{AB}$ and $\overline{A'B'}$ is determined by the system of two linear equations over $\mathbb{Q}(M')$ and thus its coordinates belong to $\mathbb{Q}(M')$.

If $A, B, C, D, E \in M$ then the intersection of the line $\overline{AB}$ and the circle centered at C with radius $|DE|$ is determined by the system of the linear and quadratic equations over $\mathbb{Q}(M')$ and thus its coordinates are roots of quadratic polynomials over $\mathbb{Q}(M')$.

The intersection of two circles equals the intersection of one of them and the line connecting the intersection points, thus this case follows from the previous one. □

Corollary 22.4. *If a point $(x, y) \in \mathbb{R}^2$ is constructible in one step from a subset $M \subset \mathbb{R}^2$ and $N = M \cup \{(x, y)\}$ then $[\mathbb{Q}(N') : \mathbb{Q}(M')] = 1, 2$ or 4, where M', N' are the sets of the coordinates of the points of M, N, respectively.*

Proof. Since $N' = M' \cup \{x, y\}$, Proposition 20.1 implies

$$[\mathbb{Q}(N') : \mathbb{Q}(M')] = [\mathbb{Q}(M' \cup \{x, y\}) : \mathbb{Q}(M' \cup \{x\})] \cdot [\mathbb{Q}(M' \cup \{x\}) : \mathbb{Q}(M')].$$

Both latter extensions are either trivial or generated by roots of quadratic polynomials, thus their degrees are 1 or 2. □

Proposition 22.5. *If $a \in \mathbb{R}$ is constructible then its minimal polynomial over $\mathbb{Q}$ has degree 2^n for some $n \in \mathbb{N}$.*

Proof. By Corollary 21.2, it suffices to show that $[\mathbb{Q}(a) : \mathbb{Q}] = 2^m$ for some $m \in \mathbb{N}$. Let $P_0, P_1, \ldots, P_s \in \mathbb{R}^2$ and $M_i = \{P_0, P_1, \ldots, P_i\}, i \geq 1$ be such that

a) $P_0 = (0,0), P_1 = (1,0)$

b) $P_s = (a, 0)$

c) P_{i+1} is constructible in one step from $M_i, i \geq 1$

By Corollary 22.4, for any $i \geq 1$ one has $[\mathbb{Q}(M'_{i+1}) : \mathbb{Q}(M'_i)] = 1, 2$ or 4 where M'_i is the set of the coordinates of the points of M_i. Then $[\mathbb{Q}(M_s) : \mathbb{Q}] = 2^r$ for some $r \in \mathbb{N}$ by Proposition 20.1. Now the identity $[\mathbb{Q}(M_s) : \mathbb{Q}] = [\mathbb{Q}(M_s) : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}]$ gives the desired result. □

Remark. If the $a \in \mathbb{R}$ has the minimal polynomial of degree 4 over $\mathbb{Q}$, it may not be constructible.

Corollary 22.6. *1. It is not possible, using only a compass and straightedge, to construct a cube with double the volume of any given cube.*

2. It is not possible, using only a compass and straightedge, to trisect any given angle.

Proof. If it is possible then $\alpha_1 = \sqrt[3]{2}$ and $\alpha_2 = 2\cos\frac{\pi}{9}$ would be constructible numbers. They are roots of the polynomials $f_1(t) = t^3 - 2$ and $f_2(t) = t^3 - 3t - 1$, respectively. These polynomials have no rational roots by the Rational root theorem and thus are irreducible over $\mathbb{Q}$. Therefore $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = [\mathbb{Q}(\alpha_2) : \mathbb{Q}] = 3$, a contradiction. □

Exercise 22.1. *Prove that a regular heptagon can not be constructed using a compass and an straightedge.*

Hint. Show that $\alpha = 2\cos\frac{\pi}{7}$ is not a constructible number by finding its minimal polynomial.