ALGEBRA 1: groups, rings and fields

Groups

The set of pairs (a, b), where a is an element of A and b is an element of B is called a **product** of A and B and is denoted by $A \times B$. A mapping $f : A \to B$ from a set A to a set B is called an **injective mapping** or **injection** or **one-to-one mapping** (these are synonyms), if it maps different elements of the set A to different elements of the set B. A mapping is called a **surjective mapping** or a **surjection** or an **onto mapping** if for every element x of set B there exists at least one element of A that is mapped to x. A mapping is called **bijective mapping** or **bijection** or a **one-to-one mapping** if it is surjective and injective.

Let A be some set, either finite or infinite. Let $S(A)$ denote the set of all bijective mappings from A to itself. If f, g are two such mappings then they can be "multiplied" using composition $f \circ g$:

$$f \circ g(a) = f(g(a)).$$

A set $S(A)$ endowed with this operation is called "permutation group (or substitution group)" or more precisely "the group of permutations of A". Identity permutation is denoted by 1_A (or Id_A as well).

$S(A)$ is also called a **symmetric group**. If A is a finite set of n elements then $S(A)$ is denoted by S_n.

Permutations can be represented by tables; for example, a permutation $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 1$, $4 \mapsto 2$ of $1, 2, 3, 4$ can be written down as $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$. The numbers are written in the ascending order in the upper line, their images are written in the lower line.

Exercise 1.1. Compute the composition

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Exercise 1.2. a. How many permutations of $1, 2, \ldots, 5$ are there? How many of them leave 1 unchanged?

b. How many of them map 1 to 5?

c. How many permutations are there such that $\sigma(1) < \sigma(2)$?

d. How many permutations are there such that $\sigma(1) < \sigma(2) < \sigma(3)$?

Exercise 1.3. How many elements are there in $S(A)$ if A is a finite set of n elements?

Exercise 1.4. Is it true that $f \circ g = g \circ f$ for any f, g?

For any permutation $f \in S(A)$ ("$\in$" means that the element belongs to the set) there exists a unique "inverse permutation" f^{-1}, i.e. a permutation such that $f \circ f^{-1} = f^{-1} \circ f = 1_A$.

A **cyclic permutation** of a set $a, b, c, d, \ldots, w$ maps a to b, b to c, c to d and so on. Such a permutation is denoted by $(a, b, c, d, \ldots, w)$. The number of elements in the brackets is its **order**. **Transposition** is a cyclic permutation of order 2; it permutes two elements and leaves all other elements unchanged.

Exercise 1.5. Let $\sigma = (123)$, $\tau = (34)$. Calculate $\tau \circ \sigma \circ \tau^{-1}$.

Exercise 1.6. Prove that every permutation is a product of transpositions.

Exercise 1.7 (*). Is it possible that a product of even number of transpositions be an identity permutation?

Hint. What happens to a polynomial $(x_1 - x_2)(x_1 - x_3)\dots(x_1 - x_n)(x_2 - x_3)\dots$ (a product of $(x_i - x_j)$ for all $i > j$) when x_i and x_j are permuted?

A permutation group $S(A)$ is endowed with the following structure: operation of multiplication of permutations, operation of taking inverse of a permutation, the identity permutation. It is useful to axiomatize this structure.

Definition 1.1. Let G be a set with the following operations defined on it: $f, g \mapsto f \cdot g$ ("multiplication"), $f \mapsto f^{-1}$ ("taking inverse") and let the "identity element" 1_G be defined as well. Let the following axioms be satisfied:

a. "Associativity": $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ for all f, g, h.

b. "Identity": $f \cdot 1_G = 1_G \cdot f = f$ for all f.

c. "Inverse element": $f \cdot f^{-1} = f^{-1} \cdot f = 1_G$ for all f.

In this case we call G a **group**.

A subset of G which is closed under these operations is called a **subgroup of** G .

Exercise 1.8. Consider a group G. Prove that for any two elements f and g of it

a. If $fg = f$ or $gf = f$ then $g = 1$;

b. If $fg = 1$ or $gf = 1$ then $g = f^{-1}$.

Remark. This means that to define a group structure on a set G it suffices to define an operation of multiplication. Identity element and operation of taking inverse are uniquely determined by it and can be then reconstructed.

Exercise 1.9. Are these sets (with indicated operations) groups?

a. Natural numbers with an operation of addition;

b. Integer numbers with an operation of addition;

c. Integer numbers with an operation of multiplication;

d. Rational numbers with an operation of multiplication;

e. Real numbers with an operation of addition;

f. Real numbers with an operation of multiplication;

g. (*)Planar motions with an operation of composition;

h. Numbers strictly greater than -1 and strictly less than 1 with an operation defined by the formula $u * v = (u + v)/(1 + uv)$ (check that the operation is defined correctly);

i. Figures (sets of points) on a plane with an operation of union;

j. **(*)**Figures (sets of points) on a plane with an operation of symmetric difference: $A * B$ contains points that belong to precisely to one of the figures (A or B);

k. **(*)**Mappings from a fixed set C into a fixed group G with an operation $(f \cdot g)(s) = f(s)g(s)$.

"Product of groups" G_1 and G_2 is a set of pairs (g_1, g_2), $g_1 \in G_1, g_2 \in G_2$ with an operation

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$$

A mapping $f : G \to G'$ from a group G into a group G' is called a **homomorphism** if it preserves the multiplication: $f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2)$. A homomorphism is called a **monomorphism**, if it is injective, an **epimorphism** if it is surjective and an **isomorphism** if it is bijective. Groups G, G' are **isomorphic** if there exists an isomorphism between them. An isomorphism of a group into itself is called an **automorphism**.

Exercise 1.10. Prove that if $f : G \to G'$ is a homomorphism of groups then for any $g \in G$ $f(1_G) = 1_{G'}$ and $f(g^{-1}) = (f(g)^{-1})$.

Definition 1.2. If a homomorphism $G \to S(A)$ of a group G into a group $S(A)$ of permutations of a set A is defined then one says that G **acts on a set** A (and indeed every element of G permutes the elements of A somehow). The action of G on A can be thought of as a mapping $G \times A \xrightarrow{\rho} A$, $a, g \mapsto \rho(g, a)$. Sometimes the notation for an action of a group on a set is even simpler: $a, g \mapsto g(a)$.

Exercise 1.11. Prove that every group admits an injective homomorphism into a permutation group (of a not necessarily finite set).

Hint. Think about what the meaning of the following phrase can be: "Group G acts on itself by multiplication on the left".

Exercise 1.12. Is it true that

a. every group that consists of two elements is isomorphic to permutation group S_2;

b. every group that consists of six elements is isomorphic either to permutation group S_3 or to the product of two non-trivial (i.e. those that have more than one element) groups.

Exercise 1.13 (*). Prove that permutation group S_n is not isomorphic to the product of two non-trivial groups.

Exercise 1.14. Let G be a group and $g \in G$ its element. Is it true that the sequence $g, g^2, g^3, \ldots$ is periodic? Is it true if G is a finite group?

Let n be a natural number. It is said that $g \in G$ is an **element of order** n in a group G if $g^n = 1_G$ but $g^k \neq 1_G$ for any $k < n$.

Exercise 1.15 (!). Consider a finite group of n elements. Prove that n is divisible by the order of every element of that group.

Hint. Consider the action of the group on itself by multiplication on the left.

Exercise 1.16 (*). Consider a group with an even number of elements. Prove that it contains an element of order 2.

Exercise 1.17 (*). Is it true that

a. the group D_{12} of rotations of a regular 12-gon is isomorphic to a product $D_6 \times S_2$ where D_6 is a group of rotations of a regular hexagon;

b. the group D_6 is isomorphic to a product $D_3 \times S_2$ where D_3 is a group of rotations of a triangle.

A group is called **commutative** or an **Abelian group** if $f \cdot g = g \cdot f$ for all f, g. Two elements f, g **commute** if $f \cdot g = g \cdot f$.

Exercise 1.18. Which groups out of those considered in the exercise 1.9 are commutative?

Exercise 1.19 (*). a. A **center** of a group G is a set consisting of all the elements $g \in G$ such that $gg' = g'g$ for all $g' \in G$. Prove that center is a subgroup.

b. Consider a group G such that there exist an element in it of order > 2. Consider a subgroup G' such that all elements $g \in G$ that do not belong to G' have order 2. Give an example of such a situation (or prove that it is not possible). Is G always finite when the mentioned conditions hold?

c. In the conditions of a previous question prove that G' is an abelian group

d. Let G' contain a center G. Prove that a group G is uniquely (up to an isomorphism) determined by the G' subgroup if the condition from (2) holds. (G' is called then a dihedral group)

e. Consider a dihedral group G corresponding to an abelian group G' as shown above. Let G' be a product of S_2 and some other abelian group: $G' = S_2 \times G''$. Prove that G is a product of S_2 and a dihedral group.

Rings and fields

Consider real numbers, integer numbers and finite decimal fractions. There are the following operations defined on these structures

a. Addition which is commutative and makes a group out of a set (addition is designated as "+"; taking an inverse element is designated as "-")

b. Multiplication which is also commutative but does not make a group out of any of the considered sets because some elements are non-invertible (multiplication is designated by a dot; the dot is often omitted: one writes xy instead of $x \cdot y$).

It is useful to axiomatize these structures.

Definition 1.3. Let R be a set with two operations $a, b \mapsto a + b$ (addition) and $a, b \mapsto a \cdot b$ (multiplication). Let elements 0 and 1 (zero and identity) be defined in R. If the following holds then R is called a **ring**:

a. R is a commutative group with respect to the operation of addition, 0 is a the identity element in this group

b. 1 is an identity with respect to multiplication: $1 \cdot a = a \cdot 1 = a$ for all a.

c. Associativity for multiplication: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

d. Distributivity: $a \cdot (b + c) = a \cdot b + a \cdot c$.

If the multiplication is commutative then one says that a ring R is commutative. If, moreover, the multiplication is invertible for all $a \neq 0$, i.e. $R\backslash\{0\}$ is a group with respect to multiplication then R is called a **field**.

In this chapter as well as in several following chapters we will consider only commutative rings and we will omit the word "commutative" for brevity; unless it is stated otherwise explicitly all the rings are assumed to be commutative.

Exercise 1.20. Are the following sets (equipped with natural operations unless they are specified explicitly) the rings:

a. natural numbers

b. integer numbers

c. even integer numbers

d. rational numbers

e. irrational numbers

f. finite decimal fractions

g. pairs of integer numbers with the coordinatewise addition and multiplication

h. pairs of integer numbers with the coordinatewise addition and multiplication defined by the formula $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$

i. **(*)** pairs of rational numbers with the coordinatewise addition and multiplication defined by the formula $(a, b) \cdot (c, d) = (ac + 2bd, ad + bc)$.

j. **(*)**figures on the plane (addition is symmetric difference, multiplication is intersection).

k. **(*)**mappings from a fixed set C into a fixed group G with an operation $(f \cdot g)(s) = f(s)g(s)$.

Exercise 1.21. Which rings from the exercise 1.20 are fields?

Exercise 1.22. Consider a ring R. Consider a set of sequences

$$a = (a_0, a_1, \dots, a_i, \dots, 0, 0, \dots)$$

consisting of elements of R with the finite number of non-zero elements. Define the operations on this set as follows

$$(a + b)_i = a_i + b_i,$$

$$(a \cdots b)_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Prove that this set is a ring (check in particular that multiplication is associative).

The ring defined in the exercise 1.22 is called a **ring of polynomials of single variable** on R, it is denoted by $R[x]$. Elements of $R[x]$ are called "polynomials". They are usually written down in the form $a_0 + a_1 x + \cdots + a_i x^i$ (for all $j > i$, a_j are zero).

In the algebra course we will suppose the notion of a real number known, (for example, you can think about real numbers as of infinite decimal fractions with usual operations defined on the

fractions). The rigorous definition is given in the course of geometry, topology and analysis. All we need in the algebra course is

Important note: Real numbers form a field.

This "important note" is also proven in the course of geometry, topology and analysis. Besides that, we need the following property :

Exercise 1.23 (*). Prove that every equation of the form

$$x^{2n+1} + a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \cdots + a_1x + a_0 = 0$$

has a real solution.

You should try solving this exercise when you are familiar with the notion of a real number.

Exercise 1.24 (*). Will the ring defined in the exercise 1.20 9 be a field if we change "rational numbers" for "real numbers" in the definition?

Exercise 1.25. Consider a fixed natural number n. Natural numbers divided by n have remainders 0, 1, 2, $\dots n-1$. Let us denote the operation of taking remainders by $\mod n$. Two numbers that have the same remainders $\mod n$ are called equal modulo n. Let us define addition and multiplication on a set of numbers $\mod n$ in such a way that

$$(x \mod n) + (y \mod n) = ((x+y) \mod n),$$
$$(x \mod n) \cdot (y \mod n) = (xy \mod n)$$

would hold for all pairs of integer numbers x, y. Prove that this definition is correct and the set of remainders form a ring.

Exercise 1.26 (*). Prove that the set of remainders $\mod n$ with the addition and multiplication defined as above form a field iff n is a prime number.

Remark. If you cannot solve this problem right away, put it away: the same problem will be reintroduced without an asterisk after defining some useful intermediate notions.

Exercise 1.27. Build the field which consists of

a. 2 elements

b. 3 elements

c. (*)4 elements.

Exercise 1.28 (*). Prove that there is no field that consists of 6 elements

Exercise 1.29. Prove that if p is a prime number then a field that consists of p elements is unique up to isomorphism.

Definition 1.4. Characteristic of a field k is 0 if $1 \in k$ has infinite order with respect to addition, otherwise it is equal to the order p of an element $1 \in k$ if it is finite.

Exercise 1.30. Prove that if the characteristic p of a field k is not zero then p is a prime number.

Exercise 1.31 (*). Consider a field of characteristic p. Prove that Frobenius mapping $x \mapsto x^p$ preserves multiplication and addition (just like with the groups such a mapping is called a homomorphism).

Hint. Use the binomial theorem.

Exercise 1.32 (*). Deduce Fermat's smaller theorem from that: x^p is equal to x modulo p for any integer number x.

Let $P = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial with the coefficients in the field k. A **root** P is an element α of a field k such that $P(\alpha) = 0$.

Exercise 1.33. Let α be the root of a polynomial P over a field k. Prove that a polynomial P can be divided by $z - \alpha$ in the ring $k[z]$

Hint. Use the long division of polynomials:

$$\begin{array}{rl|l} x^2 + 2x - 12 & & x+5 \\ \cline{3-3} x^2 + 5x & & x-3 \\ \cline{1-1} \quad -3x - 12 & & \\ \quad -3x - 15 & & \\ \cline{1-1} \qquad\qquad 3 & & \end{array}$$

Exercise 1.34. Prove that nonzero polynomial of degree n over a field cannot have more than n different roots.

Hint. Use the previous exercise.

Let P be a nonzero polynomial over a field k. A polynomial P is called **irreducible** if it cannot be represented as a product of polynomials of smaller degree.

Consider the set of remainders modulo P in a ring $k[x]$.

Exercise 1.35. Prove that this is a ring (we denote it by $k[x] \mod P$).

Complex numbers

The set of integer numbers is denoted by $\mathbb{Z}$ and the set of real numbers is denoted by $\mathbb{R}$. Let $\mathbb{C}$ be a set of pairs of real numbers (a, b) with addition defined by the formula $(a, b)+(c, d) = (a+c, b+d)$ and with multiplication defined by formula

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

Elements of $\mathbb{C}$ are called complex numbers.

Exercise 1.36. Check that $\mathbb{C}$ is a ring. Prove that an equation $x^2 + 1 = 0$ has a solution in $\mathbb{C}$. How many solutions does it have?

Exercise 1.37. Let us take a solution of an equation $x^2 + 1$ in $\mathbb{C}$ and denote it by $\sqrt{-1}$. Prove that any complex number can be uniquely represented in the form $a + b\sqrt{-1}$, $a, b \in \mathbb{R}$.

Exercise 1.38. Build an isomorphism $\mathbb{C} \cong (\mathbb{R}[x] \mod P)$ where P is a polynomial $P = x^2 + 1$.

Exercise 1.39. Consider a complex number $z := a + b\sqrt{-1}$. A number conjugate to z is the number $\overline{z} := a - b\sqrt{-1}$. Prove that complex conjugation preserves multiplication and addition in $\mathbb{C}$ (such mappings are called automorphisms of the field $\mathbb{C}$).

Exercise 1.40. Consider a complex number $z := a + b\sqrt{-1}$. Prove that $z\overline{z}$ is real (it means that in the representation of a complex number (x, y) the component y is zero).

Exercise 1.41. Consider a complex number $z := a + b\sqrt{-1}$. Prove that $z\overline{z} = a^2 + b^2$. That means in particular the this number is always nonnegative and equals zero only if $z = 0$. $z\overline{z}$ is often written down as $|z|^2$ since the length of a vector (a, b) on a plane equals $\sqrt{a^2 + b^2}$ (the distance between z 0, $|z|$ is called a modulus of z).

Exercise 1.42. Deduce from the previous problem that complex numbers form a field.

Hint. $z^{-1} = \overline{z}|z|^{-2}$

Exercise 1.43. Prove "triangle inequality": $|z_1| - |z_2| \leqslant |z_1 + z_2| \leqslant |z_1| + |z_2|$

Exercise 1.44. Prove that $|z_1 z_2| = |z_1||z_2|$.

Exercise 1.45 (!). Let $z = a + b\sqrt{-1}$ be a complex number with the modulus equal to 1: $|z| = 1$. Let us regard the multiplication by z as a transformation of a plane $\mathbb{R}^2$ associated naturally with $\mathbb{C}$. Prove that if $z \neq 1$ then this transform is planar motion with a single fixed point $0 \in \mathbb{R}^2$.

Exercise 1.46 (!). It is known from geometry that a planar motion with the only fixed point $0 \in \mathbb{R}^2$ is a rotation by some angle φ around 0. Given φ, how a and b can be found in task 1.45?

Remark. The angle φ is called an **argument** of complex number z.

Exercise 1.47 (!). Prove the formula $\cos(\varphi + \psi) = \cos\varphi \sin\psi + \sin\varphi \cos\psi$.

Hint. Use the previous problem.

Exercise 1.48 (!). Prove that an equation $z^n = 1$ has precisely n complex solutions.

Hint. Use the trigonometric interpretation of complex numbers.

Exercise 1.49 (*). Consider a polynomial P of a degree less than n and let $\zeta_1, \ldots, \zeta_n$ be "the roots of n-th degree from 1" or, simply put, let $\zeta_1, \ldots, \zeta_n$ be all complex $z^n = 1$. Prove that the mean $\frac{1}{n}\sum P(\zeta_i)$ of values of P in all the points ζ_i equals $P(0)$.

Hint. Use the trigonometric interpretation of complex numbers.

Exercise 1.50 (*). Consider a polynomial P of a degree less than n. Let Ξ be a regular n-gon on a complex plane $\mathbb{C} = \mathbb{R}^2$. Prove that the value of P in the center of Ξ equals to the mean of values of P in the vertices of Ξ.

Hint. Use the previous problem.

Remark. Archimedes defined the perimeter of a circle as a limit of perimeters of polygons inscribed into it. If we follow Archimedes then we can define the mean of a function f defined on a circle as a limit (by n) of means $\frac{1}{n}\sum f(\zeta_i)$ where z_i are vertices of regular n-gons inscribed into the circle. One can deduce from the previous problem that the mean of values of a polynomial function P on a unity circle $|z| = 1$ equals the value of P in its center.

Exercise 1.51. Calculate the group of automorphisms of $\mathbb{C}$

a. (*)which translate $\mathbb{R} \subset \mathbb{C}$ into itself.

b. which translate the subfield $\mathbb{R} \subset \mathbb{C}$ into itself and do not move its elements.

Exercise 1.52 (!). Let us change the definition of complex numbers. Instead of

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

let us put

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

Let us denote the obtained structure by $\mathbb{R}_2$. Is $\mathbb{R}_2$ a ring? Is it a field? Find all solutions of an equation $z^2 = 1$ in $\mathbb{R}_2$. Find all the solutions of an equation $z^2 = 0$ in $\mathbb{R}_2$.

Exercise 1.53 (!). Let us change the definition of complex numbers. Instead of

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

let us put

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

Let us denote the obtained structure by $\mathbb{R}_\varepsilon$. Is $\mathbb{R}_\varepsilon$ a ring? Is it a field? Is it isomorphic to $\mathbb{R}_2$ from the previous problem? Find all the solutions of an equation $z^2 = 1$.

Exercise 1.54 (*). Find all the solutions of an equation $z^2 = z$ in two previous problems.

Exercise 1.55 (*). Let $P = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n with n roots lying outside the unit circle. Prove that $\frac{a_k}{a_0} < C_n^k$ where $C_n^k = \frac{n!}{k!(n-k)!}$ is a binomial coefficient.